Question #1 *Topic 1*

DRAG DROP -

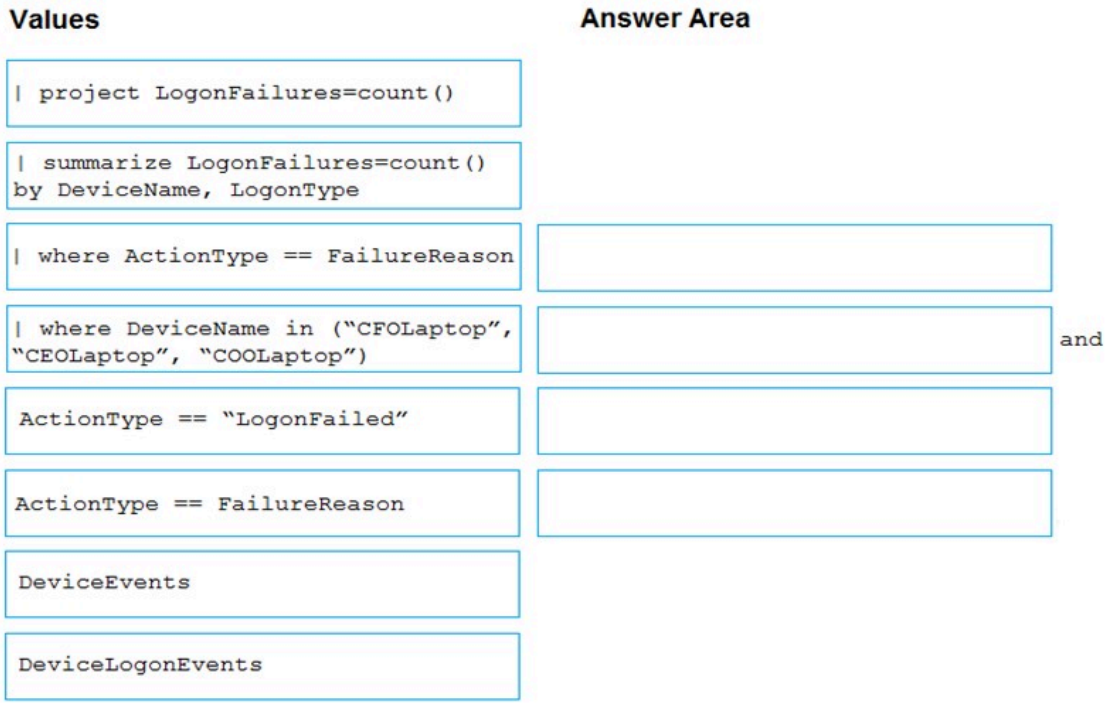
You are investigating an incident by using Microsoft 365 Defender.

You need to create an advanced hunting query to count failed sign-in authentications on three devices named CFOLaptop, CEOLaptop, and COOLaptop.

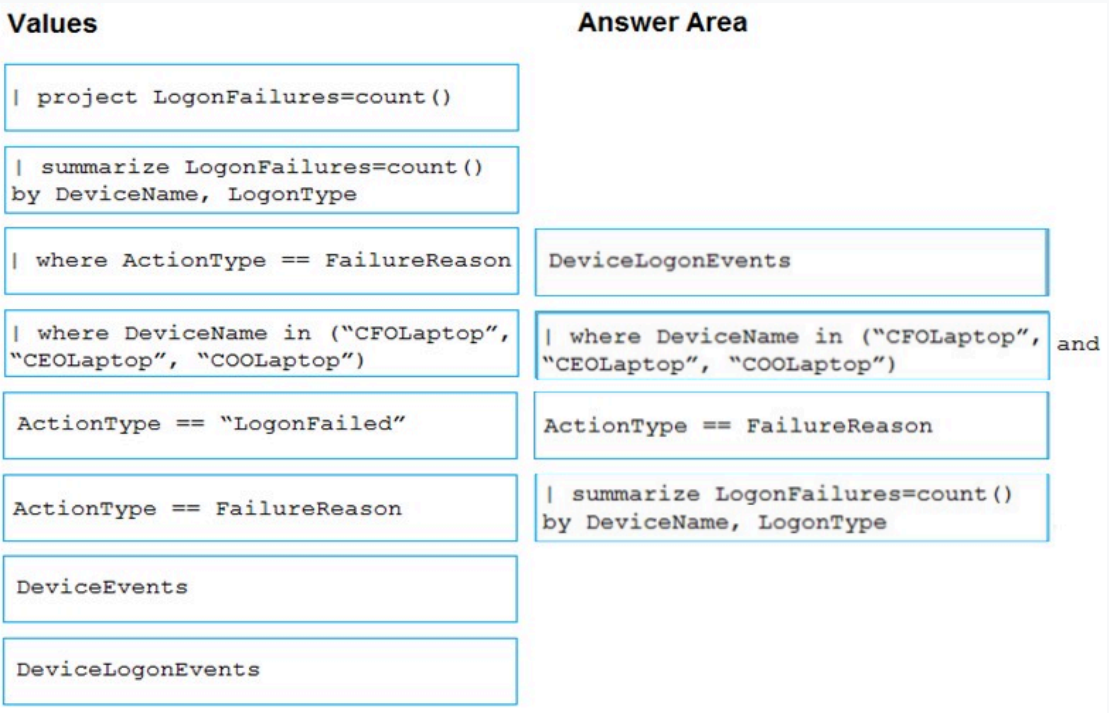
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



DigitalNomad Highly Voted 3 months, 2 weeks ago

DeviceLogonEvents

| where DeviceName in ("CFOLaptop" , "CEOLaptop") and ActionType == "LogonFailed"

| summarize LogonFailures=count() by DeviceName , LogonType

This is the correct answer , I tested it .
upvoted 119 times

Nikki0222 2 months, 1 week ago
This answer is correct
upvoted 1 times

CatoFong 2 years, 5 months ago
DigitalNomad is correct.
upvoted 3 times

sasasach 1 year, 9 months ago
correct.
upvoted 3 times

danb67 1 year, 2 months ago
Me too and correct
upvoted 1 times

ReffG Highly Voted 3 years, 4 months ago
I think the third box is answered wrong. ActionType == "LogonFailed" should be the correct answer.
upvoted 21 times

mikl Most Recent 1 month, 1 week ago
ChatGPT says :

DeviceLogonEvents
| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop")
| where LogonType == "Failed"
| summarize FailedSignInCount = count() by DeviceName
upvoted 1 times

Apocalypse03 3 months, 1 week ago
The correct answer is:

DeviceLogonEvents

| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") and

ActionType == FailureReason

|s summarize LogonFailures=count () by DeviceName, LogonType

Here is a brief explanation of how this query works:

The DeviceLogonEvents table is selected, which contains logon events for devices.

The where clause filters the events to only include those that have a DeviceName of CFOLaptop, CEOLaptop, or COOLaptop, and an ActionType of FailureReason. This effectively filters the events to only include failed logon events from the specified devices.

The summarize clause counts the number of events that match the previous criteria, grouping the results by DeviceName and LogonType. The count() function counts the number of events in each group, and the LogonFailures alias is used to label this count in the resulting output.
upvoted 3 times

EricChu 2 years ago
How can a reason be an action???? Action type is a reason, did you hear yourself?
upvoted 1 times

Hawklx 5 months, 3 weeks ago
Please fix this answer
upvoted 2 times

Vamshi_Pasham 9 months, 2 weeks ago

In given answer, ActionType should be "LogonFailed".
upvoted 2 times

mc250616 1 year, 1 month ago
Hi All,
Checked again in real environment. Shown answer is not correct as Failure Reason is not one fo the ActionTypes and no result by this search.
Correct Answer is ;

DeviceLogonEvents
| where DeviceName in ("CFOLaptop" , "CEOLaptop", "COOLaptop") and
ActionType == "LogonFailed"
| summarize LogonFailures=count() by DeviceName , LogonType
upvoted 2 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

NathanZ 1 year, 5 months ago
Correct answer should be: ActionType="LogonFailed".
When running this query, there is no any result returned.
DeviceLogonEvents
| where ActionType == FailureReason
upvoted 1 times

cyber_mks 1 year, 9 months ago
correct Answer is DeviceLogonEvents

| where DeviceName in ("CFOLaptop", "CEOLaptop", "COOLaptop") and

ActionType == FailureReason

|s summarize LogonFailures=count () by DeviceName, LogonType
upvoted 1 times

gyaansastra 2 years ago
Only 3 types of ActionType exist based on the schema. Try yourself with a long time range (e.g below last 14days)

DeviceLogonEvents
| where TimeGenerated >= ago(14d)
| distinct ActionType

Result:
LogonSuccess
LogonFailed
LogonAttempted

That should clear the doubts that "LogonFailed" is the correct option, not "FailureReason". Strongly suggest going through the official schema and the actual query for validation.
upvoted 6 times

BhanuD 2 years, 1 month ago
Under DeviceLogonEvents schema, below are the ActionType values available and FailureReason is the column in the schema that can be fetched
ActionType values:
LogonAttempted
LogonFailed
LogonSuccess
and hence the answer is ActionType == 'LogonFailed' ; also a string should be mentioned in a single or double quotes
upvoted 2 times

arunrider 2 years, 2 months ago

Tested, ActionType == LogonFailed
upvoted 4 times

Pandaguo 2 years, 8 months ago
DeviceLogonEvents
|where Devicename in ("CFOlaptops", "CEOLaptop") and ActionType == "LogonFailed"
|summarize LoginFailures=count() by DeviceName, LogonType
upvoted 3 times

oreoale 2 years, 9 months ago
See DeviceLogonEvents options -> https://docs.microsoft.com/en-us/azure/azure-monitor/reference/tables/devicelogonevents
upvoted 4 times

chaska 2 years, 9 months ago
Answer is correct
DeviceLogonEvents
| where DeviceName in ("CFOLaptop","CEOLaptop","COOLaptop") and ActionType == FailureReason
| summarize count() by DeviceName, LogonType,TimeGenerated
As far as I know ActionType contains only LogonSuccess, LogonAttempted and empty value.
Empty value in same rows in columns ActionType and FailureReason means failed sign-in authentications.
upvoted 3 times

Badr_j 2 years, 9 months ago
ActionType == "LogonFailed" is the correct option,
upvoted 4 times

Question #2 *Topic 1*

You need to receive a security alert when a user attempts to sign in from a location that was never used by the other users in your organization to sign in.
Which anomaly detection policy should you use?

A. Impossible travel

B. Activity from anonymous IP addresses

C. Activity from infrequent country

D. Malware detection

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Community vote distribution
C (100%)

teehex Highly Voted 3 years, 7 months ago
Activity from infrequent country is the correct answer.

First, both "Impossible travel" and "Activity from infrequent country" are detection rule that help prevent breaches from foreign attackers.

The difference between the rule is the type of historical data. "Impossible travel" actually compares between the new location's sign-in with the last known one. So it basically means if someone already logged into a location (corporate network with USA-based IP range) and now he is logged into a China network then it is likely the user is compromised (assume the organization doesn't have any traffic/record/association with China network). Moreover it is based on geographically distant locations within a time period shorter. So in my example China is too far from USA.

"Activity from infrequent country" is a bit different. Instead of comparing with the last known location, it detects if an account is logged in from a country that has never been accessed by any user in the organization. This rule is based on user behavior using entity behavioral analytics and machine learning.
upvoted 50 times

peponokefalos 1 year, 1 month ago
Really nice explanation. Thank you for that!
upvoted 2 times

dandirindan 2 years, 7 months ago
great explanation
upvoted 2 times

teehex 3 years, 7 months ago
In addition to my explanation:
- Impossible travel often looks into one sign-in attempt from TWO different geo-based location.
- Activity from infrequent country often looks into a location that no one ever used. So basically it just perform a check among all historical locations and does the comparison.
upvoted 11 times

TheMCT Highly Voted 3 years, 9 months ago
Given Answer, C, is correct
upvoted 36 times

Startkabels 3 years, 2 months ago
Agree, I work with these policies daily
upvoted 5 times

prabhjot 2 years, 11 months ago
this is correct as explained here also - https://docs.microsoft.com/en-us/defender-cloud-apps/investigate-anomaly-alerts

upvoted 4 times

mikl Most Recent 1 month, 1 week ago

Selected Answer: C

Explanation:
The "Activity from infrequent country" anomaly detection policy generates alerts when a user attempts to sign in from a location (country or region) that has not been previously used by other users in the organization. This is designed to detect potentially suspicious or unauthorized login attempts.

upvoted 1 times

nk_exam 1 month, 3 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

Nikki0222 2 months, 1 week ago

Answer is C

upvoted 1 times

ESAJRR 1 year, 1 month ago

Selected Answer: C

C. Activity from infrequent country

upvoted 2 times

chepeerick 1 year, 2 months ago

Selected Answer: C

Option C

upvoted 2 times

Wedge34 1 year, 3 months ago

Selected Answer: C

C is the right answer

upvoted 2 times

tatendazw 1 year, 7 months ago

Triggered by anomaly detection rule policy "Activity from infrequent country", this requires 7 days to learn the locations frequently used
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy#activity-from-infrequent-country

upvoted 1 times

cyber_mks 1 year, 9 months ago

C, is correct

upvoted 2 times

CarlosE 1 year, 11 months ago

Selected Answer: C

C is correct

upvoted 2 times

emmanuelodenyire 1 year, 11 months ago

Selected Answer: C

I will go with C

upvoted 1 times

simonseztech 2 years, 4 months ago

Selected Answer: C

https://docs.microsoft.com/en-us/defender-cloud-apps/investigate-anomaly-alerts

upvoted 1 times

Pandaguo 2 years, 8 months ago

C is right

upvoted 1 times

Tx4free 2 years, 10 months ago

Selected Answer: C

C is correct

upvoted 1 times

ubt 2 years, 10 months ago

Selected Answer: C

Activity from infrequent country

This detection considers past activity locations to determine new and infrequent locations. The anomaly detection engine stores information about previous locations used by users in the organization. An alert is triggered when an activity occurs from a location that wasn't recently or never visited by any user in the organization.

upvoted 1 times

Minghon 2 years, 12 months ago

Selected Answer: C

Activity from infrequent country

This detection considers past activity locations to determine new and infrequent locations. The anomaly detection engine stores information about previous locations used by users in the organization. An alert is triggered when an activity occurs from a location that wasn't recently or never visited by any user in the organization.

upvoted 1 times

Question #3 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.
You have Microsoft SharePoint Online sites that contain sensitive documents. The documents contain customer account numbers that each consists of 32 alphanumeric characters.
You need to create a data loss prevention (DLP) policy to protect the sensitive documents.
What should you use to detect which documents are sensitive?

A. SharePoint search

B. a hunting query in Microsoft 365 Defender

C. Azure Information Protection

D. RegEx pattern matching

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

Community vote distribution
D (59%) C (41%)

teehex Highly Voted 3 months, 2 weeks ago
Azure API is the correct answer. The question is asking what you need. It is not asking you how to do it.

You must use Azure AIP as a tool for DLP. And then Regex is a way to build your pattern in case there is not any built-in sensitive pattern type that supports your case (account number with 32 char).

So bonus the regex ^[a-zA-Z0-9]{32}$
upvoted 62 times

cedreh 2 weeks, 2 days ago
You can use a regex in Microsoft Purview Data Loss Prevention (DLP) to define patterns that help you identify and classify sensitive data, or to help detect patterns in content.
https://learn.microsoft.com/en-us/purview/dlp-policy-learn-about-regex-use
REF Guide: https://docs.google.com/document/d/15AgfSOKqg-51pM8O9zp08DHXIrLIXw6Ir4ae_m0WkTY
upvoted 1 times

Chris2pher 4 months, 2 weeks ago
The key word is "use to detect" AIP is a tool right? And it uses the regex to "detect". So I think its Regex that is used to detect not the tool AIP.
upvoted 1 times

ANDRESCB1988 3 years, 5 months ago
is correct!
upvoted 1 times

Startkabels 3 years, 2 months ago
Agreed
upvoted 1 times

Question #4 *Topic 1*

Your company uses line-of-business apps that contain Microsoft Office VBA macros.

You need to prevent users from downloading and running additional payloads from the Office VBA macros as additional child processes.

Which two commands can you run to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -
4EFC -AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

B.

```
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
```

C.

```
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC
-AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions AuditMode
```

D.

```
Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB -401B -4EFC -
AADC -AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled
```

Suggested Answer: *BC*

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

JohnAvlakiotis Highly Voted 3 years, 3 months ago

Should be A, D.

upvoted 101 times

Metasploit 3 months, 2 weeks ago

A,D.

These are 2 complete solutions on their own. Not a step by step by step.

1) Add the rule and enable it.

2) Add the rule, set the rule to overwrite existing rules, and enable it.

"Set-MpPreference will always overwrite the existing set of rules. If you want to add to the existing set, use Add-MpPreference instead."

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#powershell

The command does not need to mention anything about block because the GUID references a Rule with already set actions.

Configuration Manager name: Block Office application from creating child processes

GUID: d4f940ab-401b-4efc-aadc-ad5f3c50688a

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?source=recommendations&view=o365-worldwide#block-all-office-applications-from-creating-child-processes

upvoted 22 times

AlaReAla 3 years, 3 months ago

I echo, as the requirement is not for audit, but to prevent. So the answer should be A & D.

upvoted 15 times

Startkabels 3 years, 2 months ago

Agree, auditing doesnt prevent anything only monitors and reports

upvoted 1 times

JohnAvlakiotis 3 years, 2 months ago

Agreed, link to reinforce https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#powershell

upvoted 6 times

smanzana 1 year, 1 month ago

I agree, A and D
upvoted 1 times

BMG6 1 year, 4 months ago
agree @JohnAvlakiotis A,D...
The question or task is to PREVENT. Audits do not accomplish this task.
upvoted 8 times

Haz56 Highly Voted 3 years ago
I would say A&D as the question states "Each correct answer presents a complete solution.", so choosing one of the audit options would not be a complete solution on its own to prevent the action
upvoted 13 times

pedromonteirozikado 2 years, 11 months ago
Yes, normally we add a new audit policy with Add-MpPreference and change the policy to enabled with Set-MpPreference, but in this case, each correct answers presents a complete solution, A&D Right, cause Set can change and create policies too, and Add-MpPreference can only add new policies.
upvoted 2 times

Nikki0222 Most Recent 2 months, 1 week ago
Answer is A,D
upvoted 3 times

Hawklx 5 months, 3 weeks ago
It is A and D but we cannot vote for it
upvoted 3 times

4b097e5 6 months, 1 week ago
A and D is correct since we need to prevent users and not monitor them.
upvoted 2 times

Harryd82 8 months ago
A & D is correct answer
upvoted 1 times

28meters 8 months, 1 week ago
It is A and D. B and C Place their respective commands in audit mode, which only generates logs and does not take any other action
upvoted 1 times

AVN1711 8 months, 1 week ago
correct me if I am wrong, but: first sentence is "Your company uses line-of-business apps that contain Microsoft Office VBA macros." that is mean you already have something and it should work, so you set to Audit only as an exclusion for this particular Macros you need to use, al others/new still gonna be blocked.. so the correct answer is B and C
upvoted 1 times

Dracula666 1 year, 2 months ago
Add-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EfC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-demonstration-attack-surface-reduction-rules?view=o365-worldwide#scenario-2-asr-rule-blocks-the-test-file-with-the-corresponding-vulnerability

Set-MpPreference -AttackSurfaceReductionRules_Ids D4F940AB-401B-4EFC-AADC-AD5F3C50688A -AttackSurfaceReductionRules_Actions Enabled

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/troubleshooting-mode-scenarios?view=o365-worldwide
upvoted 1 times

donathon 1 year, 4 months ago
should be AD.
upvoted 1 times

tatendazw 1 year, 7 months ago
A&D https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide#powershell
upvoted 2 times

wyindualizer 1 year, 9 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view=o365-worldwide

upvoted 1 times

SavageJ 1 year, 9 months ago

Set-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions Enabled

--

Add-MpPreference -AttackSurfaceReductionRules_Ids <rule ID> -AttackSurfaceReductionRules_Actions AuditMode

upvoted 1 times

Nailik_Ms 1 year, 11 months ago

Audit does not mean Blocking Question stands for "You need to prevent users from downloading and running additional payloads from the Office VBA macros as additional child processes." Auditing something you are not implementing anything to prevent, but to gain the knowledge to later on take the action you want to.

upvoted 2 times

Atun23 2 years, 2 months ago

According to MS content this should be A and D, because the company is trying to prevent, not checking first if it will work.

Audit mode for evaluation

Use audit mode to evaluate how attack surface reduction rules would affect your organization if enabled. Run all rules in audit mode first so you can understand how they affect your line-of-business applications. Many line-of-business applications are written with limited security concerns, and they might perform tasks in ways that seem similar to malware. By monitoring audit data and adding exclusions for necessary applications, you can deploy attack surface reduction rules without reducing productivity

upvoted 2 times

ArunRavilla 2 years, 3 months ago

It is A & D. I am 100% sure.

upvoted 2 times

Sango 2 years, 4 months ago

A and D are the only logical two: Must use Set-MpPreference with Enabled and then Add-MpPreference with Enabled. Audit does not block.

upvoted 2 times

Question #5 *Topic 1*

Your company uses Microsoft Defender for Endpoint.
The company has Microsoft Word documents that contain macros. The documents are used frequently on the devices of the company's accounting team.
You need to hide false positive in the Alerts queue, while maintaining the existing security posture.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Resolve the alert automatically.

B. Hide the alert.

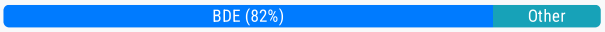
C. Create a suppression rule scoped to any device.

D. Create a suppression rule scoped to a device group.

E. Generate the alert.

Suggested Answer: *BCE*
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-alerts

Community vote distribution



KingSize Highly Voted 3 months, 2 weeks ago
You can Hide or Resolve alert and all of those actions you can perform on any device or device groups or single device. But in question there is accounting team so there will be device group.
Answer should be ABD
upvoted 56 times

AnonymousJhb 2 years, 9 months ago
D is wrong.
This "group" feature is only available in Suppress alerts from Microsoft Defender for Cloud.
This question context is for Manage Microsoft Defender for Endpoint alerts.
There are two contexts for a suppression rule that you can choose from:
-Suppress alert on this device
-Suppress alert in my organization
upvoted 6 times

Metasploit 3 months, 1 week ago
BDE.
This changed. I know, not in the docs(Docs are old and not updated). I had to go to the tech community.

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/introducing-the-new-alert-suppression-experience/ba-p/3562719
upvoted 8 times

BhanuD 2 years, 1 month ago
Hi, may be the documentation is not updated, the scope is to select organization or user/device/device groups, as they mentioned clearly as accounts department, device group need to be selected
upvoted 3 times

Ashfaq2 3 years, 7 months ago
Suppression rule can not create based on Device Group
upvoted 5 times

sasasach 2 years ago
I checked it in MS defender itself, you can create suppression rule based on device group
upvoted 3 times

jethi 3 years, 6 months ago
Suppression rule can be created based on a device group. Verified it on the defender portal itself. Correct answer is BDE

upvoted 35 times

uday1985 8 months, 1 week ago
why generating alerts when the ask to suppress
upvoted 1 times

xRiot007 1 month ago
Because you want to see the alert for insights. Suppressing an alert means that the alert will get generated, but the underlying action will not be executed.
upvoted 1 times

AlaReAla 3 years, 3 months ago
it cannot be A as we need to hide, not resolve (so it should be B). I suppose it can to D, and E is anyhow the right option. So in all, ans should be BDE.
upvoted 12 times

sadako 2 years, 9 months ago
Shortcut for easier reference:
Hide alert
Create supression rule to device group
Generate alert
upvoted 3 times

sadako 2 years, 9 months ago
Sorry i was wrong. Correct shortcut should be:
Resolve alert
Hide alert
Create supression rule to device group
upvoted 4 times

PTIN Highly Voted 3 years, 8 months ago
Given answer BCE is correct. The question states "alerts must be hidden from queue". Automatically resolving is not correct solution as that will still show up in the queue. Hence given answer BCE is correct
upvoted 19 times

Metasploit 2 years, 2 months ago
Not A = Resolved alerts stay in Alerts queue marked as resolved.
B = You can hide alerts from the system.
C = 1.)Suppress alert on this device or 2.) Suppress alert in my organization (For MS Defender for Endpoint)
Not D = Because C
E = Because you cannot do either of the other without an alert.
upvoted 1 times

Metasploit 3 months, 1 week ago
Correction: BDE
This question bugged me. The new alert suppression rules allows for much more.

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/introducing-the-new-alert-suppression-experience/ba-p/3562719
upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago
Answer is BDE.
upvoted 1 times

Metasploit 3 months, 1 week ago
Selected Answer: BDE
NOT A = Resolved alerts stay in Alerts queue marked as resolved.
B = You can hide alerts from the system.
NOT C = Not best practice.
D = Because, Best practice and New alert suppression rules allow for groups and much more(The docs are still old, below is a link for evidence to this claim)

https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/introducing-the-new-alert-suppression-experience/ba-p/3562719

E = Because you cannot do either of the other without an alert.
upvoted 7 times

Apocalypse03 3 months, 1 week ago

Selected Answer: BDE

Generate the alert. This will trigger the alert for the detected macro in the Word document.
Hide the alert. This will prevent the alert from appearing in the Alerts queue.
Create a suppression rule scoped to a device group. This will ensure that the rule only applies to the devices of the accounting team, while maintaining the existing security posture for other devices in the company.
upvoted 4 times

Lone__Wolf 3 months, 1 week ago

Selected Answer: BDE

Here's a brief explanation of each option:

E. Generate the alert: You need to generate the alert first so that you can see it in the Alerts queue.

B. Hide the alert: After generating the alert, you can hide it if you want to remove it from view.

D. Create a suppression rule scoped to a device group: You can also create a suppression rule scoped to a specific device group if you want to only apply it to a specific group of devices. This helps you maintain the existing security posture.
upvoted 11 times

EricShon 3 months, 1 week ago

Selected Answer: BDE

B. Hide the alert (for immediate, manual action)
D. Create a suppression rule scoped to a device group (for a targeted, long-term solution)
E. Generate the alert
upvoted 6 times

user636 3 months, 1 week ago

Selected Answer: BDE

You can either hide or automatically resolve the alert using a suppression rule in MDE.
Ref: https://learn.microsoft.com/en-us/defender-endpoint/manage-alerts#suppress-alerts

The answer is:
A or B (both are correct)
D
E
upvoted 1 times

g_man_rap 3 months, 2 weeks ago

E. Generate the alert.

This step is implicit, as the alert needs to be generated and identified as a false positive before any suppression or hiding actions can be taken.
D. Create a suppression rule scoped to a device group.

After identifying the alert as a false positive, you create a suppression rule scoped to the specific device group (e.g., the accounting team's devices) to prevent similar alerts from showing up in the future.
B. Hide the alert.

Finally, you hide the current false positive alert from the queue to reduce noise, keeping the Alerts queue focused on relevant security incidents.
upvoted 1 times

4b097e5 6 months, 1 week ago

BDE is correct answer
upvoted 2 times

chepeerick 1 year, 2 months ago

Selected Answer: BDE

B and D and E

upvoted 2 times

Unlikely 1 year, 3 months ago

My 2 cents. BCE. A false positive is a false positive, regardless of which group of users causes it more often. The question states that a specific group uses the document more often than the others, not that this is a FP only when that specific group opens the document. So, more than one group of users in the company can open that document and generate the FP: hence, it makes no sense to suppress the FP for one specific group.

upvoted 1 times

BMG6 1 year, 4 months ago

BDE

No (task is to HIDE) A. Resolve the alert automatically.

B. Hide the alert.

No (task is for Accounting Computers) C. Create a suppression rule scoped to any device.

D. Create a suppression rule scoped to a device group.

E. Generate the alert.

upvoted 2 times

Abujumaa 1 year, 4 months ago

Selected Answer: BCE

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide

upvoted 1 times

mali1969 1 year, 4 months ago

We can perform three actions to hide false positives in the Alerts queue, while maintaining the existing security posture:

Create a suppression rule scoped to a device group

Hide the alert

Resolve the alert automatically

These actions will allow you to suppress alerts that are known to be harmless for a specific group of devices, such as the accounting team's devices, and remove them from the Alerts queue without affecting other alerts or devices

upvoted 1 times

donathon 1 year, 5 months ago

Selected Answer: BDE

BDE Make sense

upvoted 2 times

Yurri 1 year, 5 months ago

Selected Answer: ABD

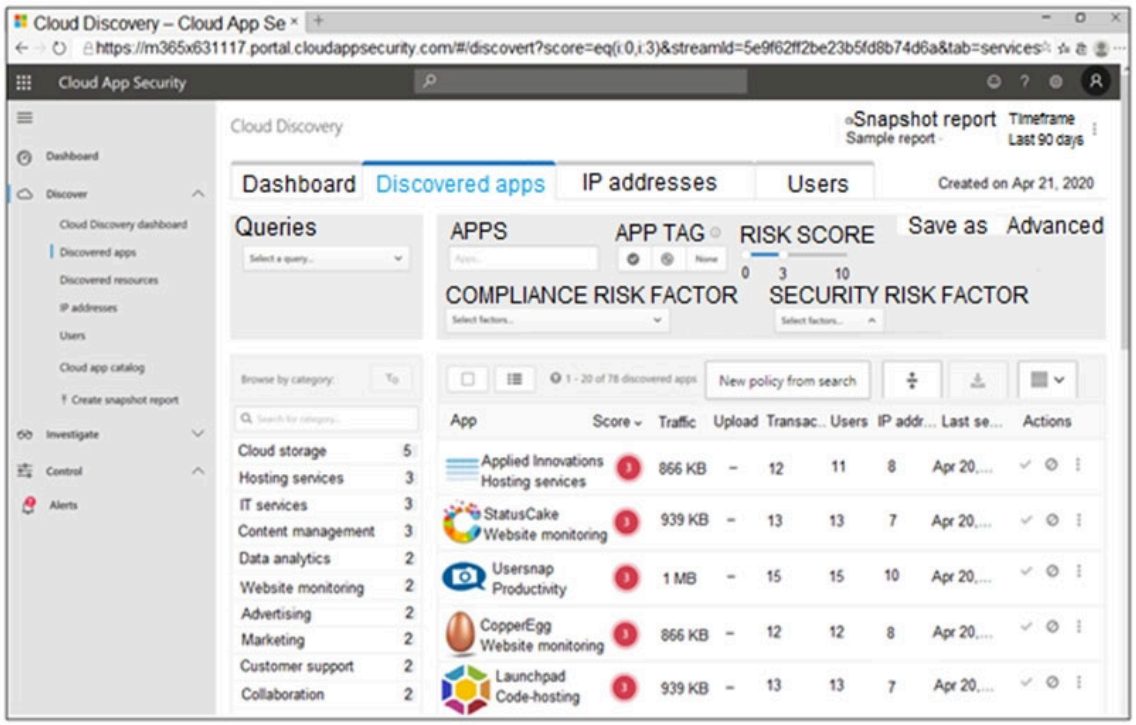
A, B, D.

upvoted 1 times

Question #6 *Topic 1*

DRAG DROP -

You open the Cloud App Security portal as shown in the following exhibit.

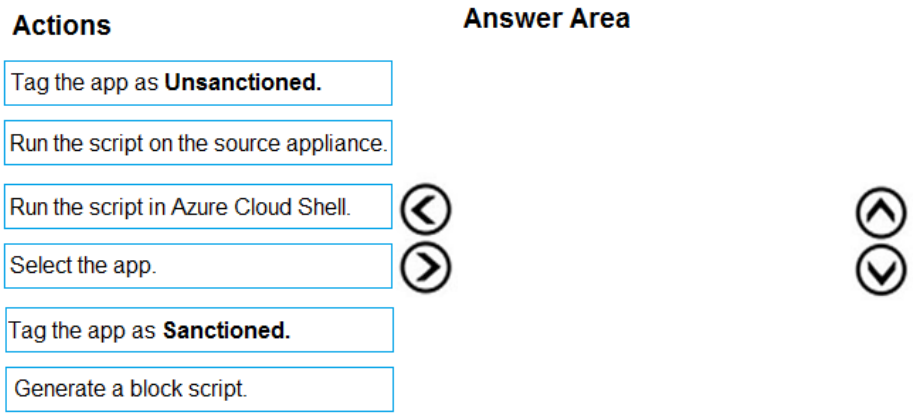


Your environment does NOT have Microsoft Defender for Endpoint enabled.

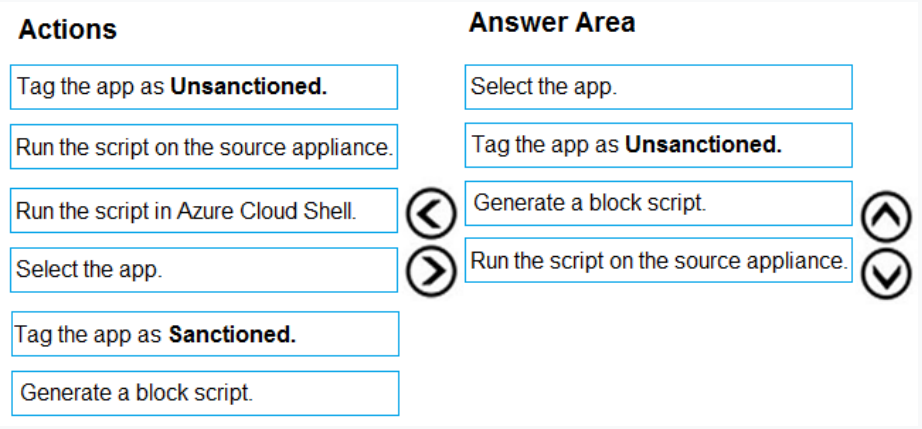
You need to remediate the risk for the Launchpad app.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

hteams Highly Voted 3 months, 2 weeks ago
The "source appliance" mentioned here is the Firewall or Proxy in use. The Block script is specific to the product in use. The block is done by the firewall / proxy . Hope this helps
you can find the screenshots at this link https://docs.microsoft.com/en-us/defender-cloud-apps/governance-discovery
upvoted 20 times

iwhoelse Highly Voted 1 year, 10 months ago
Answer as shown is correct
upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago
Given answer is correct
upvoted 2 times

g_man_rap 4 months, 1 week ago
Select the app.
You need to identify and select the Launchpad app within your management interface to apply further actions.

Tag the app as Unsanctioned.
Marking the app as "Unsanctioned" identifies it as not allowed within the organization's environment, signaling that it should be blocked or restricted.

Generate a block script.
After tagging the app as unsanctioned, you generate a block script that can be used to enforce the blocking of the app across your network.

Run the script on the source appliance.
Finally, you deploy the block script to the relevant network appliance or gateway device to actively block the app's traffic and mitigate the associated risks.
upvoted 3 times

e072f83 8 months ago
select the app,
Tag the app as Unsanctioned,
Generate a block script,
Run the script on the source appliance
upvoted 5 times

estyj 12 months ago
In this case it says your environment does NOT have MS Defender for Endpoint enabled, so even if you tag app as unsanctioned it will not block but enables you to monitor its use with Cloud Discover filters. In this case you need to generate block script and for the network source appliance, firewall, proxy and import the file you created to your appliance to actually block the app.
upvoted 3 times

smanzana 1 year, 1 month ago
It's correct
upvoted 1 times

chepeerick 1 year, 2 months ago
This is correct
upvoted 1 times

tatendazw 1 year, 7 months ago
https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#block-apps-by-exporting-a-block-script
upvoted 3 times

Hami3191 2 years, 5 months ago
correct answer
upvoted 4 times

vijeet 2 years, 9 months ago
If your tenant uses Microsoft Defender for Endpoint, Zscaler NSS, or iboss, any app you mark as unsanctioned is automatically blocked by Defender for Cloud Apps, and the following sections regarding creating blocking scripts are unnecessary. For more information, see Integrate with Microsoft Defender for Endpoint, Integrate with Zscaler, and Integrate with iboss respectively.
upvoted 3 times

pedromonteirozikado 2 years, 11 months ago

The answer provided is correct.

upvoted 4 times

cloudster998 2 years, 11 months ago

After you've reviewed the list of discovered apps in your environment, you can secure your environment by approving safe apps (Sanctioned) or prohibiting unwanted apps (Unsanctioned) in the following ways.

upvoted 2 times

Qadir 3 years, 3 months ago

On other websites they have mentioned as "TAG the app as sanctioned"

upvoted 1 times

AlaReAla 3 years, 3 months ago

I differ with your opinion. it should be Unsanction. The above URL clearly says "You can unsanction a specific risky app by clicking the three dots at the end of the row. Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters."

upvoted 9 times

AlaReAla 3 years, 3 months ago

Somehow I still have doubts whether it should be executed on Source appliance OR Azure Cloud Shell? Any thoughts will be helpful.

upvoted 1 times

zaqwsx 3 years, 2 months ago

I will go with the source appliance, you need to create a script to block it on the endpoint

upvoted 3 times

felipe_g 2 years, 10 months ago

But it says that Ms Defender for Endpoint is not deployed

upvoted 2 times

Anko6116 1 year, 10 months ago

In the provided article it is stated clearly that you should run on source appliance. Section: Block apps by exporting a block script; step 5: "Import the file created to your appliance."
https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery

upvoted 3 times

HOTSPOT -

You have a Microsoft 365 E5 subscription.

You plan to perform cross-domain investigations by using Microsoft 365 Defender.

You need to create an advanced hunting query to identify devices affected by a malicious email attachment.

How should you complete the query? To answer, select the appropriate options in the answer area.

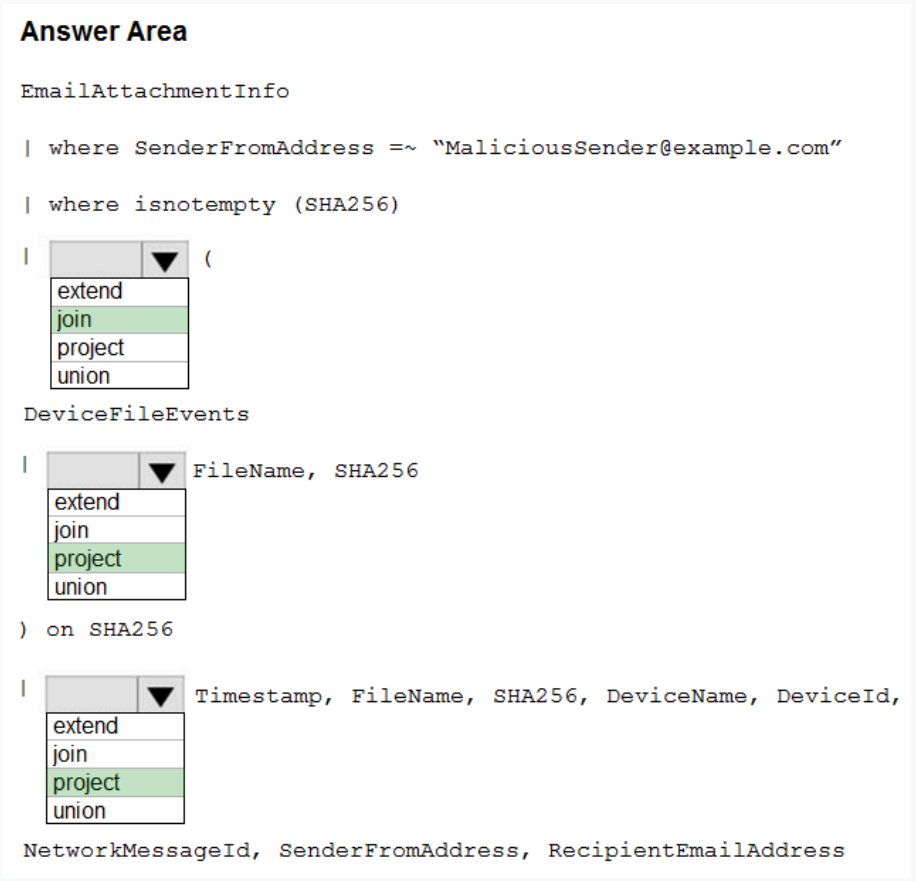
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
| where isnotempty (SHA256)
| [extend / join / project / union] (
DeviceFileEvents
| [extend / join / project / union] FileName, SHA256
) on SHA256
| [extend / join / project / union] Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/mtp/advanced-hunting-query-emails-devices?view=o365-worldwide

teehex Highly Voted 3 years, 7 months ago

EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com" //Get emails with attachments identified by a SHA-256
| where isnotempty(SHA256)
| join (
//Check devices for any activity involving the attachments
DeviceFileEvents
| project FileName, SHA256
) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress

Already posted here https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your-devices
upvoted 51 times

JoeP1 1 year, 5 months ago

On that web site the current version has "| project FileName, SHA256, DeviceName, DeviceId"
with both DevcieName and DeviceId on that line.
Without DeviceName and DeviceId explicitly listed it should probably be Extend on that line with the full set of answers: Join, Extend, Project.
upvoted 3 times

PJR Highly Voted 3 months, 1 week ago

The query posted on MS docs doesnt actually work (I have tested in a live tenant) - it needs to be amended to match the below before it returns results (note the requirement to add DeviceName, and DeviceId fields to the first project statement).

EmailAttachmentInfo
| where SenderFromAddress =~ "mcasdemo@juno.com"
| where isnotempty(SHA256)
| join (
DeviceFileEvents
| project FileName, SHA256, DeviceName, DeviceId

) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress

But if you choose the following from the answers presented in the question you will get the results you need to answer the question:

EmailAttachmentInfo
| where SenderFromAddress =~ "mcasdemo@juno.com"
| where isnotempty(SHA256)
| join (
DeviceFileEvents
| extend FileName, SHA256
) on SHA256
| project Timestamp, FileName, SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress

ie Choose, Join, Extend, Project from the drop downs

This has also been tested on live tenants and returns the correct result.
upvoted 35 times

DigitalNomad 3 years, 2 months ago
you are correct , I have tested it ,the query in the docs is correct as it contains DeviceName , DeviceId , but the one in the exam question is missing the DeviceName , DeviceId , so the answer should be Join , Extend , Project as you mentioned , but in case the real exam question has DeviceName , DeviceId then Join , Project , Project can be a correct answer like the example in the docs
upvoted 7 times

Contactfornitish 2 years, 10 months ago
Well! Extend operator is for calculated columns and would followed by a custom variable name and equal to sign (something akin to let but in context of table)

Doesn't make sense to use the same in join context

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/extendoperator
upvoted 3 times

Contactfornitish 2 years, 10 months ago
Refer to topic 1 question 17 on examtopics itself for differently worded but the same query
upvoted 1 times

arcausbd 1 year, 3 months ago
Microsoft documents correct but in the above question DeviceName, DeviceId are missing.
as per Microsoft documents Kusto query should be:
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
//Get emails with attachments identified by a SHA-256
| where isnotempty(SHA256)
| join (
//Check devices for any activity involving the attachments
DeviceFileEvents
| project FileName, SHA256, DeviceName, DeviceId
) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress
link: https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#:~:text=Check%20if%20files%20from%20a%20known%20malicious%20sender%20are%20on%20your%20devices
upvoted 1 times

Nikki0222 Most Recent 2 months, 1 week ago
Join , project, project
upvoted 1 times

Apocalypse03 3 months, 1 week ago

The EmailAttachmentInfo table is selected, which contains information about email attachments.

The where clause filters the attachments to only include those that were sent from the address "MaliciousSender@example.com" and have a non-empty SHA256 hash value. This effectively filters the results to only include attachments from the specified sender and that have a known hash value.

The join operator combines the results of the previous step with the results of a second query that selects the DeviceFileEvent table and projects the FileName and SHA256 fields. This effectively creates a join between the two tables based on the SHA256 field, linking the attachments with file events on devices.

The project operator selects the desired fields from the joined results and includes them in the final output.
upvoted 2 times

0610fcd 3 months, 1 week ago
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
//Get emails with attachments identified by a SHA-256
| where isnotempty(SHA256)
| join (
//Check devices for any activity involving the attachments
DeviceFileEvents
| project FileName, SHA256, DeviceName, DeviceId
) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress
upvoted 1 times

KTM_999 3 months, 1 week ago
Check file from a known malicious sender

EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
//Get emails with attachments identified by a SHA-256
| where isnotempty(SHA256)
| join (
//Check devices for any activity involving the attachments
DeviceFileEvents
| project FileName, SHA256, DeviceName, DeviceId
) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress
- https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your-devices
upvoted 1 times

scfitzp 5 months, 3 weeks ago
You have to use join, EXTEND, project.
If you use join, project, project you get the following error

'project' operator: Failed to resolve scalar expression named 'DeviceName'
upvoted 1 times

4b097e5 6 months, 1 week ago
given answer is correct as you can project anything and it doesn't matter if the question doesn't have device name and device id in it as compared to Microsoft docs. The answer should still remain the same as Join, Project, Project
upvoted 1 times

emartiy 7 months ago
When clearly read this KQL hunting query.. First you get EmailAttachmentInfo based on some filters and then add second column by using Join operator (check this syntax and you will see it is clearly "Join") the other 2 is Project. You return selected entities of event table log to merge all in a table (output). I will chose Join, Project Project for my exam if I see this question in exam :)
upvoted 1 times

emartiy 7 months ago

First column of "Join" operator is Email AttachmentInfo and second column is DeviceFileEvents.. So join is the first selection and other 2 is only get specific entities in log table (FileName, TimesStamp, RecipientsEmailAddresses etc..

upvoted 1 times

Harryd82 8 months ago

Join, Extend, Project.

upvoted 1 times

ae88d96 10 months, 2 weeks ago

The answer provided is correct. It is also mentioned here https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your-devices

upvoted 2 times

smanzana 1 year, 1 month ago

join-extend-project —> for the answer presented for Exam Topics)

or

join-project-project —> if the answer were “join (DeviceFileEvents | project FileName, SHA256, DeviceName, DeviceId) on SHA256” —> including “DeviceName” and “DeviceId”

upvoted 1 times

mb0812 10 months, 1 week ago

Its

wrong. extend keyword usage includes '='

upvoted 1 times

billo79152718 1 year, 5 months ago

join

extend

project

upvoted 2 times

donathon 1 year, 5 months ago

Join, Project, Project

upvoted 2 times

User_Mowgli 2 years, 2 months ago

Join, Extend, Project.

upvoted 1 times

danb67 2 years, 4 months ago

Correct Answer is 100% Join/Project/Project. This does not give error at all.

Why would we use extend here? Extend is for creating calculated columns and there is no requirement for this.

See https://www.examtopics.com/discussions/microsoft/view/60115-exam-sc-200-topic-1-question-17-discussion/

EmailAttachmentInfo
| where isnotempty (SHA256)
| join (DeviceFileEvents
| project FileName, SHA256)
on SHA256
| project Timestamp, NetworkMessageId, etc, etc

upvoted 2 times

Metasploit 2 years, 2 months ago

Please proof test before you answer. I receive the below errors when creating the hunting query on advanced hunting page with join,project,project. Why? because "Only the columns specified in the arguments are included in the result. Any other columns in the input are dropped." https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/projectoperator. For this current query to work, "DeviceName" and "DeviceID" need to be projected by the project within the join.

"Error message

'project' operator: Failed to resolve scalar expression named 'DeviceName'
How to resolve
Fix semantic errors in your query"

Correct answer is: Join, extend, project.
Extend can just append a column as well.
upvoted 13 times

gyaansastra 2 years ago
@Metasploit is absolutely correct.
upvoted 2 times

danb67 1 year, 2 months ago
Quite a few of the KQL queries in these dumps are wrong so I would not assume you are seeing the full query. I would be ready both both scenarios for the exam. Either the query above is in full and correct which means Metasploit is correcrt. Or the Query is missing the Projection of DeviceId and I am correct.
upvoted 1 times

danb67 1 year, 2 months ago
You recieve the error because the query is wrong and is missing DeviceName imo. So if the query itself is correct and not missing part of it then you are correct. If the query is wrong and is actally missing parts then I am correct.
upvoted 1 times

Shubham020 2 years, 9 months ago
The correct answer is join/extend/project
This case is little different from the case given in the link below
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your-devices

In this case inside join there is no DeviceName and DeviceID(in this queue), to join the column of this table we have to extend it.

I tested this in live environment with join, project, project, it gives an error. Join, extend, project just says no results found and if I change the sender email address I'm getting results.
upvoted 5 times

Question #8 *Topic 1*

You have the following advanced hunting query in Microsoft 365 Defender.

```
DeviceProcessEvents
| where Timestamp > ago (24h)
and InitiatingProcessFileName =~ 'runsll32.exe'
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
and FileName in~ ('schtasks.exe')
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine
```

You need to receive an alert when any process disables System Restore on a device managed by Microsoft Defender during the last 24 hours.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a detection rule.

B. Create a suppression rule.

C. Add | order by Timestamp to the query.

D. Replace DeviceProcessEvents with DeviceNetworkEvents.

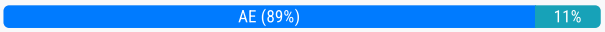
E. Add DeviceId and ReportId to the output of the query.

Suggested Answer: *AE*

Reference:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/custom-detection-rules

Community vote distribution



teehex Highly Voted 3 months, 1 week ago

Correct query is

DeviceProcessEvents
| where Timestamp > ago (24h)
//Pivoting for rundll32
| where InitiatingProcessFileName =~ 'rundll32.exe'
//Looking for empty command line
and InitiatingProcessCommandLine !contains " " and InitiatingProcessCommandLine != ""
//Looking for schtasks.exe as the created process
and FileName in~ ('schtasks.exe')
//Disabling system restore
and ProcessCommandLine has 'Change' and ProcessCommandLine has 'SystemRestore'
and ProcessCommandLine has 'disable'
| project Timestamp, AccountName, ProcessCommandLine, DeviceId, ReportId

Given answer is correct.
- Create detection rule
- Add ReportId and DeviceId to the output. Both fields are supported in DeviceProcessEvents table.(https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-deviceprocessevents-table?view=o365-worldwide)

The sample query can be found here https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-find-ransomware?view=o365-worldwide#turning-off-system-restore

upvoted 45 times

ArciOfficial Highly Voted 3 years, 5 months ago

Given answer is CORRECT:

According to the link below, DeviceID and ReportID are REQUIRED columns for any custom query.

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide#suppress-an-alert-and-create-a-new-suppression-rule

upvoted 8 times

im20batman 1 year ago

You mean this link

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide

upvoted 1 times

nk_exam Most Recent 1 month, 3 weeks ago

Given answers are correct

upvoted 1 times

Nikki0222 2 months, 1 week ago

Given answer is correct

Question #9 *Topic 1*

You are investigating a potential attack that deploys a new ransomware strain.
You have three custom device groups. The groups contain devices that store highly sensitive information.
You plan to perform automated actions on all devices.
You need to be able to temporarily group the machines to perform actions on the devices.
Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Assign a tag to the device group.

B. Add the device users to the admin role.

C. Add a tag to the machines.

D. Create a new device group that has a rank of 1.

E. Create a new admin role.

F. Create a new device group that has a rank of 4.

Suggested Answer: *ACD*
Reference:
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/4-manage-access

Community vote distribution
ACD (98%)

Metasploit Highly Voted 3 months, 2 weeks ago

Selected Answer: ACD

Setting the scene:
There are 3 device groups.
You want to take action on all devices. Meaning you want 1(One) Device group with all devices.

--> A: So you create this custom group(AllDeviceTempGroup) and add a Tag filter(RansomIRTag) to group devices into this device group.
You see that there are no devices in this group. Why? You have not tagged your devices yet.

--> B: You add the tag, RansomIRTag, to all devices.
You notice that your devices have not populated your new device group, AllDeviceTempGroup. Why?
In the details of the question, you are informed that these devices already have a group. Which means if your group is not promoted to highest rank, then the devices will choose their original group instead.

-->C: Promote AllDeviceTempGroup to highest rank.
upvoted 84 times

Nikki0222 2 months, 1 week ago
This answer is correct
upvoted 1 times

Wutan 1 year, 11 months ago
This is so well explained and in depth, thank you so much.
upvoted 3 times

DaraVasu 1 year, 10 months ago
Great explanation
upvoted 2 times

Metasploit 2 years, 2 months ago
Answer is ACD. My brain listed the answers in order of 1,2,3,a,b,c while I typed.
upvoted 7 times

Ken88 Highly Voted 2 years, 9 months ago

Selected Answer: ACD

Admin role is not required.
Given answer:ACD is correct
upvoted 9 times

chepeerick Most Recent 1 year, 2 months ago
Selected Answer: ACD
correct
upvoted 1 times

Kanguro007 1 year, 12 months ago
https://www.drware.com/how-to-use-tagging-effectively-in-microsoft-defender-for-endpoint-part-1/
upvoted 1 times

Hamatew 1 year, 12 months ago
Thanks for the explanation. Probably i skipped some aspect while studying, i have this question, Assuming i have 100s of devices how can i tag all at once. I need to give RansomIRtag to 100 devices, will i start adding one by one?
upvoted 1 times

Tx4free 2 years, 10 months ago
Selected Answer: ACD
Best answer
upvoted 2 times

Tx4free 2 years, 10 months ago
Selected Answer: ACE
Best answer
upvoted 2 times

liberty123 2 years, 10 months ago
Selected Answer: ACD
ACD correct
upvoted 3 times

stromnessian 2 years, 11 months ago
ACD. No admin role is required in the scenario given (automated), and obviously the rank needs to be 1, not 4 for the group that contains the tagged devices.
upvoted 2 times

RandomNickname 2 years, 12 months ago
Think given answer is correct, but not 100%.
C: Tag all machines (as requested), to ensure they can be grouped temporarily.
A: Add the tagged machines to the group to be able to perform automated actions on all.
D: Ensure has rank of 1, so given tagged machines are added, in case of devices match other groups.
upvoted 7 times

Mastersin 3 years, 1 month ago
BDE
https://docs.microsoft.com/en-us/learn/modules/deploy-microsoft-defender-for-endpoints-environment/6-configure-device-groups
upvoted 3 times

Nail 3 years, 1 month ago
As far as I can tell, you can't assign tag to a device group, only devices. And why would you need to assign tags to both devices and device groups? So I think the answer must be CDE.
upvoted 2 times

Nail 3 years ago
On second thought, I think this answer is correct, ACD. You would add the tag to the devices, then assign the tag to the device group to create a group based on the tags, and then rank it #1 so it takes precedence over the other groups.
upvoted 11 times

kakakayayaya 3 years, 2 months ago
Correct answer but reference is not so useful.
upvoted 1 times

Metasploit 2 years, 2 months ago
Watch the video in the reference. The video explains this answer 100%. ACD.

upvoted 1 times

Question #10 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Entity tags, you add the accounts as Honeytoken accounts.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution
A (100%)

kwach Highly Voted 3 years, 8 months ago
correct answer is A:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts
upvoted 12 times

Tx4free Highly Voted 2 years, 10 months ago
Selected Answer: A
Best answer
upvoted 6 times

Nikki0222 Most Recent 2 months, 1 week ago
Yes , correct
upvoted 2 times

chepeerick 1 year, 2 months ago
Yes, correct
upvoted 1 times

Task 3 years, 7 months ago
Correct answer
upvoted 3 times

Question #11 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: From Azure AD Identity Protection, you configure the sign-in risk policy.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution
B (100%)

Metasploit Highly Voted 2 years, 2 months ago
Selected Answer: B
Honeytoken entities are used as traps for malicious actors. Any authentication associated with these honeytoken entities triggers an alert.

Settings>Identities>Entity tags>Honey Token> Add Users or Devices
upvoted 9 times

Task Highly Voted 3 years, 7 months ago
Correct
upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago
No, correct
upvoted 2 times

chepeerick 1 year, 2 months ago
no, this is correct
upvoted 1 times

Tx4free 2 years, 10 months ago
Selected Answer: B
Correct answer
upvoted 4 times

Question #12 *Topic 1*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: You add the accounts to an Active Directory group and add the group as a Sensitive group.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution
B (100%)

stromnessian Highly Voted 2 years, 11 months ago
Selected Answer: B
This is what honeytoken accounts are meant for (i.e. dormant accounts that generate alerts if accessed). Sensitivity tags are meant for active users and groups.
upvoted 11 times

Nikki0222 Most Recent 2 months, 1 week ago
No, correct
upvoted 1 times

cloudster998 3 months, 2 weeks ago
Manually tagging entities

You can also manually tag entities as sensitive or honeytoken accounts. If you manually tag additional users or groups, such as board members, company executives, and sales directors, Defender for Identity will consider them sensitive.
upvoted 3 times

chepeerick 1 year, 2 months ago
Correct B
upvoted 1 times

Taisuke 2 years, 4 months ago
Selected Answer: B
Best answer.
upvoted 1 times

Tx4free 2 years, 10 months ago
Selected Answer: B
Best answer
upvoted 4 times

sunnybb269 2 years, 10 months ago
Selected Answer: B
Correct answer
upvoted 3 times

PLhiro 2 years, 11 months ago
Why B?
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

upvoted 1 times

Metasploit 2 years, 2 months ago

B = No

The URL you posted is the answer to your question. Lookup HoneyToken Accounts. :)

"... you need to configure several accounts for attackers to exploit."

upvoted 1 times

Task 3 years, 7 months ago

Correct

upvoted 2 times

Question #13 *Topic 1*

You implement Safe Attachments policies in Microsoft Defender for Office 365.
Users report that email messages containing attachments take longer than expected to be received.
You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.
What should you configure in the Safe Attachments policies?

A. Dynamic Delivery

B. Replace

C. Block and Enable redirect

D. Monitor and Enable redirect

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

Community vote distribution
A (100%)

jasonfmj Highly Voted 3 years, 4 months ago
Correct
Dynamic Delivery Delivers messages immediately, but replaces attachments with placeholders until Safe Attachments scanning is complete.
For details, see the Dynamic Delivery in Safe Attachments policies section later in this article.

Avoid message delays while protecting recipients from malicious files.
Enable recipients to preview attachments in safe mode while scanning is taking place.
upvoted 42 times

ifaiyazhossain Most Recent 1 month, 1 week ago
Selected Answer: A
A is the right answer.
upvoted 1 times

Nikki0222 2 months, 1 week ago
Dynamic delivery , correct
upvoted 1 times

Apocalypse03 3 months, 1 week ago
Selected Answer: A
To reduce the amount of time it takes to deliver email messages that contain attachments while still scanning the attachments for malware and blocking any messages that contain malware, you should configure the Safe Attachments policies to use the "Dynamic Delivery" option.

Dynamic Delivery is a feature in Microsoft Defender for Office 365 that allows you to optimize the delivery of email messages containing attachments by scanning the attachments for malware before they are delivered to the recipient's mailbox. This allows you to quickly deliver messages that are deemed safe while still protecting against malware threats.

To configure the Safe Attachments policies to use Dynamic Delivery, you can go to the Mail flow > Safe attachments policies page in the Microsoft 365 admin center and select the "Dynamic Delivery" option for each policy.

Options B, C, and D are not relevant to reducing the delivery time for email messages with attachments and do not provide the same level of protection against malware threats as Dynamic Delivery.
upvoted 4 times

Ramye 10 months, 3 weeks ago
Selected Answer: A
If you're interested to set up the Safe Attachment / Dynamic Delivery here are the steps
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-policies-configure?view=o365-worldwide

upvoted 1 times

chepeerick 1 year, 2 months ago

Selected Answer: A

Correct, A

upvoted 1 times

gepoy01 1 year, 7 months ago

Dynamic Delivery

upvoted 2 times

TeeKay_From_the_South 1 year, 7 months ago

Dynamic Delivery. A is the correct answer.

upvoted 1 times

kovora 2 years, 2 months ago

Correct Answer is A

upvoted 1 times

bluegeek 2 years, 4 months ago

Selected Answer: A

Correct answer

upvoted 2 times

eveyklel 2 years, 6 months ago

Correct

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide#dynamic-delivery-in-safe-attachments-policies

upvoted 1 times

M0809 2 years, 8 months ago

Dynamic Delivery Correct!

upvoted 2 times

TomG 2 years, 9 months ago

Selected Answer: A

Correct Answer is A

upvoted 3 times

Tx4free 2 years, 10 months ago

Selected Answer: A

Correct answer

upvoted 3 times

stromnessian 2 years, 11 months ago

Selected Answer: A

Badly worded question but that's all part of the MS exam experience.

upvoted 4 times

Question #14 *Topic 1*

HOTSPOT -

You are informed of an increase in malicious email being received by users.

You need to create an advanced hunting query in Microsoft 365 Defender to identify whether the accounts of the email recipients were compromised. The query must return the most recent 20 sign-ins performed by the recipients within an hour of receiving the known malicious email.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
let MaliciousEmails = [ ▼ EmailAttachementInfo / EmailEvents / IdentityLogonEvents ]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [ ▼ EmailAttachementInfo / EmailEvents / IdentityLogonEvents ]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [ ▼ select 20 / take 20 / top 20 ]
```

Suggested Answer:

Answer Area

```
let MaliciousEmails = [ ▼ EmailAttachementInfo / EmailEvents / IdentityLogonEvents ]
| where MalwareFilterVerdict == "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName =
tostring(split (RecipientEmailAddress, "@") [0]);

MaliciousEmails
| join ( [ ▼ EmailAttachementInfo / EmailEvents / IdentityLogonEvents ]
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
| where (LogonTime - TimeEmail) between (0min.. 60min)
| [ ▼ select 20 / take 20 / top 20 ]
```

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

pedromonteirozikado Highly Voted 3 months, 2 weeks ago

The first answer "EmailEvents" is right because only EmailEvents table have the Subject column, but both EmailEvents and EmailAttachmentInfo have the ThreatType table (old MalwareFilterVerdict).

The second answer: IdentityLogonEvents, is right, because is the only table that have identity objects related.

The third answer: take 20, according to MS "here is no guarantee which records are returned, unless the source data is sorted.", "take and limit are synonyms".
I tested by myself, and the only query that return the latest results was: top 20 by Timestamp, because only "top 20" didn't work.
upvoted 41 times

Tuitor01 4 weeks ago
it would be top 20 by some table. So answer is de facto take 20 indeed.
upvoted 1 times

jasonfmj Highly Voted 3 months, 1 week ago
//Define new table for malicious emails
let MaliciousEmails=EmailEvents
//List emails detected as malware, getting only pertinent columns
| where ThreatTypes has "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(split(RecipientEmailAddress, "@")[0]);
MaliciousEmails
| join (
//Merge malicious emails with logon events to find logons by recipients
IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
//Check only logons within 30 minutes of receipt of an email
| where (LogonTime - TimeEmail) between (0min.. 30min)
| take 10
upvoted 11 times

Thezuland1098 Most Recent 2 months, 3 weeks ago
Why use take and not top in this scenario?
The query in your case doesn't explicitly mention sorting the logon events by a specific column (e.g., timestamp). It simply limits the results to a certain number, so take is appropriate here.
If you wanted the 20 most recent logon events, you could use top 20 by LogonTime, which ensures that you are retrieving the most recent events sorted by time.
upvoted 1 times

talosDevbot 3 months ago
The output of KQL queries are sorted by descending order of the first column.
So take 20 works out here
upvoted 2 times

oreoale 3 months, 1 week ago
The answer is correct. Here is an example: https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#review-logon-attempts-after-receipt-of-malicious-emails

//Define new table for malicious emails
let MaliciousEmails=EmailEvents
//List emails detected as malware, getting only pertinent columns
| where ThreatTypes has "Malware"
| project TimeEmail = Timestamp, Subject, SenderFromAddress, AccountName = tostring(split(RecipientEmailAddress, "@")[0]);
MaliciousEmails
| join (
//Merge malicious emails with logon events to find logons by recipients
IdentityLogonEvents
| project LogonTime = Timestamp, AccountName, DeviceName
) on AccountName
//Check only logons within 30 minutes of receipt of an email
| where (LogonTime - TimeEmail) between (0min.. 30min)
| take 10
upvoted 4 times

g_man_rap 4 months, 1 week ago

EmailEvents is used to filter out the malicious emails.
IdentityLogonEvents is used to check for sign-ins by those who received the malicious emails.
top 20 ensures that only the most recent 20 sign-in events are returned, which matches the requirement of the task.
upvoted 2 times

emartiy 7 months ago
EmailEvents, IdentityLogonEvents, take 20 because take operator in kql returns most recents records in event table..
upvoted 2 times

chepeerick 1 year, 2 months ago
correct, There is no guarantee which records are returned, unless the source data is sorted. If the data is sorted, then the top values will be returned.
upvoted 1 times

tatendazw 1 year, 7 months ago
EmailEvents, IdentityLogonEvents, take 20
upvoted 3 times

Ramkid 1 year, 11 months ago
Given Answer is correct, check the following page that has this query under the section "Review logon attempts after receipt of malicious emails"
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#review-logon-attempts-after-receipt-of-malicious-emails
upvoted 4 times

danb67 1 year, 2 months ago
This query is wrong and Microsoft need to fix this page. Take 10 will never give you the most recent logins. It gives a random 10 results and is different each time you run it.
upvoted 1 times

danb67 1 year, 2 months ago
ignore this wrong question
upvoted 1 times

Fukacz 2 years, 3 months ago
Correct. Take 20 is equal to top 20 by timestamp here.
upvoted 4 times

danb67 1 year, 2 months ago
why? Would it not need by Timestamp at the end
upvoted 1 times

its_me_Nat 2 years, 9 months ago
take 20 is correct if you need to select most recent logins.
upvoted 1 times

jetodo7615 2 years, 12 months ago
Answer is correct, but the solution is incomplete, as the results needs to be sorted before "take" command (most recent logons). "Top" is not an option here as it needs "by" argument to be correct.
upvoted 6 times

RandomNickname 2 years, 12 months ago
Believe given answer to be correct
upvoted 4 times

ReginaldoBarreto 3 years, 1 month ago
take operator
There is no guarantee which records are returned, unless the source data is sorted.
---
for this query the correct would not use top ?
Since they ask for recent records
upvoted 3 times

pedromonteirozikado 2 years, 11 months ago
Yes, | top 20 by Timestamp
upvoted 3 times

zedricko 3 years, 1 month ago

I guess so top should be used in this case

upvoted 2 times

j888 2 years, 8 months ago

As per 'Pedromonteirozikado' it is missing "by Timestamp" statement. So the given answer is correct.

upvoted 1 times

Question #15 *Topic 1*

You receive a security bulletin about a potential attack that uses an image file.
You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.
Which indicator type should you use?

A. a URL/domain indicator that has Action set to Alert only

B. a URL/domain indicator that has Action set to Alert and block

C. a file hash indicator that has Action set to Alert and block

D. a certificate indicator that has Action set to Alert and block

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

Community vote distribution
C (100%)

HSBNZ Highly Voted 3 months, 1 week ago
The correct answer it seems like, as steps for to Create an indicator for files from the settings page
1. In the navigation pane, select Settings > Endpoints > Indicators (under Rules).

2. Select the File hashes tab.

3. Select Add indicator.

4. Specify the following details:

5. Indicator - Specify the entity details and define the expiration of the indicator.
* Action - Specify the action to be taken and provide a description.
* Scope - Define the scope of the device group.
* Review the details in the Summary tab, then select Save.
upvoted 25 times

Tx4free Highly Voted 2 years, 10 months ago
Selected Answer: C
Correct answer
upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago
C correct answer
upvoted 1 times

Makawai 1 year, 2 months ago
C is the right answer
upvoted 1 times

chepeerick 1 year, 2 months ago
C, correct
upvoted 1 times

kamun1st 2 years ago
Selected Answer: C
correct
upvoted 3 times

Question #16 *Topic 1*

Your company deploys the following services:
✑ Microsoft Defender for Identity
✑ Microsoft Defender for Endpoint
✑ Microsoft Defender for Office 365
You need to provide a security analyst with the ability to use the Microsoft 365 security center. The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint. The solution must use the principle of least privilege.
Which two roles should assign to the analyst? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. the Compliance Data Administrator in Azure Active Directory (Azure AD)

B. the Active remediation actions role in Microsoft Defender for Endpoint

C. the Security Administrator role in Azure Active Directory (Azure AD)

D. the Security Reader role in Azure Active Directory (Azure AD)

Suggested Answer: *BD*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/rbac?view=o365-worldwide

Community vote distribution
BD (81%) BC (19%)

PhilAus Highly Voted 3 months, 2 weeks ago
Provided answer B and D is correct.
Security Reader - can access M365 Security Center.
Active Remediation Actions role in Defender for Endpoint meets need to 'approve and reject' pending actions with respect to Defender For Endpoint.
Requirement does not need more.
upvoted 25 times

Metasploit Highly Voted 3 months, 1 week ago
Selected Answer: BD
This question is tricky.

If you follow the question directly, they are not asking either/or. They want you to assign 2 roles to the Analyst each being half of the entire solution. Using least privileges the answer should be BD.

Not A = Too many other permissions not needed.
B = the Active remediation actions role in Microsoft Defender for Endpoint is enough for the task to be done of approving/rejecting pending actions.
Not C = Would be able to fulfill both B and D and (more), not least privilege.
D = Quite redundant, but gives reader roles read access to the portal up until RBAC is turned on the defender permissions. Least Privilege.
¯_(□)_/¯
upvoted 9 times

danb67 1 year, 2 months ago
B is not enough to approve/reject email related pending actions though is it? https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-action-center?view=o365-worldwide So a user assigned only the active remediation roles will not be able to approve or reject email related pending actions. So answer is BC
upvoted 2 times

WORKTRAIN 8 months, 3 weeks ago
You are right. But the question states "The analyst must be able to approve and reject pending actions generated by Microsoft Defender for Endpoint", so we don't have to take in consideration the other defender components.
B and D are the correct answers.
upvoted 1 times

Nikki0222 Most Recent 2 months, 1 week ago

BD correct

upvoted 2 times

HOTSPOT -

You have a Microsoft 365 E5 subscription that uses Microsoft Defender and an Azure subscription that uses Azure Sentinel.

You need to identify all the devices that contain files in emails sent by a known malicious email sender. The query will be based on the match of the SHA256 hash.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256)

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- DeviceId
- RecipientEmailAddress
- SenderFromAddress
- SHA256

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Suggested Answer:

Answer Area

```
EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
where isnotempty [ ▼ ]
```

- (DeviceId)
- (RecipientEmailAddress)
- (SenderFromAddress)
- (SHA256) ✓

```
| join (
DeviceFileEvents
| project FileName, SHA256
) on [ ▼ ]
```

- DeviceId
- RecipientEmailAddress
- SenderFromAddress
- SHA256 ✓

```
| project Timestamp, FileName, SHA256, DeviceName, DeviceId,
NetworkMessageId, SenderFromAddress, RecipientEmailAddress
```

Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

HSBNZ Highly Voted 3 years, 4 months ago

Correct answer as per the link, EmailAttachmentInfo
| where SenderFromAddress =~ "MaliciousSender@example.com"
//Get emails with attachments identified by a SHA-256
| where isnotempty(SHA256)
| join (
//Check devices for any activity involving the attachments
DeviceFileEvents
| project FileName, SHA256, DeviceName, DeviceId
) on SHA256
| project Timestamp, FileName , SHA256, DeviceName, DeviceId, NetworkMessageId, SenderFromAddress, RecipientEmailAddress
upvoted 39 times

Metasploit 2 years, 2 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your-devices
upvoted 4 times

Ramye 10 months, 1 week ago

when I run this query given above by copy / paste in Microsoft Defender Advanced Hunting, it gives the below error:
Semantic error
Error message
'project' operator: Failed to resolve table or column expression named 'DeviceFileEvents'
How to resolve
Fix semantic errors in your query

Note: not too savvy on the query builder yet but learning. How do I fix this semantic error? Thx
upvoted 1 times

Apocalypse03 Highly Voted 2 years ago

Answer is correct.

Here is a brief explanation of how this query works:

The where clause filters the EmailAttachmentInfo table to only include attachments sent by the specified sender and that have a non-empty SHA256 hash value. This effectively filters the results to only include attachments from the specified sender and that have a known hash value.

The join operator combines the results of the previous step with the results of a second query that selects the DeviceFileEvent table and projects the FileName, SHA256, DeviceName, and DeviceId fields. This effectively creates a join between the two tables based on the SHA256 field, linking the attachments with file events on devices.

The project operator selects the desired fields from the joined results and includes them in the final output.

This query will work in both Microsoft Defender and Azure Sentinel, as it is a valid advanced hunting query in both platforms.
upvoted 33 times

Nikki0222 Most Recent 2 months, 1 week ago

Correct
upvoted 2 times

chepeerick 1 year, 2 months ago

Correct
upvoted 1 times

trashbox 1 year, 3 months ago

The answer is correct. SHA256 and SHA256.

Check if files from a known malicious sender are on your devices

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#check-if-files-from-a-known-malicious-sender-are-on-your-devices

upvoted 2 times

Question #18 *Topic 1*

You need to configure Microsoft Cloud App Security to generate alerts and trigger remediation actions in response to external sharing of confidential files.
Which two actions should you perform in the Cloud App Security portal? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant.

B. Select Investigate files, and then filter App to Office 365.

C. Select Investigate files, and then select New policy from search.

D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings.

E. From Settings, select Information Protection, select Files, and then enable file monitoring.

F. Select Investigate files, and then filter File Type to Document.

Suggested Answer: *DE*
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/tutorial-dlp https://docs.microsoft.com/en-us/cloud-app-security/azip-integration

Community vote distribution
DE (75%) CE (19%) 4%

liberty123 Highly Voted 3 months, 2 weeks ago
Selected Answer: DE
DE is correct , I have seen these configurations in Microsoft Learning video:
https://www.microsoft.com/en-us/videoplayer/embed/RE4CMYG?postJsllMsg=true
upvoted 25 times

danituga 7 months ago
The timestamp in the video is 08:20
upvoted 2 times

Nikki0222 Most Recent 2 months, 1 week ago
DE correct
upvoted 3 times

talosDevbot 2 months, 4 weeks ago
Selected Answer: DE
DE
upvoted 2 times

Adam7777 3 months ago
A, D

A: focuses on ensuring that only files classified with Azure Information Protection (AIP) labels are scanned, which is crucial for identifying sensitive or confidential files. By limiting the scope to AIP-classified files, you ensure that the system focuses on files requiring protection. This ensures the system scans the right files, adhering to the principle of least privilege, while identifying confidential files for monitoring and action.

D: This automates the scanning of new files for AIP labels, ensuring ongoing protection of sensitive files.
upvoted 1 times

g_man_rap 4 months, 1 week ago
Selected Answer: CD
Select Investigate files, and then select New policy from search (Option C). This allows you to create a new policy based on your search criteria, which can include conditions for external sharing of confidential files.
From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure

Information Protection classification labels and content inspection warnings (Option D). This ensures that new files are automatically scanned for classification labels and content inspection warnings, which can trigger alerts and remediation actions.

upvoted 1 times

e072f83 7 months, 3 weeks ago

C + D

D to enalble AIP

C to scan the existing files.

upvoted 1 times

czaaa 11 months ago

Microsoft Cloud App Security is now known as **Microsoft Defender for Cloud Apps**

This name change was part of a broader rebranding effort by Microsoft to consolidate its security and compliance services under the Microsoft Defender brand.

upvoted 1 times

zoodata 1 year ago

Selected Answer: CE

C and E

upvoted 1 times

chepeerick 1 year, 2 months ago

Selected Answer: DE

DE, correct

upvoted 2 times

donathon 1 year, 4 months ago

Selected Answer: DE

Make sense

upvoted 1 times

tatendazw 1 year, 7 months ago

Correct, go to M365 Defender settings, Cloud apps, Info Protection, MS Info Protection - "Auto scan new files .." and then Save and got to Files "File monitoring" Save. https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration#enable-microsoft-purview-information-protection

upvoted 3 times

Holii 1 year, 8 months ago

Once again based on your intuition due to Microsoft's vague answer choices.

Based on the following: "generate alerts and [[trigger remediation actions]]"
The answer would be CE.
D would label the files with the appropriate Sensitive Data Classification Label and can block the file from being sent externally, but that does not 'trigger a remediation option' in response to an alert via MCAS. That's done within MPIP Compliance portal.

If we're discussing how to remediate an alert from MCAS, you would use "Send alerts to Microsoft Power Automate" in an MCAS Policy and automate the remediation there.

upvoted 3 times

palito1980 1 year, 11 months ago

Selected Answer: DE

D:
Settings>Information Protection>Microsoft Information Protection>Automatically scan new files for Microsoft Information Protection classification labels and content inspection warnings.

E:
Settings>Information Protection>Files>Enable file monitoring.

upvoted 4 times

Locian 1 year, 11 months ago

D and E to achieve both outcomes

upvoted 1 times

jrjrjrchlv 1 year, 11 months ago

Selected Answer: DE

D. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings. This will enable Cloud App Security to automatically scan new files for Azure Information Protection classification labels and content inspection warnings, which can be used to detect and protect confidential files.

E. From Settings, select Information Protection, select Files, and then enable file monitoring. This will enable Cloud App Security to monitor files for external sharing and other activities, and to generate alerts and trigger remediation actions in response to potential threats or policy violations.

upvoted 3 times

Tagwa 1 year, 12 months ago

DE tested

upvoted 1 times

nazgul250 1 year, 12 months ago

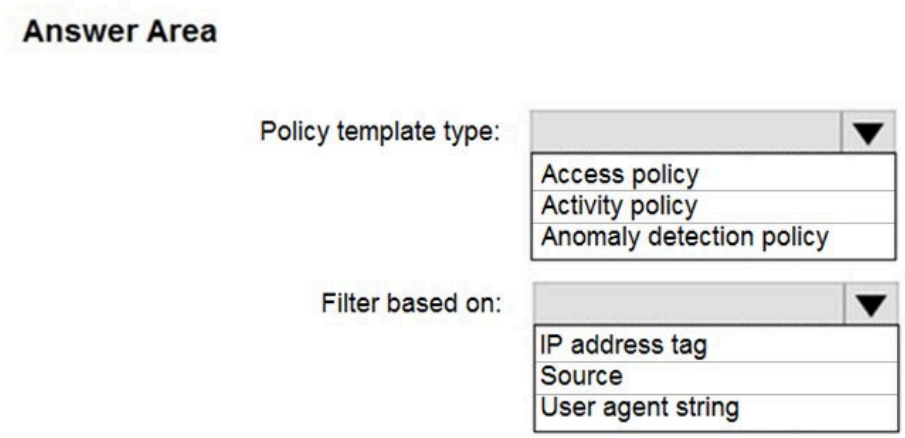
Selected Answer: CE

C and E

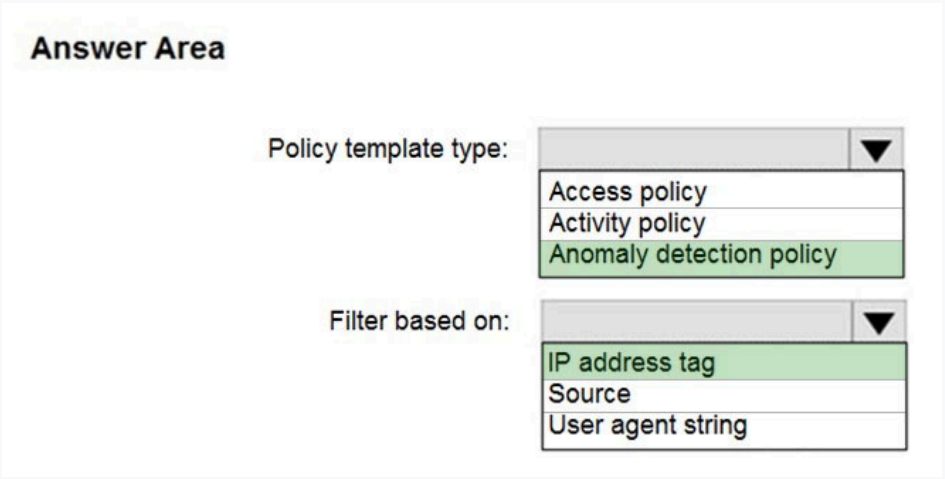
upvoted 2 times

Question #19 *Topic 1*

HOTSPOT -
You purchase a Microsoft 365 subscription.
You plan to configure Microsoft Cloud App Security.
You need to create a custom template-based policy that detects connections to Microsoft 365 apps that originate from a botnet network.
What should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:



Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/cloud-app-security/anomaly-detection-policy

Efficia Highly Voted 3 years, 1 month ago
Policy template type: Activity Policy
Filter based on: IP address tag

Tested on the MCAS portal. When you select Activity policy only you get to filter from IP address.
upvoted 60 times

Nikki0222 2 months, 1 week ago
This is correct
upvoted 1 times

AnonymousJhb 2 years, 9 months ago
its NOT Activity Policy, as per https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

anomaly-detection-policy:
Activity from suspicious IP addresses:
This detection identifies that users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses are involved in malicious activities, such as performing password spray, Botnet C&C, and may indicate compromised account. This detection uses

a machine-learning algorithm that reduces "false positives", such as mis-tagged IP addresses that are widely used by users in the organization.
upvoted 5 times

MNC 2 years, 4 months ago
anomaly detection policy doesn't exists
upvoted 6 times

Metasploit 2 years, 2 months ago
It actually does, it is called cloud discovery anomaly detection policy; but not suitable for this question as you cannot filter by any of the mentioned filters in the question.
upvoted 8 times

Holii 1 year, 8 months ago
There are Anomaly Detection Policies as pre-built templates to use UEBA specifically for suspicious IP Address behavior (Botnet C&C)
BUT it does not have a filter, only a source.

So, correct. A custom policy with a filter would have to come from an Activity Policy, albeit redundant.
upvoted 6 times

Metasploit 2 years, 2 months ago
Agreeing with this answer, just tested it as well.

Activity Policy Type.
Filter: IP address> Tag >equals >Botnet

Access Policy: Does not seem to have a filter section.
Cloud Discovery Anomaly Detection Policy: Does not meet any of the options to filter here.
upvoted 11 times

stromnessian Highly Voted 2 years, 11 months ago
Control -> Templates -> Logon from a risky IP address -> Create (activity) policy -> Activities matching any of the following -> IP address | Category | equals | Risky.
Answer is Activity policy, IP address.
For anyone who thinks it's "Anomaly detection policy", state the exact steps please and say why the steps above are wrong.
upvoted 16 times

vijeet 2 years, 9 months ago
Activity from suspicious IP addresses
This detection identifies that users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses are involved in malicious activities, such as performing password spray, Botnet C&C, and may indicate compromised account. This detection uses a machine-learning algorithm that reduces "false positives", such as mis-tagged IP addresses that are widely used by users in the organization
upvoted 1 times

7d801bf Most Recent 6 months ago
Anomaly detection policy and Ip address Tag
upvoted 1 times

smanzana 1 year, 1 month ago
Policy template type: Activity Policy
Filter based on: IP address tag
upvoted 1 times

prkhrkmr 1 year, 3 months ago
IP Address Tag is available in both Access and Activity policies.
Check it out:
https://security.microsoft.com/cloudapps/policy/activity/create
https://security.microsoft.com/cloudapps/policy/access/create
There are no customizable policies under "Anomaly Detection Policy" to narrow down just to Botnet IPs. The built-in Anomaly Detection Policy called "Activity from suspicious IP addresses" is not customizable.
upvoted 2 times

donathon 1 year, 4 months ago

So I physically tested and I found the filter only in activity policy template

upvoted 2 times

Big_Billy_Gates 1 year, 5 months ago

Why are so many people saying Activity Policy? It's wrong.

'Anomaly detection policy' and 'IP address tag' *are* the correct answers.

The question asks for a policy to detect connections from a Botnet related IP address, this is done using the 'Activity from suspicious IP addresses' anomaly detection policy.

The list of available anomaly detection policies can be found here: https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

upvoted 2 times

danlo 1 year, 1 month ago

You can't filter on "Activity from suspicious IP addresses" that's the problem

upvoted 1 times

TiredofTesting 2 years ago

Looks like it is leaning more for 1) Activity Policy and 2) IP address tag.

While I want to say Anomaly detection policy for the 1st answer, when I tested it in the lab, it came back with no templates under that category. While Activity Policy came back with a bunch related to logins from risky IP, potential ransomware activity, etc.

upvoted 4 times

Apocalypse03 2 years ago

Policy template type: Activity Policy
Filter based on: IP address tag

Activity policies in Cloud App Security are designed to detect specific types of activity in the cloud apps that are being monitored. The "Botnet Network Activity" policy template is a pre-defined policy that is designed to detect and alert on suspicious activity from botnet networks. This policy uses a combination of machine learning and threat intelligence to identify botnet network activity, such as attempts to compromise accounts or access sensitive data.

"Access Policy," is a type of policy that is used to control access to specific cloud apps or resources based on specified conditions, such as the location of the user or the type of device being used.

"Anomaly detection policy," is a type of policy that is used to detect anomalies in the activity of specific cloud apps or resources based on specified conditions, such as the number of times a resource is accessed or the type of activity that is being performed. Neither of these options is suitable for detecting connections to Microsoft 365 apps that originate from a botnet network.

upvoted 8 times

Holii 1 year, 8 months ago

There is no "Botnet Network Activity" pre-defined policy template default...
and "This policy uses a combination of machine learning and threat intelligence to identify botnet network activity" sounds like Anomaly Detection Policy...

Anomaly Detection Policy uses UEBA to conduct machine learning on user analytics to predict whether IP addresses are being conducted suspiciously or coming from a potential Botnet C&C.
Source: https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

Now, the question strictly asks for a FILTER to be applied to "IP Addresses"
Cloud Discovery Anomaly Detection Policies "Apply to" IP addresses or Users, they do not "Filter" for them...so due to the nature of the grammar of this question I would say Activity Policy, since they are more open to creating a CUSTOM policy based on a TEMPLATE and capable of applying a FILTER for IP addresses.

But if you're asking which one is the 'technically' correct one now that UEBA is fleshed out in the Microsoft ecosystem, it is 100% Anomaly Detection Policy.

upvoted 1 times

Ahmed_Root 2 years ago

https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy it is anomaly detection policy and the other "suspicious ip address" actually which is not here. but you can find the response in the link.

"

Activity from suspicious IP addresses:

These IP addresses are involved in malicious activities, such as performing password spray, Botnet C&C, and may indicate compromised account...

"

upvoted 1 times

Atun23 2 years, 2 months ago

I'm really confused on this one

For anomaly detections says "such as mis-tagged IP addresses" so it doesn't use IPs tagged as malicious, and the filter used according to scenario in filter can only be IP address tag.

If we were to choose anomaly detections, the filter should be source, as it originates from a botnet.

Activity from suspicious IP addresses

This detection identifies that users were active from an IP address identified as risky by Microsoft Threat Intelligence. These IP addresses are involved in malicious activities, such as performing password spray, Botnet C&C, and may indicate compromised account. This detection uses a machine-learning algorithm that reduces "false positives", such as mis-tagged IP addresses that are widely used by users in the organization.

https://docs.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

upvoted 1 times

amsioso 2 years, 4 months ago

https://docs.microsoft.com/en-us/defender-cloud-apps/control-cloud-apps-with-policies

upvoted 3 times

Ahmed_Root 2 years ago

yes this link is helpful also this one https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

it is clear that the first response is "anomaly detection policy" but there is not "ip add tag" filter in it" there is "risky ip address" and such filters.

upvoted 2 times

de_cs_bacsi 2 years, 4 months ago

There is an exact filter type what is needed under the creation of "Activity policy":

"Select a filter --> IP Address --> Select a filter --> Tag --> Select IP address tag --> Botnet"

And there is no "Anomaly policy" after pushing the "Create policy" button so all the Anomaly Policies are built-in and not custom ones.

Thus:

Policy template type: Activity Policy

Filter based on: IP address tag

upvoted 6 times

Whatsamattr81 2 years, 4 months ago

Also, when creating a policy based on the anomaly template, none of the options in the second part of the question are valid options.

upvoted 1 times

Whatsamattr81 2 years, 4 months ago

I think the answer is in the word 'custom'... The anomaly policies are just built in pols that have no actions associated. An activity policy can be used to the same effect, IP Tag and IP Category can be used. You also need to scope the policy to M365 apps - can you do that on anomaly detection ?

upvoted 2 times

danb67 1 year, 2 months ago

Thank you I thought I was going mad. Custom is the word everyone is missing here. Activity Policies allow you to choose 'No Template' which is a custom template. You do not get the option to choose or customise ' a template' in an access policy. You choose a category. It is asking us to detect the activity. Activity Policy is the correct answer.

upvoted 2 times

LotusBeta 2 years, 5 months ago

The question says "You need to create a custom template-based policy"...only Anomaly detection policy has template with which we can create policy. Answer "Anomaly detection policy" and "IP address tag" are correct.
upvoted 3 times

yoton 1 year, 11 months ago
Activity Policy can also create custom templates.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#review-logon-attempts-after-receipt-of-malicious-emails
upvoted 1 times

Joshing 2 years, 5 months ago
The correct answer has to be the following.

Policy template type: Activity Policy
Filter based on: IP address tag

Reason being that you cannot create an anomaly detection policy as it's a built-in policy. Also, you cannot filter the policy based on IP address tags either. Activity Policy and IP address tag has to be the correct selection.

If it asked for you to ensure that activity from Botnets were alerted on and it was to be filtered for specific users then yes this policy could be edited to suit that but currently as it stands you cannot create this policy or filter by IP tags.
upvoted 6 times

Question #20 *Topic 1*

Your company has a single office in Istanbul and a Microsoft 365 subscription.
The company plans to use conditional access policies to enforce multi-factor authentication (MFA).
You need to enforce MFA for all users who work remotely.
What should you include in the solution?

A. a fraud alert

B. a user risk policy

C. a named location

D. a sign-in user policy

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

Community vote distribution
C (100%)

Startkabels Highly Voted 3 years, 2 months ago
Named location so you can enforce MFA except for the named location, thus forcing it for everyone who works remotely
upvoted 22 times

Efficia Highly Voted 3 years, 1 month ago
Selected Answer: C
Named locations can be defined by IPv4/IPv6 address ranges or by countries.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#named-locations
upvoted 12 times

Nikki0222 Most Recent 2 months, 1 week ago
C is correct
upvoted 1 times

smanzana 1 year, 1 month ago
Named location
upvoted 1 times

chepeerick 1 year, 2 months ago
Selected Answer: C
Correct, the C
upvoted 1 times

Sango 2 years, 5 months ago
The key here is "all users who work remotely." Only a named location can be used to define a CA rule to allow MFA for everyone except a trusted location like the office's internal IP ranges.
upvoted 4 times

xbonex99 2 years, 5 months ago
C with New reference
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa
upvoted 3 times

Tx4free 2 years, 10 months ago
Selected Answer: C
Best choice
upvoted 3 times

casti 2 years, 11 months ago
Selected Answer: C
Correct
upvoted 4 times

zaqwsx 3 years, 2 months ago

correct

upvoted 3 times

Eltooth 3 years, 2 months ago

Correct - named location.

upvoted 3 times

Question #21 *Topic 1*

You are configuring Microsoft Cloud App Security.
You have a custom threat detection policy based on the IP address ranges of your company's United States-based offices.
You receive many alerts related to impossible travel and sign-ins from risky IP addresses.
You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.
You need to prevent alerts for legitimate sign-ins from known locations.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Configure automatic data enrichment.

B. Add the IP addresses to the corporate address range category.

C. Increase the sensitivity level of the impossible travel anomaly detection policy.

D. Add the IP addresses to the other address range category and add a tag.

E. Create an activity policy that has an exclusion for the IP addresses.

Suggested Answer: *AD*

Community vote distribution

JohnAvlakiotis Highly Voted 3 years, 3 months ago
This answer looks wrong and since there is no reference link to support it I challenge it. To me the correct answer is B,E.
upvoted 40 times

JohnAvlakiotis 3 years, 2 months ago
Apologies, the answer provided is correct. I just know checked the site myself and the options exist, you add the IP address range and a tag and then you check to override the data enrichment by providing a location that goes along with that IP range.

So, A & D stand correct.
upvoted 52 times

BtwIdonno 2 months, 1 week ago
Do you mean A & B are the right options?
upvoted 2 times

Neela 2 years, 9 months ago
https://docs.microsoft.com/en-us/defender-cloud-apps/api-data-enrichment
upvoted 8 times

AVN1711 8 months ago
https://learn.microsoft.com/en-us/defender-cloud-apps/api-data-enrichment
upvoted 1 times

zaqwsx 3 years, 2 months ago
For me also BE
add Ip to corporate or exclude IP address from alert
upvoted 5 times

AlaReAla 3 years, 3 months ago
I echo your thoughts, I can get a few hints to support your answer at below location:

https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts
upvoted 2 times

a9e34f5 8 months, 3 weeks ago
It is clearly B and E. It is evident here in the Microsoft Learn documentation in the link that you provided AlaReAla. "This detection uses a machine learning algorithm that ignores obvious B-TP conditions, such as when the IP addresses on both sides of the travel are considered safe, the travel is trusted and excluded from triggering the Impossible travel detection. For example, both sides are considered safe if they

are tagged as corporate. However, if the IP address of only one side of the travel is considered safe, the detection is triggered as normal." which about 20 percent down on the page under Impossible Travel. I hope this helps.

upvoted 1 times

Startkabels 3 years, 2 months ago

At least B makes sense as the question reads a custom policy based on a custom IP range is in place. So false positive alerts that are generated by activity from the offices would be solved by adding their IP ranges in the custom IP range used in the policy..

upvoted 3 times

Startkabels 3 years, 2 months ago

https://docs.microsoft.com/en-us/cloud-app-security/ip-tags

upvoted 3 times

stromnessian Highly Voted 2 years, 10 months ago

Selected Answer: AB

A - this seems correct, as if you override the automatic detection of location for company IP address ranges, you can prevent the impossible travel alerts.

B - This makes sense as you need to define your corporate address ranges so that they are not seen as risky.

C - Increasing the sensitivity of the impossible travel detection would create more alerts.

D - Why would you set the IP addresses to the "Other" category when there is a "Corporate" category that fits the description?

E - Creating a new policy when there is already an existing one that you need to reduce the alerts from, would not reduce the number of alerts.

upvoted 36 times

Whatsamattr81 2 years, 4 months ago

Best answer IMHO. Stop (it says configure, it should say untick) the enrichment (for the impossible travel) add the addresses of your US offices, part of your company, to the corporate range.

upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago

AB correct

upvoted 2 times

Thezuland1098 2 months, 3 weeks ago

Selected Answer: AB

Without Data Enrichment we cant use the categories

A. The Data Enrichment API enables you to manage identifiable IP address ranges, such as your physical office IP addresses. IP address ranges allow you to tag, categorize, and customize the way logs and alerts are displayed and investigated.

B. Add the IP addresses to the corporate address range category. This action allows you to define the IP address ranges that belong to your organization and exclude them from anomaly detection policies such as impossible travel or sign-ins from risky IP addresses.

upvoted 2 times

shannon_c0le1 6 months, 1 week ago

Selected Answer: AB

A and B

upvoted 1 times

Avaris 6 months, 2 weeks ago

Selected Answer: AB

A and B is correct

upvoted 1 times

Avaris 6 months, 2 weeks ago

Selected Answer: AB

defo A, B

upvoted 1 times

DChilds 8 months, 1 week ago

This question was in the exam 27/04/2024.

upvoted 2 times

Ramye 10 months, 1 week ago

Selected Answer: AB

Based on the below information published here: https://learn.microsoft.com/en-us/defender-cloud-apps/ip-tags#create-an-ip-address-range

Corporate: These IPs should be all the public IP addresses of your internal network, your branch offices, and your Wi-Fi roaming addresses.
upvoted 1 times

chepeerick 1 year, 2 months ago
correct A and D
upvoted 2 times

prkhrkmr 1 year, 3 months ago
Only B seems to be the correct option as you can see the explanations of the difference "categories" here:
https://learn.microsoft.com/en-us/defender-cloud-apps/ip-tags#create-an-ip-address-range
upvoted 2 times

prkhrkmr 1 year, 3 months ago
Selected Answer: BC
B & C seem to be the only "available" configuration settings.

C.
Impossible Travel: https://security.microsoft.com/cloudapps/policy/anomaly/60253687a702c5eb0e8d86ca
Apart from increasing or decreasing Sensitivity (or excluding certain users), there is no other filter available. The answer option C should be corrected to "Decrease the sensitivity" and then it is the right answer ;-)

B.
Logon from Risky IP: https://security.microsoft.com/cloudapps/policy/activity/create?template=5b3116e1996fe317b4a1b25e
This looks at "Risky" category IP addresses only, so if the offices IPs are added to "Corporate" category or "Other" category, they go automatically out of scope for this policy. So even option D. can be considered a correct answer.

A. is irrelevant as "User enrichment" is the only "enrichment" related setting found: https://security.microsoft.com/cloudapps/settings?tabid=discovery-userEnrichment
E. is unnecessary as explained in B. above
upvoted 2 times

Gurulee 1 year, 3 months ago
Selected Answer: AB
A, B appear to be the best answers.
upvoted 1 times

mali1969 1 year, 3 months ago
Selected Answer: BE
To prevent alerts for legitimate sign-ins from known locations, you need to perform the following two actions:

B. Add the IP addresses to the corporate address range category. This action allows you to define the IP address ranges that belong to your organization and exclude them from anomaly detection policies such as impossible travel or sign-ins from risky IP addresses. You can add the IP addresses of your company's United States-based offices to the corporate address range category in the Microsoft 365 Defender portal, under Cloud Apps,
E. Create an activity policy that has an exclusion for the IP addresses. This action allows you to create a custom alert based on user activities and apply filters or exclusions to refine the results
upvoted 2 times

donathon 1 year, 4 months ago
C: No way to adjust
D: Doesn't make sense
E: Not possible to exclude the IP totally
upvoted 1 times

Oryx360 1 year, 4 months ago
Yes B & E is correct
upvoted 1 times

masterdeep 1 year, 5 months ago
B. Add the IP addresses to the corporate address range category.
E. Create an activity policy that has an exclusion for the IP addresses.

Explanation:

B. Add the IP addresses to the corporate address range category: By adding the IP addresses of your company's United States-based offices to the corporate address range category, you inform Microsoft Cloud App Security that these IP addresses are trusted and belong to your organization. This helps to avoid unnecessary alerts for legitimate sign-ins from these known locations.

E. Create an activity policy that has an exclusion for the IP addresses: By creating an activity policy and excluding the IP addresses of your United States-based offices, you can specify that alerts related to sign-ins from these locations should not be generated. This action ensures that legitimate sign-ins from your corporate offices are not considered as risky or impossible travel, thus reducing the number of unnecessary alerts.

The other options (A, C, and D) are not directly related to preventing alerts for legitimate sign-ins from known locations
upvoted 3 times

Question #22 *Topic 1*

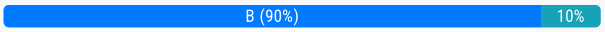
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Microsoft Defender for Identity integration with Active Directory.
From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.
Solution: You add each account as a Sensitive account.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

Community vote distribution



Nikki0222 2 months, 1 week ago
No correct
upvoted 2 times

g_man_rap 4 months, 1 week ago
Sensitive accounts are typically those you want to protect and monitor closely, such as high-privilege accounts (e.g., domain admins).
upvoted 1 times

Rand0mConsultant 6 months, 1 week ago
On Exam 25/06/2024
upvoted 3 times

33c26f0 11 months ago
Would it not be to set the account entity type as Honeytoken and not sensitive
upvoted 4 times

chepeerick 1 year, 2 months ago
option b
upvoted 2 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 1 times

imhere4you 1 year, 6 months ago
On exam - 19 June 2023
upvoted 1 times

lhadam_ 1 year, 6 months ago
Selected Answer: A
I think it's A - it would do the same thing
upvoted 1 times

lhadam_ 1 year, 6 months ago
wait nevermind lol my bad
upvoted 1 times

zellck 1 year, 7 months ago
Selected Answer: B

B is the answer.

https://learn.microsoft.com/en-us/defender-for-identity/entity-tags#sensitive--tags
The Sensitive tag is used to identify high value assets. The lateral movement path also relies on an entity's sensitivity status. Some entities are considered sensitive automatically by Defender for Identity, and others can be added manually.

upvoted 4 times

altecer 1 year, 10 months ago

On exam 2-11-2023

upvoted 1 times

tolu_x 1 year, 12 months ago

answer is correct

upvoted 1 times

saltytomato 2 years, 4 months ago

Selected Answer: B

B is the correct answer

upvoted 2 times

Tx4free 2 years, 10 months ago

Selected Answer: B

Correct

upvoted 3 times

irash1993 2 years, 10 months ago

Answer B is correct

upvoted 2 times

Question #23 *Topic 1*

You have a Microsoft 365 tenant that uses Microsoft Exchange Online and Microsoft Defender for Office 365.
What should you use to identify whether zero-hour auto purge (ZAP) moved an email message from the mailbox of a user?

A. the Threat Protection Status report in Microsoft Defender for Office 365

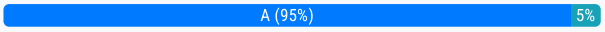
B. the mailbox audit log in Exchange

C. the Safe Attachments file types report in Microsoft Defender for Office 365

D. the mail flow report in Exchange

Suggested Answer: *A*
To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

Community vote distribution



us3r Highly Voted 2 years, 7 months ago

Selected Answer: A

A) answer refers to Threat Explorer

To determine if ZAP moved your message, you have the following options:
Number of messages: Use the Mailflow view in the Mailflow status report to see the number of ZAP-affected messages for the specified date range.
Message details: Use Threat Explorer (and real-time detections) to filter All email events by the value ZAP for the Additional action column.

answer D (Exchange mailflow) ≠ Mailflow view in the Mailflow status report
upvoted 12 times

vincenttoolate 2 years, 5 months ago

Yes, the answer D said "mail flow report in Exchange", this is not the same as "Mail Status Report" at Microsoft Defender for Office 365.

A is correct as per: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-email-security-reports?view=o365-worldwide#threat-protection-status-report

"The report provides the count of email messages with malicious content, such as files or website addresses (URLs) that were blocked by the anti-malware engine, zero-hour auto purge (ZAP), and Defender for Office 365 features like Safe Links, Safe Attachments, and impersonation protection features in anti-phishing policies."
upvoted 7 times

rdy4u Highly Voted 2 years, 8 months ago

To determine if ZAP moved your message, you have the following options:
• Number of messages: Use the Mailflow view in the Mailflow status report to see the number of ZAP-affected messages for the specified date range.
• Message details: Use Threat Explorer (and real-time detections) to filter All email events by the value ZAP for the Additional action column.

D should be.,=
upvoted 5 times

HAjouz Most Recent 3 weeks, 2 days ago

Selected Answer: B

While the Threat Protection Status report in Microsoft Defender for Office 365 provides an overview of threats detected and actions taken, it doesn't specifically track individual email movements caused by zero-hour auto purge (ZAP).

The mailbox audit log in Exchange is more precise for this purpose because it logs detailed actions on emails, including those moved by ZAP. This allows you to see exactly when and why an email was moved from a user's mailbox.

upvoted 1 times

Nikki0222 2 months, 1 week ago

A correct

upvoted 2 times

chepeerick 1 year, 2 months ago

option A

upvoted 2 times

Oryx360 1 year, 4 months ago

Selected Answer: B

It is the Mailbox Audit Log and all the other answers are wrong:
Zero-hour auto purge (ZAP) is a feature in Exchange Online Protection (EOP) that detects and removes emails containing malware even after they have been delivered to mailboxes.

upvoted 1 times

danlo 1 year, 1 month ago

ZAP is not logged in the Exchange mailbox audit logs as a system action.

upvoted 2 times

Anko6116 1 year, 10 months ago

Selected Answer: A

Correct seems to be A based on provided article. Section: How to see if ZAP moved your message.

https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

B - does not make sense to check Safe Attachments when we're looking for mails.
C & D: ZAP is not logged in the Exchange mailbox audit logs as a system action.

upvoted 5 times

Lone__Wolf 1 year, 10 months ago

Yes.. The correct option to identify whether ZAP moved an email message from the mailbox of a user is the Threat Protection Status report in Microsoft Defender for Office 365. This report provides information about the actions taken by Microsoft Defender for Office 365, including ZAP, to protect the tenant against malicious email messages.
The zero-hour auto purge (ZAP) is not logged as a system action in the Exchange mailbox audit logs. So B is incorrect.

upvoted 1 times

UmarCyber 1 year, 10 months ago

To determine if ZAP moved your message, you can use either the Threat Protection Status report or Threat Explorer (and real-time detections).

So the answer is - A

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide

upvoted 2 times

Ramkid 1 year, 11 months ago

Correct Answer,
Just check this https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#how-to-see-if-zap-moved-your-message

upvoted 1 times

AbdulMueez 2 years, 1 month ago

The answer is A

upvoted 2 times

Metasploit 2 years, 2 months ago

Selected Answer: A

A by process of elimination.

Not the following:
b = ZAP is not logged as system action in auditlog in exchange
c = The Safe attachment file types report has been deprecated and is now replaced by the Threat Protection Status Report.
d= The mail flow report in "Exchange". Not the "Mail Flow status Report". The mail flow reports in "Exchange" are not relevant here.

upvoted 3 times

amsioso 2 years, 3 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/view-email-security-reports?view=o365-worldwide#threat-protection-status-report

upvoted 1 times

Whatsamattr81 2 years, 4 months ago

Keyword here is 'an' email message. Not how many email messages.

Number of messages: Use the Mailflow view in the Mailflow status report to see the number of ZAP-affected messages for the specified date range.

Message details: Use Threat Explorer (and real-time detections) to filter All email events by the value ZAP for the Additional action column.

To check 'an email', use Threat Explorer first

upvoted 2 times

prjreddit 2 years, 5 months ago

Selected Answer: A

The answer is A. The mail flow report does show the flow of all mail on aggregate - so you do see the number of mails moved by ZAP - but the questions state a mail from a specific user - that you see in the Threat Explorer.

upvoted 2 times

Mthaher 2 years, 8 months ago

it should be D the mail flow report in Exchange .

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#how-to-see-if-zap-moved-your-message

upvoted 5 times

Question #24 *Topic 1*

You have a Microsoft 365 subscription that contains 1,000 Windows 10 devices. The devices have Microsoft Office 365 installed.
You need to mitigate the following device threats:
➪ Microsoft Excel macros that download scripts from untrusted websites
➪ Users that open executable attachments in Microsoft Outlook
➪ Outlook rules and forms exploits
What should you use?

A. Microsoft Defender Antivirus

B. attack surface reduction rules in Microsoft Defender for Endpoint

C. Windows Defender Firewall

D. adaptive application control in Azure Defender

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction?view=o365-worldwide

Community vote distribution
B (100%)

Metasploit Highly Voted 2 years, 2 months ago
Selected Answer: B
B: Attack Surface Reduction rules.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide

Block all Office applications from creating child processes
Block executable content from email client and webmail
upvoted 13 times

Nikki0222 Most Recent 2 months, 1 week ago
B correct
upvoted 1 times

An1996 1 year, 1 month ago
B--Attack Surface Reduction rules.
upvoted 1 times

billo79152718 1 year, 7 months ago
B. Attack surface reduction rules in Microsoft Defender for Endpoint
upvoted 1 times

UmarCyber 1 year, 10 months ago
Selected Answer: B
B is the correct answer!
upvoted 1 times

Apocalypse03 2 years ago
Selected Answer: B
Attack Surface Reduction rules.
upvoted 2 times

Question #25 *Topic 1*

You have a third-party security information and event management (SIEM) solution.
You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.
What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.

B. Configure the Diagnostics settings in Azure AD to stream to an event hub.

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

Community vote distribution
B (100%)

rdy4u Highly Voted 2 years, 8 months ago
Routing logs to an Azure event hub allows you to integrate with third-party SIEM tools like Sumologic and Splunk.
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub
upvoted 16 times

Nikki0222 Most Recent 2 months, 1 week ago
B correct
upvoted 1 times

chepeerick 1 year, 2 months ago
Selected Answer: B
Correct is B
upvoted 1 times

Apocalypse03 2 years ago
Selected Answer: B
B is correct
upvoted 3 times

Jadeitalia365 2 years, 3 months ago
Selected Answer: B
B is correct
upvoted 2 times

Whatsamattr81 2 years, 4 months ago
Can do with B or D depending on the SIEM... But B would likely work with all.
upvoted 1 times

Holii 1 year, 8 months ago
Question explicitly states third-party SIEM. This needs to be streamed to an Event Hub -> SIEM. B.
upvoted 4 times

CatoFong 2 years, 5 months ago
Selected Answer: B
B is correct
upvoted 2 times

giver 2 years, 5 months ago
answer is correct B
upvoted 2 times

Hami3191 2 years, 5 months ago
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring#:~:text=Stream%20logs%20to,event%20hub.

upvoted 3 times

feye2020 2 years, 6 months ago

Thanks

upvoted 2 times

DRAG DROP -

You have an Azure subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains two users named User1 and User2.

You plan to deploy Azure Defender.

You need to enable User1 and User2 to perform tasks at the subscription level as shown in the following table.

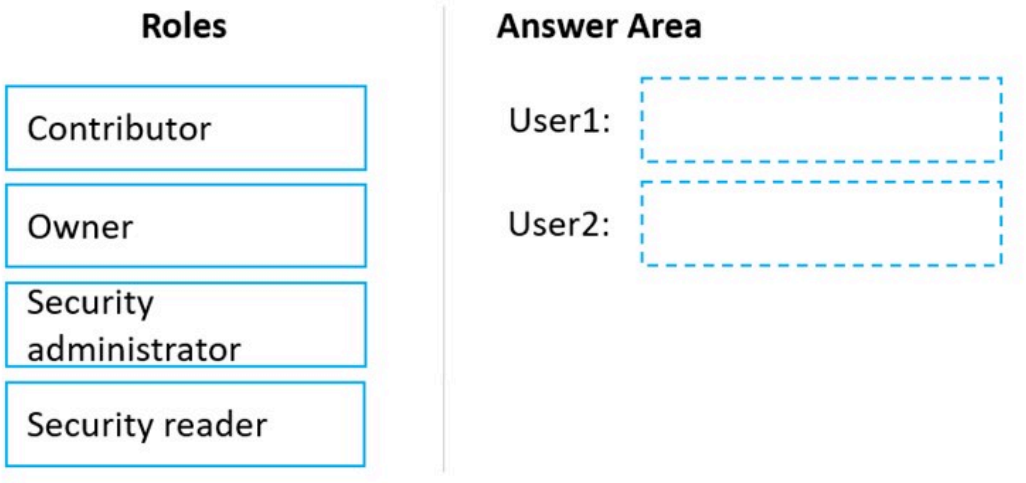
User	Task
User1	• Assign initiatives • Edit security policies • Enable automatic provisioning
User2	• View alerts and recommendations • Apply security recommendations • Dismiss alerts

The solution must use the principle of least privilege.

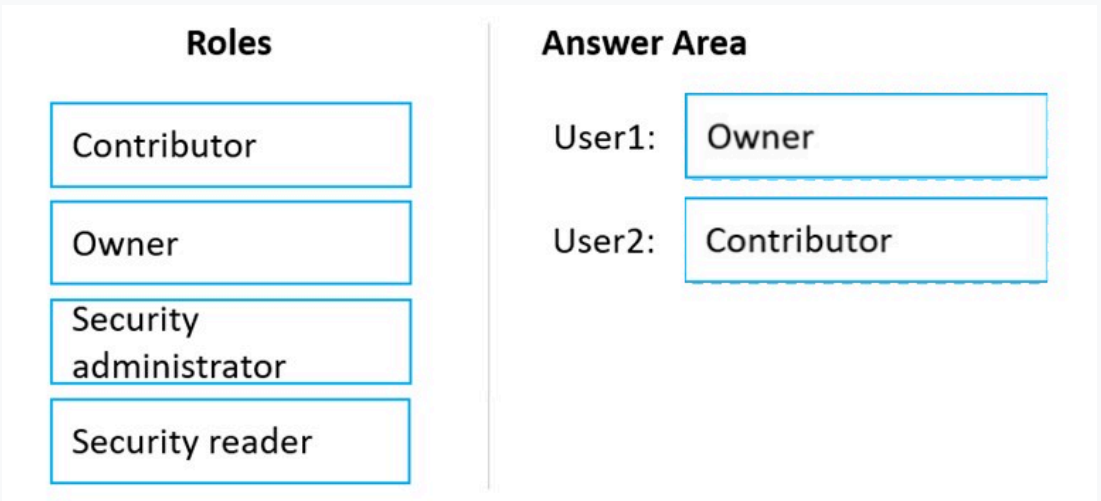
Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

Select and Place:



Suggested Answer:



Box 1: Owner -

Only the Owner can assign initiatives.

Box 2: Contributor -

Only the Contributor or the Owner can apply security recommendations.

Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

Lion007 Highly Voted 3 months, 2 weeks ago

Answer is correct, but the justification provided is not quite accurate.
User1: Owner
User2: Contributor

You can't choose 'Security Admin' because the key in the questions is 'at the subscription level'. Read the Security Admin section in the documentation https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

At the Subscription Level, only Contributor and Owner can :
- Apply security recommendations
- Add/Assign initiatives
- Edit security policy
- Dismiss alerts

However, only the Owner can 'Enable auto provisioning'... to be the owner of the extension you're deploying. "For auto provisioning, the specific role required depends on the extension you're deploying." Check the section under the roles table https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions

All roles can 'view' alerts and recommendations.
upvoted 58 times

Tanasi 2 years, 3 months ago

This guy is correct. Details here:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-loganalytic#availability
upvoted 5 times

j888 Highly Voted 2 years, 8 months ago

Wouldn't this be contributors for both?
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 16 times

LotusBeta 2 years, 5 months ago

Sorry i was wrong to upvote this answer, the right answer is Owner and then Contributor.
upvoted 4 times

Tohar 2 years ago

That's correct. Because only Owner can ASSIGN Initiatives at the subscription level.
upvoted 3 times

Adam7777 Most Recent 2 months, 4 weeks ago

user1: Contributor
user2: Security Reader

user1, Don't need to be an owner or Security Administrator to do the mentioned tasks.
user2, only needs to read and apply security recommendations and dismiss alerts, Hence, Seucirty reader is the only option
upvoted 1 times

Murtuza 1 year ago

The other give away in this question is security administrator no such thing so you can easily rule that out . Its actually security admin in Azure AD RBAC role
upvoted 1 times

danlo 1 year, 1 month ago

Is Security Administrator a typo? There's an Entra AD role named that but RBAC is "Security Admin"
upvoted 1 times

chepeerick 1 year, 2 months ago

correct
upvoted 1 times

Marchiano 1 year, 5 months ago

User 1: Owner
User 2: Contributor
Keyword: at subscription level

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions

upvoted 3 times

UmarCyber 1 year, 10 months ago

At subscription level only owner can 'Add/assign initiatives (including) regulatory compliance standards)'. Answer is correct.

upvoted 4 times

Matshedy 1 year, 11 months ago

Correct answer:
User 1: contributor
User 2: contributor

upvoted 1 times

zafara55 2 years ago

Apology. Security Administrator is not correct for user 1. It's not applied at the subscription level.

upvoted 1 times

zafara55 2 years ago

Security Administrator is also correct for user 1.
Security Admin can Add/assign initiatives (including) regulatory compliance standards)

upvoted 1 times

Snaileyes 2 years, 2 months ago

At the given reference URL… Contributor can also assign initiatives… So… Contributor for both!

upvoted 1 times

Reyrain 2 years, 1 month ago

no, it is quite clear that is not the case from the (above) linked article.

upvoted 1 times

Pandaguo 2 years, 2 months ago

The solution must use the principle of least privilege....
contributor priviledge is lower than owner I suppose, if so the first one why don't select contributor ?

upvoted 2 times

Tanasi 2 years, 3 months ago

Solution is correct.
Owner and Contributor are required. If you enable Auto Provisioning, there are resources that require you to be Owner on that subscription.

Details here:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-loganalytic#availability

upvoted 3 times

Tanasi 2 years, 3 months ago

Contributor on subscription role for both. Remember that big difference between Contributor and Owner is that Owner also has access to modify RBAC (which is not required here, and will not adhere to Principle of Least Privilege)

upvoted 3 times

Stiobhan 2 years, 4 months ago

Right answer is contributor for both:
Action Security Reader /
Reader Security Admin Contributor / Owner Contributor Owner
(Resource group level) (Subscription level) (Subscription level)
Add/assign initiatives (including) regulatory compliance standards) - - - ✔ ✔
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions
It's right there in the link. Remember, it asking at the subscription level.

upvoted 3 times

bluegeek 2 years, 4 months ago

Given answer is correct. Key part is "at the subscription level"
Security admin only has access in Defender for cloud and not other Azure services
https://docs.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 2 times

Question #27 *Topic 1*

HOTSPOT -

You have a Microsoft 365 E5 subscription that contains 200 Windows 10 devices enrolled in Microsoft Defender for Endpoint.

You need to ensure that users can access the devices by using a remote shell connection directly from the Microsoft 365 Defender portal. The solution must use the principle of least privilege.

What should you do in the Microsoft 365 Defender portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To configure Microsoft Defender for Endpoint:

- Turn on endpoint detection and response (EDR) in block mode
- Turn on Live Response
- Turn off Tamper Protection

To configure the devices:

- Add a network assessment job
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

Suggested Answer:

Answer Area

To configure Microsoft Defender for Endpoint:

- Turn on endpoint detection and response (EDR) in block mode
- Turn on Live Response
- Turn off Tamper Protection

To configure the devices:

- Add a network assessment job
- Create a device group that contains the devices and set Automation level to Full
- Create a device group that contains the devices and set Automation level to No automated response

Box 1: Turn on Live Response -

Live response is a capability that gives you instantaneous access to a device by using a remote shell connection. This gives you the power to do in-depth investigative work and take immediate response actions.

Box: 2 -

Network assessment jobs allow you to choose network devices to be scanned regularly and added to the device inventory.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-devices?view=o365-worldwide

Lion007 Highly Voted 2 years, 6 months ago

The first answer is correct, but the second answer is wrong.

The network assessment job has nothing to do with the question. It is a feature to scan networks and discover network devices for vulnerability management. The correct answer should be "Automation in Full mode", because it is the only correct answer since the last provided answer is to set Automation to "Not automated" which is not correct as per Microsoft docs on Live Response, check it out here "Ensure that the device has an Automation Remediation level assigned to it." https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

upvoted 59 times

Nikki0222 2 months, 1 week ago

Correct

upvoted 2 times

CatoFong 2 years, 5 months ago

Lion007 is correct. Turn on Live Response >> Automation level to Full

upvoted 9 times

urisoft 1 year, 11 months ago

I subscribe to the above: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/automation-levels?view=o365-worldwide#levels-of-automation

upvoted 1 times

rdy4u Highly Voted 2 years, 8 months ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

Ensure that the device has an Automation Remediation level assigned to it.
You'll need to enable, at least, the minimum Remediation Level for a given Device Group. Otherwise you won't be able to establish a Live Response session to a member of that group.

upvoted 11 times

Adam7777 Most Recent 2 months, 4 weeks ago

1. Turn on Liv response
2. Create a device group that contains the devices and set Automation level to No automated response, because setting "no automated response" ensures that Defender for Endpoint will not automatically take any actions on devices, but users can still use Live Response. This adheres to the principle of least privilege, as users are not granted unnecessary automated control over devices.

upvoted 1 times

chepeerick 1 year, 2 months ago

Turn On Live response and full level

upvoted 2 times

donathon 1 year, 3 months ago

Turn on Live reponse and Full automation

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 2 times

Marchiano 1 year, 6 months ago

Box 1: Turn on Live Response
Fact: Live response requires Automated investigation to be turned on before you can enable it in the advanced settings section in the Microsoft Defender for Endpoint portal. - this also gives the answer to Box 2

Box 2: Create a device group that contains the devices and set Automation level to Full
"With no automation, automated investigation doesn't run on your organization's devices."
no automation = automated investigation is off, not on, and it needs to be on (Full Remediation) for Live Response to work.

upvoted 2 times

ct1984 1 year, 8 months ago

The second answer is obviosuly wrong. Why isnt this page updated?

upvoted 9 times

doch 1 year, 11 months ago

1. Turn On Live Response
2. Automation Level should be full. Ensure that the device has an Automation Remediation level assigned to it. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?source=recommendations&view=o365-worldwide

upvoted 2 times

Fukacz 2 years, 3 months ago

Second need to be full. Whole concept of REMEDIATION during live connect is based on Remediation assigned. If its off, then Live connect wont start.

upvoted 3 times

DumbBobJohnson 2 years, 8 months ago

The second answer should be the last one. It has to have a minimum Remediation level
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide

upvoted 4 times

vincenttoolate 2 years, 6 months ago

no, the last one is "no automated response", which means "no automation".
"Create a device group that contains the devices and set Automation level to full" is the only answer have automation remediation enabled.

upvoted 2 times

avr 2 years, 6 months ago

it says "no automated response" but still is a Remediation Level and the question says "least privileges" so, the second answer should be the last one

upvoted 2 times

abdulwaheed525 2 years, 8 months ago

The second answer for the creation of a network assessment job is confusing. Could someone explain?

upvoted 1 times

StaxJaxson 2 years, 7 months ago

Its a red herring - its wrong - nothing to do with AIR/LR.

upvoted 3 times

Question #28 *Topic 1*

HOTSPOT -

You have a Microsoft 365 subscription that uses Microsoft 365 Defender and contains a user named User1.

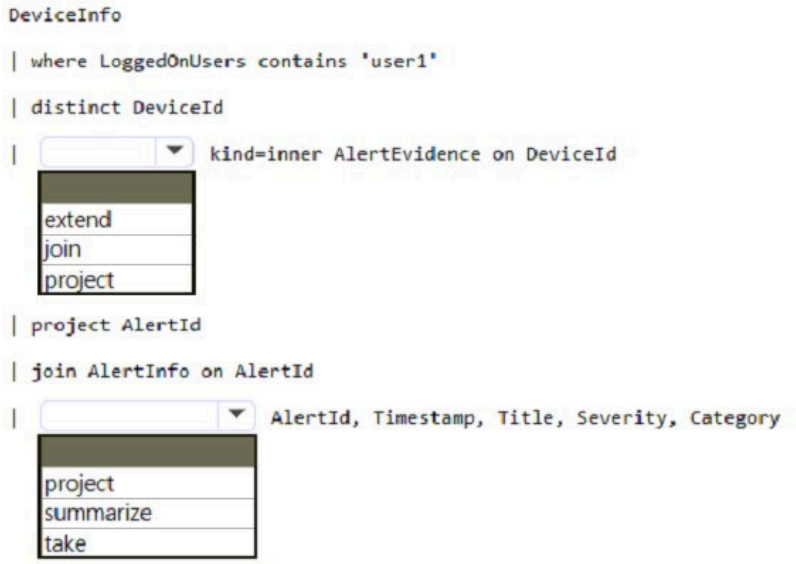
You are notified that the account of User1 is compromised.

You need to review the alerts triggered on the devices to which User1 signed in.

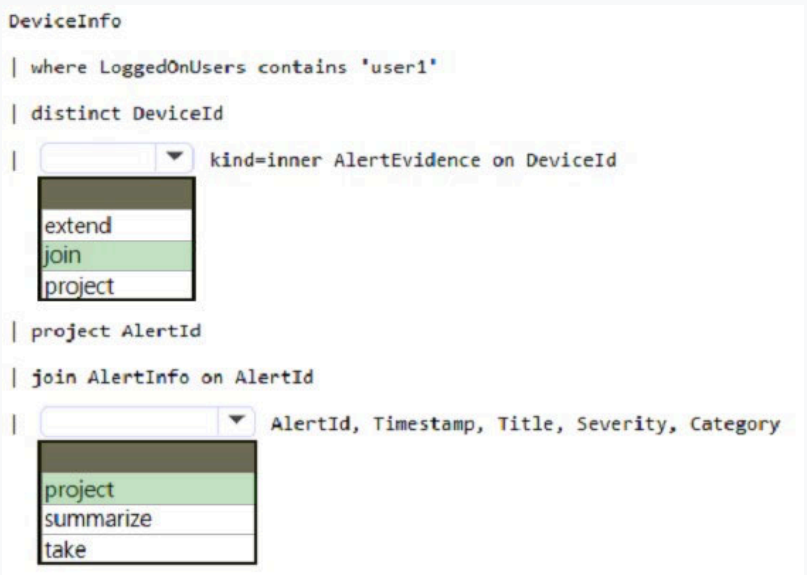
How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Box 1: join -

An inner join.

This query uses kind=inner to specify an inner-join, which prevents deduplication of left side values for DeviceId.

This query uses the DeviceInfo table to check if a potentially compromised user (<account-name>) has logged on to any devices and then lists the alerts that have been triggered on those devices.

DeviceInfo -

//Query for devices that the potentially compromised account has logged onto

| where LoggedOnUsers contains '<account-name>'

| distinct DeviceId

//Crosscheck devices against alert records in AlertEvidence and AlertInfo tables

| join kind=inner AlertEvidence on DeviceId

| project AlertId

//List all alerts on devices that user has logged on to

| join AlertInfo on AlertId

| project AlertId, Timestamp, Title, Severity, Category
DeviceInfo LoggedOnUsers AlertEvidence "project AlertID"

Box 2: project -
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide

Apocalypse03 Highly Voted 2 years ago
Correct: join & project

Filtering the DeviceInfo table to only include rows where the LoggedOnUsers field contains the string "user1".
Removing duplicates based on the DeviceId field.
Joining the resulting set of devices with the AlertEvidence table based on the DeviceId field.
Projecting the AlertId field from the resulting set.
Joining the resulting set of alerts with the AlertInfo table based on the AlertId field.
Projecting the AlertId, Timestamp, Title, Severity, and Category fields from the resulting set of alerts.
This query retrieves a list of alerts that are related to devices where the user "user1" is logged on, and it includes the alert ID, timestamp, title, severity, and category for each alert. The "join" and "project" operations in the query are used to combine and filter the data from the various tables in the ATP data model.
upvoted 16 times

Nikki0222 2 months, 1 week ago
Correct
upvoted 2 times

smanzana 10 months, 2 weeks ago
Join
Project
upvoted 1 times

ACSC Highly Voted 2 years, 1 month ago
Correct, join & project
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#get-device-information
upvoted 5 times

chepeerick Most Recent 1 year, 2 months ago
correct
upvoted 2 times

trashbox 1 year, 3 months ago
"join" and "project" are correct.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-query-emails-devices?view=o365-worldwide#get-device-information
upvoted 2 times

RobertDuval 1 year, 8 months ago
In Exam today (21 April 2023)
upvoted 3 times

Lone__Wolf 1 year, 10 months ago
Correct!
upvoted 2 times

User_Mowgli 2 years, 2 months ago
Correct. Join and project respectively.
upvoted 3 times

Question #29 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft SharePoint Online.
You delete users from the subscription.
You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted.
What should you use?

A. a file policy in Microsoft Defender for Cloud Apps

B. an access review policy

C. an alert policy in Microsoft Defender for Office 365

D. an insider risk policy

Suggested Answer: *C*
Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.
Default alert policies include:
Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

Community vote distribution
D (82%) Other

Metasploit Highly Voted 2 years, 2 months ago
Selected Answer: D
D: Insider risk policy.

Data theft by departing users:

https://learn.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-policies?view=o365-worldwide#data-theft-by-departing-users

When users leave your organization, there are specific risk indicators typically associated with data theft by departing users. This policy template uses exfiltration indicators for risk scoring and focuses on detection and alerts in this risk area.
upvoted 29 times

Bhuru 1 month, 3 weeks ago
D is also the answer on Microsoft practise test as well.
upvoted 2 times

espnadmin Highly Voted 2 years, 4 months ago
D. an insider risk policy
upvoted 20 times

RafaAbel 2 years, 4 months ago
I agree due to the context, this guy was leaving the company then being monitored by insider risk policy
upvoted 4 times

uday1985 1 year, 8 months ago
requires an alert.. stop assuming :
An insider risk policy is used to monitor and detect risky behavior by employees within an organization. This policy can help identify and prevent insider threats such as data theft, sabotage, and espionage.
upvoted 3 times

Chris2pher 1 year ago
Then how will it create an alert if the user has already been deleted?

upvoted 1 times

Ramye 11 months, 1 week ago

It says you to be notified prior to the acct was deleted

"You need to be notified if the deleted users downloaded numerous documents from SharePoint Online sites during the month before their accounts were deleted."

upvoted 1 times

mimguy 1 year, 6 months ago

It says 'You need to be notified'. The insider risk policy will detect and the alert policy will notify. It's got to be C.

upvoted 2 times

HAjouz Most Recent 3 weeks, 2 days ago

Selected Answer: A

A. a file policy in Microsoft Defender for Cloud Apps

This option allows you to create policies that can monitor and alert you on specific activities, such as downloading a large number of documents, which is crucial for identifying potential data exfiltration before user accounts are deleted.a file policy in Microsoft Defender for Cloud Apps is specifically designed to monitor and control file activities, including downloads, across your cloud environment. insider risk can be used to monitor and alert on risky activities, it is more comprehensive and typically used for ongoing monitoring of insider threats rather than specific scenarios like monitoring document downloads before account deletion.

upvoted 1 times

Nikki0222 2 months, 1 week ago

D correct

upvoted 2 times

Jacob_Plummer 4 months, 4 weeks ago

This exact question nearly word for word is on the microsoft practice exam for the SC-200 and the answer they give is "a Microsoft Purview insider risk management policy"

upvoted 2 times

Avaris 6 months, 2 weeks ago

Selected Answer: A

File policy focus on SP while alert policy focus on emails so its A and defo not user risk as this is related to the use's risk posture.

upvoted 2 times

emartiy 7 months ago

Selected Answer: C

To be notified if deleted users downloaded numerous documents from SharePoint Online sites before their accounts were deleted, consider the following approach:

Configure an Alert Policy in Microsoft Defender for Office 365 (Option C):
Set up an alert policy that monitors user activity related to document downloads in SharePoint Online.
Customize the policy to trigger alerts when specific thresholds (e.g., numerous downloads) are exceeded.
Ensure that the policy covers the relevant time frame (e.g., the month before account deletion).
Remember that alert policies allow you to proactively monitor and respond to security-related events, including user activity in SharePoint Online. 😊 1

upvoted 2 times

emartiy 7 months ago

Selected Answer: D

What the question say.. .What the selected answer and justification say.. They two are far away from each other :)) It say to method detect insider risk.. So what the policy be? :) Thanks.. If you read all units or prepation for this exam. You also will anderstand what I mean in my first sentence :)

upvoted 1 times

Zak_Zakaria 8 months ago

Also, I thought the answer would be an insider risk policy, but I'm now more convinced that it's A as explained by Copilot, I think he's right, and here is why:
-Insider Risk policy is for active users not deleted ones as mentioned in the question, and no way to set deleted users as insider risk.
-For option C: idem, we can't set alerts for deleted users who are not anymore in the company, and even if we can (technically), it won't serve

anything as long as the user is not active anymore to trigger the alert.
-But option A: is more likely correct since we can trigger the deletion of files and fine-tune to filter for users recently deleted and their activity in the last month.

I think it makes more sense, and maybe Copilot is right :).
upvoted 1 times

Baz10 10 months, 1 week ago
Anyone got any clarity on this question? I thought it was D but answer claims C. GPT says A lmao
upvoted 1 times

Durden871 9 months, 3 weeks ago
Yeah, ChatGPT is weird, but good call out to suggest it. Always forget its existence. When I enter it, it talks about editing SharePoint auditing in the compliance center and configure policies. Doesn't mention Cloud Apps. If I ask it directly what does Insider Risk Managemtn in 365 does:
nalyzes user activities, communications, and interactions within Microsoft 365 services (such as Exchange Online, SharePoint Online, OneDrive for Business, Teams, etc.) to identify patterns indicative of insider threats.

It then talks about sending alerts and messaging when there's a suspicion of insider threats.
upvoted 1 times

Durden871 9 months, 3 weeks ago
Of Course I kept playing with it and confused myself more:
"need to be notified if the deleted users downloaded numerous documents from SharePoint Online"

Navigate to Alert Policies:
Within the Compliance Center, locate the "Alert policies" section. This is where you can create and manage alert policies for various security and compliance purposes.

Create a New Alert Policy:
Click on "Create policy" or a similar option to start creating a new alert policy.
upvoted 1 times

Durden871 9 months, 3 weeks ago
Then again. The answer given is create a policy in Compliance Center, not Defender. If you ask it directly: User
"Can insider risk management be used to alert if deleted users had downloaded thousands of sharepoint files"

While IRM provides robust capabilities for identifying suspicious activities and behaviors, such as data exfiltration attempts or unusual access patterns, it may not directly offer a specific alert condition for detecting if deleted users had downloaded thousands of SharePoint files.

While IRM may not offer a predefined alert condition specifically for tracking file downloads by deleted users, you can leverage its flexibility to create custom alert policies that meet your organization's specific monitoring and security requirements.

So it really sounds like there's no correct answer listed. It's an alert policy created in the compliance center, not Defender. To be fair, the answer given also stated, "as of 2022".
upvoted 1 times

kostask 10 months, 3 weeks ago
Selected Answer: D
For sye Insider risk policy
upvoted 1 times

MentalG 11 months, 1 week ago
Definitely insider risk policy
upvoted 1 times

Chris2pher 1 year ago
weird question. It says notified, then the user was already deleted. and the monitoring was from the previous month. "notified" should not be the word it should be "report"
upvoted 1 times

MentalG 1 year, 1 month ago

Selected Answer: D

Insider risk policy gives you this ability

upvoted 1 times

chepeerick 1 year, 2 months ago

seem to be correct

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 1 times

oddsol 1 year, 2 months ago

And what was the correct solution? C?

upvoted 1 times

mali1969 1 year, 4 months ago

Selected Answer: C

Alert policies let you categorize the alerts that are triggered by a policy, apply the policy to all users in your organization, set a threshold level for when an alert is triggered, and decide whether to receive email notifications when alerts are triggered.

Default alert policies include:

Unusual external user file activity - Generates an alert when an unusually large number of activities are performed on files in SharePoint or OneDrive by users outside of your organization. This includes activities such as accessing files, downloading files, and deleting files. This policy has a High severity setting.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies

upvoted 1 times

Durden871 9 months, 3 weeks ago

But it says "Defender" not "Compliance". So while this is likely the answer, it's still wrong.

upvoted 1 times

Question #30 *Topic 1*

You have a Microsoft 365 subscription that has Microsoft 365 Defender enabled.
You need to identify all the changes made to sensitivity labels during the past seven days.
What should you use?

A. the Incidents blade of the Microsoft 365 Defender portal

B. the Alerts settings on the Data Loss Prevention blade of the Microsoft 365 compliance center

C. Activity explorer in the Microsoft 365 compliance center

D. the Explorer settings on the Email & collaboration blade of the Microsoft 365 Defender portal

Suggested Answer: *C*
Labeling activities are available in Activity explorer.
For example:

Sensitivity label applied -
This event is generated each time an unlabeled document is labeled or an email is sent with a sensitivity label.
It is captured at the time of save in Office native applications and web applications.
It is captured at the time of occurrence in Azure Information protection add-ins.
Upgrade and downgrade labels actions can also be monitored via the Label event type field and filter.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer-available-events?view=o365-worldwide

Community vote distribution
C (100%)

celomomo Highly Voted 1 year, 12 months ago
Selected Answer: C
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer?view=o365-worldwide
upvoted 6 times

Nikki0222 Most Recent 2 months, 1 week ago
C correct
upvoted 2 times

chepeerick 1 year, 2 months ago
correct C
upvoted 1 times

Holii 1 year, 8 months ago
Note that there is a method of seeing changes to sensitive labels in Microsoft Defender using Audit. Since this option isn't here, we can assume that we also have a license for Compliance since the only one that matches is C.
upvoted 2 times

ACSC 2 years, 1 month ago
Selected Answer: C
Activity explorer rounds out this suite of functionality by allowing you to monitor what's being done with your labeled content.
There are over 30 different filters available for use, some are:
Date range, Activity type, Location, User, Sensitivity label, Retention label, File path, DLP policy
upvoted 4 times

ACSC 2 years, 1 month ago
Now it is Microsoft Purview compliance portal
upvoted 5 times

Metasploit 2 years, 2 months ago
Selected Answer: C
C: Activity Explorer in M365 Compliance center

https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview?view=o365-worldwide

You can find data classification in the Microsoft Purview compliance portal (or Microsoft 365 Defender portal) > Classification > Data Classification.

You also manage these features on the data classification page:

trainable classifiers
sensitive information types
Learn about exact data match based sensitive information types
content explorer
-------> activity explorer
https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-activity-explorer?view=o365-worldwide
upvoted 3 times

PatWafy 2 years, 2 months ago
C : est la bonne réponse
upvoted 2 times

Ramkid 1 year, 11 months ago
Tres bien
upvoted 1 times

Question #31 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You need to identify all the entities affected by an incident.
Which tab should you use in the Microsoft 365 Defender portal?

A. Investigations

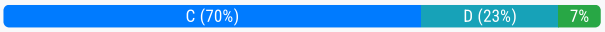
B. Devices

C. Evidence and Response

D. Alerts

Suggested Answer: *C*
The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.
Incorrect:
* The Investigations tab lists all the automated investigations triggered by alerts in this incident. Automated investigations will perform remediation actions or wait for analyst approval of actions, depending on how you configured your automated investigations to run in Defender for Endpoint and Defender for Office 365.
* Devices
The Devices tab lists all the devices related to the incident.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents

Community vote distribution



Pointless Highly Voted 3 months, 2 weeks ago
Correct Answer - C, Evidence and Response.

Question emphasizes on 'incident'. Though you can view affected entities by clicking on Alerts tab > Alert list, it will be for that particular alert one alert doesn't necessarily be an incident. An incident can have multiple alerts. So you need to click on Incidents tab, open the Incident, go to Evidences and Response tab and look there.
upvoted 27 times

Nickname01 2 years, 2 months ago
Correct answer is indeed C: wheb you click on an incident it will open the Summary tab, on the summery tab you can see the overview of evidence with a option to view all entities, this will bring you to "Evidence and Response".
upvoted 5 times

Metasploit Highly Voted 2 years, 2 months ago
Selected Answer: C
Question Keywords: "...identify all the entities AFFECTED BY AN INCIDENT."
Answer: C Evidence and response.

"The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident."

https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents?view=o365-worldwide#evidence-and-response
upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago
C correct
upvoted 2 times

Lone_Wolf 3 months, 2 weeks ago
Selected Answer: C
The "Evidence and Response" tab in the Microsoft 365 Defender portal can be used to identify all the entities affected by an incident. In the "Evidence and Response" tab, you can access information about the scope of the incident and the entities that were affected. This information can help you understand the extent of the incident and determine the necessary steps to respond to it.
upvoted 3 times

kazaki 1 year ago

Evidence and Response

upvoted 1 times

chepeerick 1 year, 2 months ago

Selected Answer: C

correct C

upvoted 1 times

Candice79 1 year, 2 months ago

Assets is actually correct https://learn.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

upvoted 1 times

hovlund 1 year, 2 months ago

That is not an option....

upvoted 1 times

Oryx360 1 year, 4 months ago

Selected Answer: A

A. Investigations

To identify all the entities affected by an incident in the Microsoft 365 Defender portal, you should use the "Investigations" tab. The Investigations tab provides a centralized location where you can manage and track incidents, perform analysis, and review related entities and evidence associated with the incident.

Using the Investigations tab, you can explore the scope of the incident, review impacted devices, users, and other entities, and gather evidence to understand the nature and extent of the security issue. This tab allows you to perform a comprehensive investigation to ensure that you have a clear understanding of the incident's impact on your environment.

The other options (B, C, and D) are relevant to incident response and security management but may not provide the same level of comprehensive analysis and entity identification as the Investigations tab.

upvoted 3 times

danb67 1 year, 2 months ago

do a lab mate this is the wrong answer - Evidence and Response is correct

upvoted 1 times

Solozero 1 year, 6 months ago

Selected Answer: C

The Alerts tab is primarily used for monitoring and managing security alerts generated by various Microsoft 365 Defender services. While it can provide insights into individual alerts, it may not provide a holistic view of all entities affected by an incident. So defintely C

upvoted 1 times

CodexFT 1 year, 8 months ago

Selected Answer: C

Evidence as response - contains all the details of entities on an incident

upvoted 2 times

Anko6116 1 year, 10 months ago

Selected Answer: C

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents?view=o365-worldwide

upvoted 1 times

Locian 1 year, 11 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

celomomo 2 years ago

The Evidence and Response tab shows all the supported events and suspicious entities in the alerts in the incident.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents?view=o365-worldwide
upvoted 3 times

celomomo 2 years ago
Answer is correct as C
upvoted 3 times

SuperGraham 2 years ago
Selected Answer: C
C - Evidence and Response
https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents#evidence-and-response
The description even says 'Microsoft 365 Defender automatically investigates all the incidents' supported events and suspicious entities in the alerts, providing you with information about the important emails, files, processes, services, IP Addresses, and more.'
upvoted 2 times

[Removed] 2 years ago
Selected Answer: C
C - Evidence and Response
https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents#evidence-and-response
The description even says 'Microsoft 365 Defender automatically investigates all the incidents' supported events and suspicious entities in the alerts, providing you with information about the important emails, files, processes, services, IP Addresses, and more.'
upvoted 2 times

[Removed] 2 years ago
C - Evidence and Response
https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-incidents#evidence-and-response
The description even says 'Microsoft 365 Defender automatically investigates all the incidents' supported events and suspicious entities in the alerts, providing you with information about the important emails, files, processes, services, IP Addresses, and more.'
upvoted 1 times

Apocalypse03 2 years ago
Selected Answer: C
To identify all the entities affected by an incident in the Microsoft 365 Defender portal, you should use the Evidence and Response tab.

The Evidence and Response tab in the Microsoft 365 Defender portal provides a detailed view of an incident, including information about the affected entities. When you select an incident in the Investigations tab, the Evidence and Response tab will display information about the affected users, devices, applications, and other entities. You can use this information to understand the scope of the incident and to determine which entities may have been compromised or affected by the incident.

The Devices, Alerts, and Investigations tabs may also contain information about affected entities, but the Evidence and Response tab provides the most comprehensive view of the entities involved in an incident.
upvoted 3 times

Question #32 *Topic 1*

You have a Microsoft 365 E5 subscription that is linked to a hybrid Azure AD tenant.

You need to identify all the changes made to Domain Admins group during the past 30 days.

What should you use?

A. the Modifications of sensitive groups report in Microsoft Defender for Identity

B. the identity security posture assessment in Microsoft Defender for Cloud Apps

C. the Azure Active Directory Provisioning Analysis workbook

D. the Overview settings of Insider risk management

Suggested Answer: *A*

Community vote distribution

A (100%)

Wutan Highly Voted 1 year, 11 months ago

Selected Answer: A

Can confirm it's A. |> Reports |> Modifications to sensitive groups

upvoted 7 times

UmarCyber 1 year, 10 months ago

Thanks for confirming buddy!

upvoted 4 times

Nikki0222 Most Recent 2 months, 1 week ago

A correct

upvoted 1 times

cjstrong 7 months, 1 week ago

Microsoft 365 defender --> Reports --> Identities --> Report Management --> Modification to sensitive groups

upvoted 1 times

Ramye 10 months, 1 week ago

hmm -- everyone saying Modifications of Sensitive Groups report under reports in Microsoft Defender for Portal but I don't see this modification of Sensitive Groups report.

Could this be now that Defender for Identity is now part of Microsoft Defender XDR?

upvoted 1 times

Ramye 10 months, 1 week ago

I think this question is no longer valid since Defender for Identity is now part of Defender XDR.

upvoted 2 times

Sparkletoss 1 month ago

Microsoft 365 defender --> Report management (will take you to identities reports)--> Modification to sensitive groups

upvoted 1 times

chepeerick 1 year, 2 months ago

correct A

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 4 times

tatendazw 1 year, 6 months ago

https://learn.microsoft.com/en-us/defender-for-identity/entity-tags#sensitive-entities

upvoted 1 times

Adom3730 1 year, 7 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/defender-for-identity/classic-reports

upvoted 2 times

Lone_Wolf 1 year, 10 months ago

Selected Answer: A

A. The Modifications of sensitive groups report in Microsoft Defender for Identity would be the best option to use to identify all the changes made to the Domain Admins group during the past 30 days. This report provides information about changes made to sensitive groups, including the Domain Admins group, in the Azure AD environment and helps to identify potential security threats.

upvoted 4 times

Gurulee 1 year, 3 months ago

Agreed! Thanks for the summarized explanation.

upvoted 1 times

Question #33 *Topic 1*

You have a Microsoft 365 subscription. The subscription uses Microsoft 365 Defender and has data loss prevention (DLP) policies that have aggregated alerts configured.

You need to identify the impacted entities in an aggregated alert.

What should you review in the DLP alert management dashboard of the Microsoft 365 compliance center?

A. the Events tab of the alert

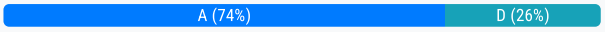
B. the Sensitive Info Types tab of the alert

C. Management log

D. the Details tab of the alert

Suggested Answer: *C*

Community vote distribution



eddz25 Highly Voted 1 year, 11 months ago

Selected Answer: A

In order to identify the impacted entities in an aggregated alert, you should review the "Events" tab of the DLP alert management dashboard in the Microsoft 365 compliance center. This tab will display a list of all the events that triggered the alert, including the specific entities (e.g. files, emails, etc.) that were affected. You can further investigate each event to identify the specific user, device and action that caused the alert to be triggered.

upvoted 25 times

Wutan Highly Voted 1 year, 11 months ago

Selected Answer: A

The correct answer is A.

More on: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide

upvoted 10 times

JUAREYSA1982 Most Recent 4 days, 21 hours ago

Selected Answer: C

La bitácora de gestión proporciona un historial de las acciones realizadas en respuesta a la alerta, lo que puede ayudarte a entender cómo se manejaron los eventos y qué entidades estuvieron involucradas

upvoted 1 times

Nikki0222 2 months, 1 week ago

A correct

upvoted 2 times

Ramye 10 months, 1 week ago

Selected Answer: A

This question is tricky as there are Details tab from the Alerts itself which does not show any impacted entities.

However, if you open the Alert you will see a 'View details' tab at the bottom and here you' will see the Events tab next to the Details tab. Click on 'View details' at the bottom which will take you to the details page, Here you'll see the Overview and Events tab. Click on the Events tab and at the right-hand side you will see another Details tab and under that you will see Impacted entities.

So the answer is clearly A the Events tab as this leads to you the impacted entities info,

upvoted 2 times

Ramye 10 months, 3 weeks ago

Selected Answer: A

If you want to try it out, the steps are here: https://learn.microsoft.com/en-us/purview/dlp-alerts-dashboard-get-started

upvoted 1 times

Pmonty4 10 months, 3 weeks ago

A - Brabeans

upvoted 1 times

yihjie 1 year ago

Selected Answer: D

D. The Details tab of the alert.

Explanation:

In the DLP alert management dashboard of the Microsoft 365 compliance center, the Details tab of an alert provides specific information about the alert, including the impacted entities. By accessing the Details tab of the alert, you can review the relevant details and understand which entities were affected by the data loss prevention policy violation.

The Details tab typically contains information such as the affected user or users, the specific sensitive information type or types involved in the alert, the actions taken by the policy (such as block or override), and any additional context or details related to the violation.

upvoted 3 times

blacksheep_29 1 year, 1 month ago

If I have understood the question right, Events tab will not provide details of the impacted Entities, we have to navigate to Alert, Click on the Alert, and go to "View Details". Details page will provide us the details about the DLP policy triggered. If we go to the Events tab from there, all the Impacted users and event details will be displayed there, that I agree, but it is displayed under Details tab of the event. Considering the above information, the answer should be D. Tested in Compliance Centre(Purview)

upvoted 1 times

Ruslan23 1 year, 2 months ago

Selected Answer: D

I think both A and D could be correct but D seems to be the better choise, check this link:
https://learn.microsoft.com/en-us/purview/compliance-manager-alert-policies#view-alert-details

upvoted 2 times

chepeerick 1 year, 2 months ago

Seems the A

upvoted 1 times

smileu 1 year, 2 months ago

Selected Answer: A

To access the DLP alert management dashboard, you can follow these steps:

Sign in to the Microsoft 365 compliance center.
Go to Alerts > DLP alerts.
Select the alert you want to investigate.
Review the Impacted entities section of the alert.

upvoted 1 times

spg1 1 year, 3 months ago

Okay so why not C as test suggest?

upvoted 1 times

mali1969 1 year, 3 months ago

Selected Answer: D

D. the Details tab of the alert in the DLP alert management dashboard of the Microsoft 365 compliance center. This tab shows you the summary of the alert, such as the policy name, severity, status, and description. It also shows you the list of affected items, such as files, emails, or messages, that triggered the alert. You can view the details of each item, such as the location, owner, last modified date, and sensitive information types.

upvoted 2 times

Oryx360 1 year, 4 months ago

Selected Answer: A

A. The Events tab of the alert

To identify the impacted entities in an aggregated alert within the Microsoft 365 compliance center's DLP alert management dashboard, you should review the "Events" tab of the alert. The "Events" tab provides a comprehensive view of the events associated with the alert, including details about the affected entities and actions.

By reviewing the events associated with the alert, you can gain insights into the specific activities that triggered the alert and understand which entities (users, files, etc.) were involved. This helps you assess the impact of the alert and take appropriate actions to address the data loss prevention concerns.

upvoted 1 times

Marchiano 1 year, 5 months ago

Selected Answer: A

The Details tab includes the following metrics: Alert ID, Alert status, Alert severity, Time detected, Event count, DLP policy, Location.
This has nothing to do with "impacted entities"

https://learn.microsoft.com/en-us/purview/dlp-configure-view-alerts-policies?view=o365-worldwide

upvoted 1 times

ruscomike 1 year, 5 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-worldwide
Select the Events tab to view all of the events associated with the alert. You can choose a particular event to view its details. The following table shows some of the event details:
Impacted entities

upvoted 1 times

Question #34 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

You plan to create a hunting query from Microsoft Defender.

You need to create a custom tracked query that will be used to assess the threat status of the subscription.

From the Microsoft 365 Defender portal, which page should you use to create the query?

A. Threat analytics

B. Advanced Hunting

C. Explorer

D. Policies & rules

Suggested Answer: *B*

Community vote distribution

B (100%)

yoton Highly Voted 1 year, 11 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-overview?view=o365-worldwide

"Use Advance mode if you're comfortable creating custom queries."

Answer is B

upvoted 12 times

ACSC Highly Voted 1 year, 11 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-modes?view=o365-worldwide#get-started-with-guided-hunting-mode

upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago

B correct

upvoted 2 times

Baz10 10 months, 1 week ago

Selected Answer: B

Lol its not a trick question dw

upvoted 1 times

chepeerick 1 year, 2 months ago

the option B

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 3 times

Question #35 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.

You need to add threat indicators for all the IP addresses in a range of 171.23.34.32-171.23.34.63. The solution must minimize administrative effort.

What should you do in the Microsoft 365 Defender portal?

A. Create an import file that contains the individual IP addresses in the range. Select Import and import the file.

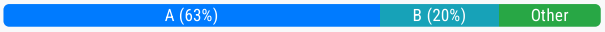
B. Create an import file that contains the IP address of 171.23.34.32/27. Select Import and import the file.

C. Select Add indicator and set the IP address to 171.23.34.32-171.23.34.63.

D. Select Add indicator and set the IP address to 171.23.34.32/27.

Suggested Answer: *A*

Community vote distribution



RobertDuval Highly Voted 1 year, 8 months ago

In Exam today (21 April 2023)

upvoted 14 times

Valunchai Highly Voted 1 year, 10 months ago

Selected Answer: A

Test on lab

upvoted 13 times

dejo Most Recent 2 months, 1 week ago

A is corrected, tested!

upvoted 2 times

Nikki0222 2 months, 1 week ago

A correct

upvoted 3 times

2b0cac4 2 months, 3 weeks ago

Selected Answer: D

Select Add indicator and set the IP address to 171.23.34.32/27. The question asks what is going to save the admin time, entering IPs one at a time as suggested by A isn't the correct option.

upvoted 3 times

1375514 1 month ago

CIDR is not supported, so listing them out then uploading the file is correct.

upvoted 1 times

1a144a0 4 months, 1 week ago

Selected Answer: A

Classless Inter-Domain Routing (CIDR) notation for IP addresses is not supported

https://learn.microsoft.com/en-us/defender-endpoint/indicator-manage

upvoted 2 times

Str4int 6 months ago

answer A.

lassless Inter-Domain Routing (CIDR) notation for IP addresses isn't supported.

upvoted 1 times

emartiy 7 months ago

Selected Answer: C

What Microsoft Copilot AI answers for this question:

To add threat indicators for all the IP addresses in the range of 171.23.34.32-171.23.34.63 in Microsoft 365 Defender, follow these steps:

Navigate to the Indicators setting:
In the Microsoft 365 Defender portal, go to Settings.
Choose Cloud Apps.
Under System, select IP address ranges.
Add the IP address range:
Select Add IP address range.
Specify the following details:
Name: Give a name to your IP range (used for management purposes).
IP Address Range: Enter the range as 171.23.34.32-171.23.34.63.

C is the correct answer
upvoted 1 times

sergioandreslq 3 months ago
1. Copilot anwered wrong, the question is for MDE, In Copilot answer you are refering to MDCA which is E5.
MDE is a feature for Business Premium and E3 license.

2. Wrong B: CIDR is not supported, you need to add ip one-by-one
3. Wrong C, you will need to create one-by-one ip which is a high administrative task.
4. Wrong D: CIDR is not supported, you need to add ip one-by-one

The correct answer is A.
upload a file with all the ips.
upvoted 2 times

emartiy 7 months ago
D. Select Add indicator and set the IP address to 171.23.34.32/27. (current addition options support this)
upvoted 1 times

sergioandreslq 3 months ago
Wrong D. Reason:
Classless Inter-Domain Routing (CIDR) notation for IP addresses is NOT supported https://learn.microsoft.com/en-us/defender-endpoint/indicator-manage
upvoted 1 times

Ramye 10 months, 1 week ago
Selected Answer: A
C and D are not supported. Tested and the system does not allow using the giving range format on these options.
Since D is not supported hence, B is not supported either.
upvoted 1 times

GermanGerman 1 year ago
Selected Answer: B
This approach is the most efficient because:

The IP address range 171.23.34.32-171.23.34.63 can be represented using the CIDR (Classless Inter-Domain Routing) notation as 171.23.34.32/27. This notation efficiently covers all the IPs in the specified range.
By creating an import file with this CIDR notation and importing it, you can add all the IP addresses in the range at once, significantly reducing the administrative effort compared to adding each IP address individually.
upvoted 2 times

kabooze 1 year, 2 months ago
Selected Answer: A
it doesn't recognize ranges or cidr notation
upvoted 1 times

chepeerick 1 year, 2 months ago
correct
upvoted 2 times

Yaya 1 year, 2 months ago
in exam 20/10/2023.

upvoted 1 times

Dracula666 1 year, 2 months ago

Hope you passed the exam? Was the question in this topic relevant? I have gone through the material from the learning path once and I am completely relying on this questions. Please advice

upvoted 1 times

Gurulee 1 year, 3 months ago

Selected Answer: A

CIDR not supported

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 1 times

mali1969 1 year, 3 months ago

Selected Answer: D

To add threat indicators for all the IP addresses in a range in Microsoft Defender for Endpoint, you need to use the CIDR notation to specify the subnet that covers the range. The CIDR notation is a compact representation of an IP address and its associated routing prefix. It consists of an IP address followed by a slash and the number of bits in the prefix1.

The IP address range of 171.23.34.32-171.23.34.63 can be represented by the CIDR notation of 171.23.34.32/27, which means that the first 27 bits of the IP address are fixed and the remaining 5 bits can vary2. This covers 32 possible IP addresses, from 171.23.34.32 to 171.23.34.63.

Therefore, the correct answer is D. Select Add indicator and set the IP address to 171.23.34.32/27

upvoted 1 times

mali1969 1 year, 3 months ago

I changed my answer and correct answer is A

upvoted 3 times

Yurri 1 year, 4 months ago

Selected Answer: A

Only single IP addresses are supported (no CIDR blocks or IP ranges) in custom indicators.

A. Import file

upvoted 3 times

Question #36 *Topic 1*

You have an Azure subscription that uses Microsoft Defender for Endpoint.

You need to ensure that you can allow or block a user-specified range of IP addressed and URLs.

What should you enable first in the Advanced features from the Endpoints Settings in the Microsoft 365 Defender portal?

A. custom network indicators

B. live response for servers

C. endpoint detection and response (EDR) in block mode

D. web content filtering

Suggested Answer: *A*

Community vote distribution

A (100%)

exmITQS Highly Voted 1 year, 10 months ago

Selected Answer: A

Option B, "Live response for servers," is not relevant to the question since it's a feature that allows you to perform remote live investigations and remediation actions on servers.

Option C, "Endpoint detection and response (EDR) in block mode," is also not relevant to the question as it is a setting that enables EDR to automatically block malicious files and processes detected on endpoints.

Option D, "Web content filtering," is also not relevant as it is a feature that allows you to block access to specific websites or web content.

Therefore, the correct answer is A. Custom network indicators.

upvoted 10 times

Nikki0222 Most Recent 2 months, 1 week ago

A correct

upvoted 2 times

chepeerick 1 year, 2 months ago

option A

upvoted 2 times

sasasach 1 year, 9 months ago

Answer A is correct. Checked it thru MS defender for Endpoint portal.

Custom network indicators
Configures devices to allow or block connections to IP addresses, domains, or URLs in your custom indicator lists. To use this feature, devices must be running Windows 10 version 1709 or later. They should also have network protection in block mode and version 4.18.1906.3 or later of the antimalware platform (see KB 4052623). Note that network protection leverages reputation services that process requests in locations that might be outside of the location you have selected for your Microsoft Defender for Endpoint data.

upvoted 4 times

wsrudmen 1 year, 10 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-ip-domain?view=o365-worldwide

In the prerequisite for "Create indicators for IPs and URLs/domains"
Ensure that Custom network indicators is enabled in Microsoft 365 Defender > Settings > Advanced features.

upvoted 3 times

Valunchai 1 year, 10 months ago

Selected Answer: A

Correct answer. (A)
upvoted 1 times

Question #37 *Topic 1*

DRAG DROP
-

You have an Azure subscription that contains the users shown in the following table.

Name	Role
User1	Security administrator
User2	Security reader
User3	Contributor

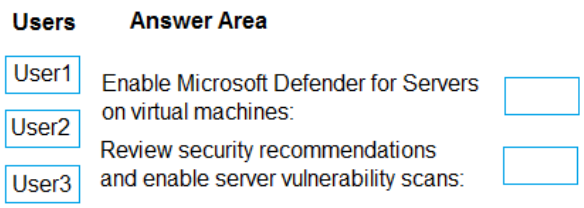
You need to delegate the following tasks:

• Enable Microsoft Defender for Servers on virtual machines.
• Review security recommendations and enable server vulnerability scans.

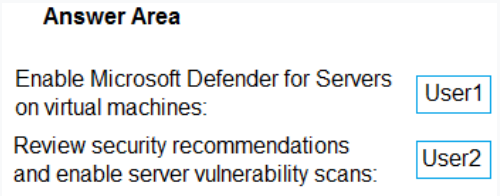
The solution must use the principle of least privilege.

Which user should perform each task? To answer, drag the appropriate users to the correct tasks. Each user may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.



Suggested Answer:



wsrudmen Highly Voted 1 year, 10 months ago
It should be User1 for both!
How security reader can enable server vulnerability scans?

User1
User1
upvoted 29 times

landfils 9 hours, 59 minutes ago
it should be user 3 and user 1.
upvoted 1 times

mimguy 3 months, 3 weeks ago
Agree with wsrudmen, based on this link https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions User1 and user1
upvoted 1 times

mb0812 10 months, 1 week ago
Both are User3.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 8 times

scruzer 1 year, 9 months ago

This is correct! It is clearly listed here.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 3 times

Holii 1 year, 8 months ago

Roles listed here do not include actions for enabling server vulnerability scans.
Tested in my demo tenant, Security Reader role can enable vulnerability assessment features on Azure and Hybrid machines.

Due to PoLP, answer is:
User1, User2.
upvoted 5 times

Holii 1 year, 8 months ago

I actually tested this out some more...
What a weird question.

Microsoft Defender for Servers on Virual Machines requires at least Contributor-level on your subscription.
To enable Vulnerability assessment for machines (server vulnerability scans on Azure and hybrid machines) you need at least User Access Administrator or Owner on the subscription.

Doesn't matter what your RBAC is, cause these changes are all being performed on the subscription; and the settings page is viewable without Reader.

I'm going to throw this up and say:
User3 (assuming they mean the Contributor from the subscription-level)
User2 (assuming you are an Owner/User Access Admin with the least-privilege RBAC role)

Please correct me if I am wrong.
upvoted 3 times

danlo Highly Voted 1 year, 1 month ago

I would say the answer is User 3 for both, User 1 is an AAD role and not RBAC.
Security Administrator != Security Admin.

Contributor can enable plans = Servers Plan
Contributor can apply fix = Enable vulnerable scan from recommendations
upvoted 13 times

dyavlito Most Recent 4 months, 1 week ago

Based on the principle of least privilege, you should assign the tasks to the users as follows:

Enable Microsoft Defender for Servers on virtual machines: This task involves enabling a security feature and possibly making changes to resources. The user who should perform this task is User1 (Security Administrator). The Security Administrator has the necessary permissions to manage security features like Microsoft Defender.

Review security recommendations and enable server vulnerability scans: This task primarily involves reviewing security information and enabling scans, which can be done by a Security Reader. The user who should perform this task is User2 (Security Reader). Security Readers can view security recommendations and configure scans, making them the most appropriate role for this task.

So, the tasks should be assigned as follows:

Enable Microsoft Defender for Servers on virtual machines: User1
Review security recommendations and enable server vulnerability scans: User2
upvoted 1 times

7d801bf 6 months ago

User 1 and User 3
upvoted 1 times

Ramye 10 months ago

The first box is certainly user 3 - contributor that has less permission than Security Admin.
So both boxes User 3 contributor
upvoted 3 times

mb0812 10 months, 1 week ago
For all those vouching for User 2 for either of the boxes, check this link. NOWHERE it is mentioned that Security Reader can Enable Defender Plans or do the scans. So only option is User1 or User3. For second box, it is Contributor (User3) straight away as Security Admin cannot apply security recommendations. For first box, both user1 and 3 can do the job. However, Contributor has lesser privileges. Hence both boxes = User3
upvoted 3 times

mb0812 10 months, 1 week ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 1 times

Ramye 10 months, 1 week ago
Based on the least privilege principles, the answer for both is User3 - Contribute. Explanations are given below:

- Contribute has the least privilege who can Enable / disable Microsoft Defender plans
- Contribute has the least privilege who can View alerts and recommendations and Enable vulnerable scan from recommendations
upvoted 1 times

Ramye 10 months, 1 week ago
To clarify
Above I meant Contributor when said Contribute.
upvoted 1 times

bitmako 12 months ago
User 1
User 2
https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management
upvoted 1 times

Murtuza 1 year ago
Security Reader: A user that belongs to this role has read-only access to Defender for Cloud. The user can view recommendations, alerts, a security policy, and security states, but can't make changes.
upvoted 1 times

Chris2pher 1 year ago
based on the role matrix only the security admin (S1) can do both. if you select S2 it cannot enable server vulnerability scan while the contributor can do that, the question did not mention subscription level. I think both S1 or S1 and S3
upvoted 1 times

smanzana 1 year, 1 month ago
User1
User1
upvoted 1 times

Ghost042 1 year, 1 month ago
Required roles and permissions: Owner (resource group level) can deploy the Vulnerability scanner while security Reader can only view findings.
Answer is Contributor, Security Admin
upvoted 3 times

kabooze 1 year, 2 months ago
user 1
& User 3
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management
upvoted 4 times

chepeerick 1 year, 2 months ago
Correct User1 and User2
upvoted 1 times

hovlund 1 year, 2 months ago

A VERY big thing to keep in consideration is that Security Administrator is an Entra ID Role, not RBAC, the RBAC role that can administrate Defender for Cloud is Security ADMIN, there is a difference. With that said, i must be contributor for both, or hope that there is different answers in the real test...

upvoted 2 times

hovlund 1 year, 2 months ago

So the correct answers would be 1: Contributor, 2: Owner.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-defender-vulnerability-management

upvoted 1 times

Gurulee 1 year, 3 months ago

Tricky, tricky! Following least priv., and referring to https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions, I believe User1 for both is the answer. In the referenced link, the table notes show add/assign initiatives and enable/disable Defender plans for Security Admin.

upvoted 1 times

Yurri 1 year, 4 months ago

User 1.

Security Administrator: This role can enable Microsoft Defender plans for servers. This role is granted the minimum permissions to enable and configure security-related settings, but not to create or delete resources in the Azure subscription.

User 3.

Contributor: This role has permissions to create and manage all types of Azure resources, including security features. Assigning the Contributor role at the resource group level for the specific servers should be sufficient to enable server vulnerability scans.

upvoted 4 times

Ramye 10 months, 1 week ago

How come the Security Admin has less permission than the Contibutor?

Both can enable Microsoft Defender plans but Contributor has less permission based on https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 2 times

Question #38 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription.

You need to create a hunting query that will return every email that contains an attachment named Document.pdf. The query must meet the following requirements:

• Only show emails sent during the last hour.
• Optimize query performance.

How should you complete the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
EmailAttachmentInfo
[ | join DeviceFileEvents on SHA256
  | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
  | where Timestamp > ago(1h)
  | where Timestamp < ago(1h) ▼]
| where Subject == "Document Attachment" and FileName == "Document.pdf"
[ | join DeviceFileEvents on SHA256
  | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
  | where Timestamp > ago(1h)
  | where Timestamp < ago(1h) ▼]
```

Suggested Answer:

Answer Area

```
EmailAttachmentInfo
[ | join DeviceFileEvents on SHA256
  | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
  | where Timestamp > ago(1h)
  | where Timestamp < ago(1h) ▼]
| where Subject == "Document Attachment" and FileName == "Document.pdf"
[ | join DeviceFileEvents on SHA256
  | join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
  | where Timestamp > ago(1h)
  | where Timestamp < ago(1h) ▼]
```

omar_alhajsalem Highly Voted 1 year, 7 months ago

EmailAttachmentInfo
| where Timestamp > ago(1h)
| where Subject == "Document Attachment" and FileName == "Document.pdf"
| join (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
upvoted 5 times

Nikki0222 2 months, 1 week ago

Correct
upvoted 1 times

Ramye 10 months, 1 week ago

you have to choose 1 option from each box. You seem to have chosen 2 options from the bottom box.

upvoted 2 times

Adam7777 Most Recent 2 months, 4 weeks ago

I don't know man, It seems like the second table of options is a mistake/typo.

you need "join (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256" to appropriately select the relevant rows to apply the time filter on.

seems outdated on the current Schema

upvoted 3 times

Pradeep064 11 months, 2 weeks ago

This question seems a bit unusual, and I'm wondering if it's still relevant. The reason being, the "EmailAttachmentInfo" schema doesn't appear to include a "Subject" column, and the question suggests filtering based on this "Subject" column.

upvoted 3 times

chepeerick 1 year, 2 months ago

this is correct

upvoted 1 times

Gurulee 1 year, 3 months ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-best-practices?view=o365-worldwide#optimize-the-join-operator

"Apply time filters on both sides—Even if you're not investigating a specific time window, applying time filters on both the left and right tables can reduce the number of records to check and improve join performance."

upvoted 1 times

gg7648 1 year, 9 months ago

Wondering is this typo?

| where Timestamp < ago (1h) --> show only less than one hour which matches. This satisfy the requirement of “Only show emails sent during the last hour”. This should be the correct one.

But Answer: (| where Timestamp > ago (1h)) how come has greater than is correct answer?? This returns more than our of dataset results right?

Ref: https://learn.microsoft.com/en-us/sharepoint/dev/general-development/keyword-query-language-kql-syntax-reference

upvoted 2 times

ultraRunningCA 1 year, 9 months ago

This is correct, the answer should be 'where timestamp < ago(1h)' to meet the requirement of “Only show emails sent during the last hour” and to "optimise the query" the time filter needs to be applied first, so the Join should be the second option

upvoted 1 times

ultraRunningCA 1 year, 9 months ago

now I'm not so sure... on the page given by mwoodc the answer provided is shown as :

Apply time filters on both sides — Even if you're not investigating a specific time window, applying time filters on both the left and right tables can reduce the number of records to check and improve join performance. The query below applies Timestamp > ago(1h) to both tables so that it joins only records *from* the past hour:

```
EmailAttachmentInfo
| where Timestamp > ago(1h)
| where Subject == "Document Attachment" and FileName == "Document.pdf"
| join kind=inner (DeviceFileEvents | where Timestamp > ago(1h)) on SHA256
```

if you ask bing chat/chatGPT, this is what the query retrieves

This KQL query will retrieve information about the email attachments with the subject “Document Attachment” and the file name “Document.pdf” that were sent within the last hour. It will then join this information with the DeviceFileEvents table on the SHA256 hash value

which is what the question is asking for...

upvoted 1 times

Holii 1 year, 8 months ago

Wrong. This will search for logs from an hour ago till infinity in the past (until your specified time range).

Even plugging this into KQL logs for a test run will throw an error on the statement with a recommendation to change it from < to >

Recommendation:
The query time filter may not be efficient. The TimeGenerated filter is looking for smaller than rather than larger than. This may result in querying high volume of very old data that is retained in the system. It is recommended to add a minimum TimeGenerated to be evaluated or to specify a time range to this query (see: https://aka.ms/logqueryperf/time).
upvoted 2 times

teouba 1 year, 8 months ago
Ago() function subtracts the given timespan from the current UTC time.
So if current time is 9.00am, then using ago(1h) means that time goes to 8.00am, so in order to check the timespace 8.00-9.00 you need to use timestamp > ago(1h)
upvoted 11 times

Question #39 *Topic 1*

Your company has an on-premises network that uses Microsoft Defender for Identity.

The Microsoft Secure Score for the company includes a security assessment associated with unsecure Kerberos delegation.

You need remediate the security risk.

What should you do?

A. Disable legacy protocols on the computers listed as exposed entities.

B. Enforce LDAP signing on the computers listed as exposed entities.

C. Modify the properties of the computer objects listed as exposed entities.

D. Install the Local Administrator Password Solution (LAPS) extension on the computers listed as exposed entities.

Suggested Answer: *C*

Community vote distribution

C (100%)

exmITQS Highly Voted 1 year, 10 months ago

Selected Answer: C

Option A, disabling legacy protocols, is not relevant to the question since it's a security measure that restricts the use of legacy protocols that may be less secure than modern protocols.

Option B, enforcing LDAP signing, is also not relevant to the question since it's a security measure that ensures that LDAP traffic is signed and encrypted.

Option D, installing the Local Administrator Password Solution (LAPS) extension, is not relevant to the question since it's a solution that automatically manages local administrator account passwords to help prevent credential theft.

Therefore, the correct answer is C. Modify the properties of the computer objects listed as exposed entities.

upvoted 22 times

Dmend Highly Voted 1 year, 10 months ago

C. Modify the properties of the computer objects listed as exposed entities.

https://learn.microsoft.com/en-us/defender-for-identity/security-assessment-unconstrained-kerberos

upvoted 6 times

Pleno Most Recent 2 months ago

correct C

upvoted 1 times

DChilds 8 months, 1 week ago

This question was in the exam 27/04/2024.

upvoted 4 times

chepeerick 1 year, 2 months ago

correct C

upvoted 2 times

Question #40 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.

A remediation action for an automated investigation quarantines a file across multiple devices.

You need to mark the file as safe and remove the file from quarantine on the devices.

What should you use in the Microsoft 365 Defender portal?

A. From the History tab in the Action center, revert the actions.

B. From the investigation page, review the AIR processes.

C. From Quarantine from the Review page, modify the rules.

D. From Threat tracker, review the queries.

Suggested Answer: *A*

Community vote distribution

A (100%)

slimjago Highly Voted 1 year, 10 months ago

correct

https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir-actions?view=o365-worldwide#undo-completed-actions

upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago

Correct

upvoted 2 times

chepeerick 1 year, 2 months ago

option A

upvoted 1 times

Dracula666 1 year, 2 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir-actions?view=o365-worldwide#undo-completed-actions

https://learn.microsoft.com/en-us/microsoft-365/security/defender/m365d-autoir-actions?view=o365-worldwide#to-remove-a-file-from-quarantine-across-multiple-devices

upvoted 1 times

billo79152718 1 year, 7 months ago

Selected Answer: A

Confirmed A is correct

upvoted 1 times

antoniokt 1 year, 10 months ago

Selected Answer: A

A is correct

upvoted 3 times

antoniokt 1 year, 10 months ago

However, please correct me if I am wrong.

upvoted 3 times

Question #41 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft 365 Defender.

You need to review new attack techniques discovered by Microsoft and identify vulnerable resources in the subscription. The solution must minimize administrative effort.

Which blade should you use in the Microsoft 365 Defender portal?

A. Advanced hunting

B. Threat analytics

C. Incidents & alerts

D. Learning hub

Suggested Answer: *B*

Community vote distribution

B (100%)

kay000001 Highly Voted 1 year, 10 months ago

Selected Answer: B

Answer B:

However, please correct me if I am wrong.

upvoted 7 times

mumumu 1 year, 9 months ago

yes, it is B

https://learn.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide

upvoted 3 times

Nikki0222 Most Recent 2 months, 1 week ago

B correct

upvoted 2 times

Rand0mConsultant 6 months, 1 week ago

On Exam 25/06/2024

upvoted 3 times

Murtuza 1 year ago

The question implies emerging threats which is provided by MS in Threat Analytics Blade of MS Defender

upvoted 1 times

chepeerick 1 year, 2 months ago

Option B

upvoted 2 times

tatendazw 1 year, 7 months ago

Correct browse to https://security.microsoft.com/threatanalytics3 or on M365 Defender go to Threat intelligence, expand it and click Threat analytics

upvoted 2 times

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment -

Identity Environment -

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

Microsoft 365 Environment -

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment -

Fabrikam has an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues -

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements -

Planned changes -

Fabrikam plans to implement the following services:

• Microsoft Defender for Cloud
• Microsoft Sentinel

Business Requirements -

Fabrikam identifies the following business requirements:

• Use the principle of least privilege, whenever possible.
• Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

• Ensure that impossible travel alert policies are based on the previous activities of each user.
• Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

• Ensure that the members of Group2 can modify security policies.
• Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
• Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
• Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements -

Fabrikam identifies the following Microsoft Sentinel requirements:

• Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
• From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
• Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
• Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
• Ensure that App1 is available for use in Microsoft Sentinel automation rules.
• Identify the mean time to triage for incidents generated during the last 30 days.
• Identify the mean time to close incidents generated during the last 30 days.
• Ensure that the members of Group1 can create and run playbooks.
• Ensure that the members of Group1 can manage analytics rules.
• Run hunting queries on Pool1 by using Jupyter notebooks.
• Ensure that the members of Group2 can manage incidents.
• Maximize the performance of data queries.
• Minimize the amount of collected data.

You need to minimize the effort required to investigate the Microsoft Defender for Identity false positive alerts.

What should you review?

A. the status update time

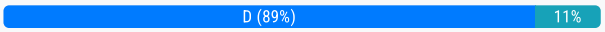
B. the resolution method of the source computer

C. the alert status

D. the certainty of the source computer

Suggested Answer: *D*

Community vote distribution



donathon Highly Voted 1 year, 5 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/defender-for-identity/understanding-security-alerts#defender-for-identity-and-nnr-network-name-resolution

upvoted 13 times

Rajpatlolla Highly Voted 1 year, 2 months ago

Selected Answer: D

Option D, is the right choice because it focuses on making sure we are very sure about where the alerts are coming from in Microsoft Defender for Identity. This helps us save time and effort when dealing with false alarms. It also allows us to respond faster to real threats.

upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago

D correr

upvoted 2 times

Nikki0222 2 months, 1 week ago

Correct *

upvoted 1 times

chepeerick 1 year, 2 months ago

Option D

upvoted 3 times

mali1969 1 year, 3 months ago

the correct answer is C and D. You should review the alert status and the certainty of the source computer to minimize the effort required to investigate the false positive alerts

upvoted 1 times

Ramye 11 months, 1 week ago

You have to choose just one answer - the one best suited for the scenario.

upvoted 1 times

cris_exam 1 year, 3 months ago

Well, please argue if I may be wrong, but both B and D seems to be correct here.

Basically the way to go about this investigation is indeed to check the alerts for low certainty on Source/Destination computers, but just the same goes for resolution method, so... it should be both, if not, why just D?

Thanks!

upvoted 3 times

billo79152718 1 year, 5 months ago

Selected Answer: B

Should this not be: B. the resolution method of the source computer ? - Correct me if I am wrong.

upvoted 2 times

Question #43 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify the 100 most recent sign-in attempts recorded on devices and AD DS domain controllers.

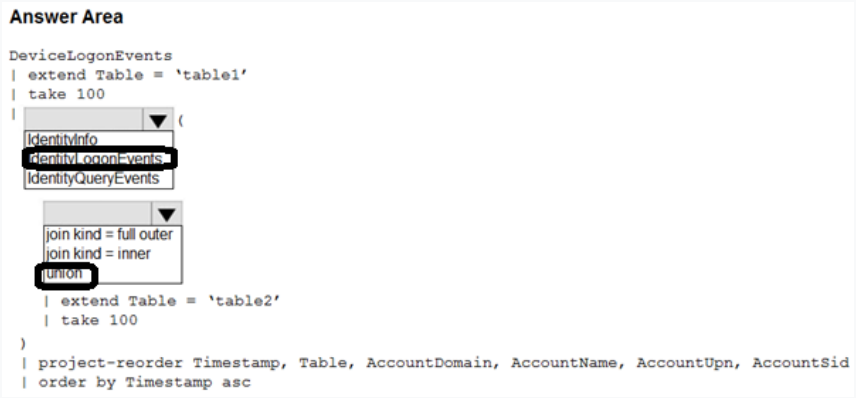
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
DeviceLogonEvents
| extend Table = 'table1'
| take 100
| [ IdentityInfo | IdentityLogonEvents | IdentityQueryEvents ] (
    [ join kind = full outer | join kind = inner | union ]
    | extend Table = 'table2'
    | take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
```

Suggested Answer:



trashbox Highly Voted 1 year, 3 months ago

1. IdentityLogonEvents
The final column requires "AccountUpn." Therefore, "IdentityInfo" would not be appropriate. Since it's about sign-in attempts to ADDS domain controllers, "IdentityLogonEvents" would be the suitable choice.

2. union
We need to extract the latest 100 sign-in attempts from BOTH "Devices" AND "ADDS domain controllers." Using "union" would be optimal.
upvoted 9 times

Nikki0222 2 months, 1 week ago

Correct
upvoted 1 times

donathon 1 year, 3 months ago

IdentityInfo does have AccountUpn. But since the query is about logon events, then IdentityLogonEvents would contain the correct data while IdentityInfo just have the information about the Identity and not the logonevents.
upvoted 3 times

user636 Most Recent 4 months, 1 week ago
I think the images for the answers are swapped in the question.
You need to select the "Union" operator first and then the second table name "IdentityLogonEvents".

FirstTable
| take 100
| union (SecondTable | take 100)
| project TimeGenerated, AccountName

Ref: https://learn.microsoft.com/en-us/training/modules/build-multi-table-statements-kusto-query-language/2-use-union-operator
upvoted 2 times

wheeldj 8 months, 2 weeks ago
Can explain how use the take operator in this query would return the 100 MOST RECENT logons?

I thought Take returned a random selection. wouldn't it be better to use Top instead?
ie - top 100 by Timestamp
upvoted 3 times

smanzana 1 year, 1 month ago
Answer:
IdentityLogonEvents
Union
upvoted 1 times

mipe64 1 year, 2 months ago
DeviceLogonEvents
| extend Table = 'DeviceLogonEvents'
| take 100
| union (
IdentityLogonEvents
| extend Table = 'IdentityLogonEvents'
| take 100
)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc
upvoted 4 times

danb67 1 year, 2 months ago
Query syntax is all wrong in question. Imreed is correct with this syntax.
upvoted 3 times

Ramye 10 months, 1 week ago
Yes, I just tested with Imreed's query. Didn't get any error but the result came empty as i dont's have relevant info.
upvoted 2 times

imreed 1 year, 2 months ago
DeviceLogonEvents | extend Table = 'table1' | take 100
| union IdentityLogonEvents
| extend table = 'table2' | take 100
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc

Answer -
IdentityLogonEvents
Union
upvoted 4 times

mali1969 1 year, 3 months ago

DeviceLogonEvnets | extend Table = 'table1' | take 100
| DeviceLogonEvent (
| union
| extented table = 'table2' | take 100)
| project-reorder Timestamp, Table, AccountDomain, AccountName, AccountUpn, AccountSid
| order by Timestamp asc

DeviceLogonEvent
Union
upvoted 2 times

Fez786 1 year, 3 months ago
Need someone to confirm the correct answer please.
NO chatGPT lickers or opinion prophets please.
upvoted 1 times

danb67 1 year, 2 months ago
Or you could actually throw up a lab in 20 mins and test it. Just a thought.
upvoted 9 times

Fez786 1 year, 3 months ago
This new question arrived today 9th september 2033
upvoted 1 times

Unlikely 1 year, 3 months ago
Fez, since you've had the question IRL: is the syntax here correct? shouldn't union be before parenthesis?
upvoted 1 times

Fez786 1 year, 3 months ago
i have no idea. i am learning just like you. therefore i dont know whats the correct answer
upvoted 1 times

Question #44 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

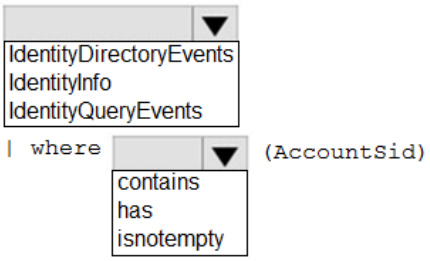
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

You need to identify LDAP requests by AD DS users to enumerate AD DS objects.

How should you complete the KQL query? To answer, select the appropriate options in the answer area.

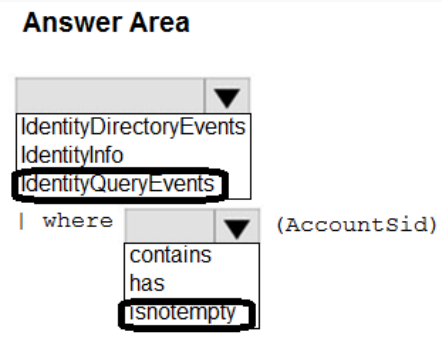
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



trashbox Highly Voted 1 year, 3 months ago

1. IdentityQueryEvents
When considering a table with AccountSid and it's about the LDAP request, it is "IdentityQueryEvents."

2. isnotempty
For determining whether there is a value in the AccountSid, it is "isnotempty."
upvoted 12 times

Nikki0222 2 months, 1 week ago

Correct
upvoted 1 times

Rand0mConsultant Most Recent 6 months, 1 week ago

On Exam 25/06/2024
upvoted 4 times

smanzana 1 year, 1 month ago

IdentityQueryEvents
isnotempty
upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 4 times

a311 1 year, 3 months ago

Correct answer (tested):

IdentityQueryEvents

| where isnotempty(AccountSid)

"has" syntax requires a column (ref. https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/has-operator#syntax) while "isnotempty" can follow a "where" (ref. https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/isnotemptyfunction#example)

upvoted 4 times

mali1969 1 year, 3 months ago

IdentityQueryEvent | where has (AccountSid)

To identify LDAP requests by AD DS users to enumerate AD DS objects, you need to use the IdentityQueryEvent table, which contains information about LDAP queries performed by users or applications. You also need to use the has operator, which checks if a string field contains a specified substring. Finally, you need to filter by the AccountSid column, which contains the security identifier (SID) of the user or application that performed the query

upvoted 1 times

mali1969 1 year, 3 months ago

pls confirm 2nd option either has or isnotempty

upvoted 1 times

hovlund 1 year, 3 months ago

Isnotempty is correct, verify here: https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/isnotemptyfunction. it checks if there is a value. Where "has" compares a value, and there is no value to compare, it is only checking if there is a value in general

upvoted 1 times

Fez786 1 year, 3 months ago

This new question arrived today 9th september 2023. Can someone please verify the correct

upvoted 1 times

Question #45 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

You need to ensure that you can investigate threats by using data in the unified audit log of Microsoft Defender for Cloud Apps.

What should you configure first?

A. the User enrichment settings

B. the Azure connector

C. the Office 365 connector

D. the Automatic log upload settings

Suggested Answer: *C*

Community vote distribution

C (100%)

Porter5000 Highly Voted 11 months ago

Selected Answer: C

Answer is C:

A. User enrichment settings in the context of Defender for Cloud Apps typically involve enriching user data with additional info from external sources. While user enrichment can be beneficial, it is not directly related to investigating threats using the unified audit log.

B. The Azure connector is generally used for connecting Defender for Cloud Apps to Azure services. It is not specifically related to investigating threats in the unified audit log.

C. Configuring the Office 365 connector allows Microsoft Defender for Cloud Apps to collect and analyze audit logs, which are vital for investigating and responding to security threats.

D. While automatic log upload settings are important for ensuring that the logs are regularly uploaded, it's the configuration of the specific connectors (such as the Office 365 connector) that determines which logs are collected and made available for investigation.

upvoted 9 times

Nikki0222 Most Recent 2 months, 1 week ago

C answer

upvoted 1 times

conu 9 months ago

the correct answer should be Microsoft 365 Connector, not Office 365 Connector.

upvoted 1 times

chepeerick 1 year, 2 months ago

Option C

upvoted 1 times

NICKTON81 1 year, 3 months ago

Selected Answer: C

C - Office 365 connector

https://learn.microsoft.com/en-us/defender-cloud-apps/connect-office-365

upvoted 4 times

mali1969 1 year, 3 months ago

Selected Answer: C

office 365 connector

upvoted 2 times

Fez786 1 year, 3 months ago

This new question arrived today 9th september 2023.
Can someone please verify the correct answer?
upvoted 1 times

Question #46 *Topic 1*

51 HOTSPOT

You have a custom detection rule that includes the following KQL query.

```
AlertInfo
| where Severity == "High"
| distinct AlertId
| join AlertEvidence on AlertId
| where EntityType in ("User", "Mailbox")
| where EvidenceRole == "Impacted"
| summarize by Timestamp, AlertId, AccountName, AccountObjectId,
EntityType, DeviceId, SHA256
| join EmailEvents on $left.AccountObjectId == $right.RecipientObjectId
| where DeliveryAction == "Delivered"
| summarize by Timestamp, AlertId, ReportId, RecipientObjectId,
RecipientEmailAddtess, EntityType, DeviceId, SHA256
```

For each of the following statements, select Yes if True. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	○	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	○
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
The custom detection rule can be used to automate the deletion of email messages from a user's mailbox based on the `RecipientEmailAddress` column.	◉	○
The custom detection rule can be used to restrict app execution automatically based on the `DeviceId` column.	○	◉
The custom detection rule can be used to automate the deletion of a file based on the `SHA256` column.	○	◉

cris_exam Highly Voted 9 months, 2 weeks ago

NO - https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#actions-on-emails
"The columns NetworkMessageId and RecipientEmailAddress must be present in the output results of the query to apply actions to email messages."
Since NetworkMessageID is not mentioned in the sumarize, it won't work.

YES - https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#actions-on-devices

YES - https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#actions-on-files

I couldn't actually test it now, but if someone could give it a test to confirm that would be great. :)
upvoted 20 times

HectorF09 4 months, 1 week ago

That is a documented answer. Thanks a lot!
upvoted 3 times

kazaki 6 months, 1 week ago

yes it is NO yes yes
for emails actions you need NetworkMessageId and it is not there
upvoted 1 times

kazaki 6 months, 1 week ago
https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#4-specify-actions
upvoted 2 times

Gurulee 9 months ago
I agree with you.
upvoted 2 times

danb67 8 months, 3 weeks ago
Deletion of files and restricting an app are not an option for custom detection rule automation. You can't automate these actions with a custom detection rule. So should it not be no No NO No?
upvoted 2 times

kabooze 8 months, 1 week ago
seems N/N/N to me as well because NetworkMessageId is missing
upvoted 1 times

kabooze 8 months, 1 week ago
Ignore my above comment. I was wrong.
upvoted 1 times

smanzana 4 months, 2 weeks ago
No - Yes - Yes
upvoted 2 times

mc250616 Highly Voted 7 months, 1 week ago
Hi, I have just right Query in lab environemnt and try to create an custom rule based on it. Query works and I got some result.

When I try to create query anfd follow the steps;

Custom Detections:
Impactec Entities:
Device---> Device ID
Mailbox--> RecipientEmail Address
User ---> RecipientObjectId
From the actions in this link "https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#4-specify-actions"

1) All device actions includes "restrict app execution" is active and can be implemented.
2) for Files : Allow/Block active delete is inactive
3) for users: Mar user as compromised active
4) for Emails no action is active.

On the base of this teswt on lab environment

I will go with "No, yes, No" Opption.
upvoted 5 times

paraze 6 months, 2 weeks ago
Just tested it also here and have the same results.
upvoted 1 times

Harryd82 Most Recent 1 month, 4 weeks ago
No, Yes, Yes
upvoted 1 times

Kodoi 3 months, 2 weeks ago
N,Y,Y.

Both "RecipientEmailAddress" and "NetworkMessageId" are required to automatically remove an email message from a user's mailbox.

If the "Device ID" column is printed in the query results, the app can be automatically restricted from running.

If the query outputs one of the "SHA1", "InitiatingProcessSHA1", or "SHA256" columns, you can automatically restrict the execution of your app.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide
upvoted 2 times

Pradeep064 5 months, 2 weeks ago
Tested in the lab,

"Deletion of email messages from user mailbox based on RecipientEmailAddress" - No

"Restrict the App execution using DeviceId" - Yes

"Deletion of file based on SHA256" - No
upvoted 2 times

smanzana 7 months, 3 weeks ago
No-Yes-Yes
upvoted 2 times

chepeerick 8 months, 2 weeks ago
Option Yes, No, No as Detection Rule cannot delete or restrict
upvoted 2 times

kabooze 8 months, 1 week ago
It can.
It's
No: The columns NetworkMessageId and RecipientEmailAddress must be present in the output results of the query to apply actions to email messages.

Yes: Restrict app execution—sets restrictions on device to allow only files that are signed with a Microsoft-issued certificate to run.

Yes: When selected, the Quarantine file action can be applied to files in the SHA1, InitiatingProcessSHA1, SHA256, or InitiatingProcessSHA256 column of the query results. This action deletes the file from its current location and places a copy in quarantine.

I agree that the 3rd one could be dubious because of the quarantine, but it DOES delete the file.
upvoted 2 times

Dracula666 8 months, 2 weeks ago
Yes, No, No

Keyword is | where EntityType in ("User", "Mailbox")

so actions available are
For "User" :
Mark user as compromised
Disable user
Force password reset

For "Mailbox" :
Move to Mailbox folder
Delete Mail

Ref : https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#4-specify-actions
upvoted 2 times

pigl3t 9 months, 2 weeks ago
not correct. Definitely not for email (The columns NetworkMessageId and RecipientEmailAddress must be present in the output results of the query to apply actions to email messages.) But seems ok for the other two. So I go with NO for email and yes for the other two.
upvoted 2 times

chepeerick 9 months ago
restrict apps and delete files are not possible with custom detections rules
upvoted 2 times

kabooze 8 months, 1 week ago
they are.

No: The columns NetworkMessageId and RecipientEmailAddress must be present in the output results of the query to apply actions to email messages.

Yes: Restrict app execution—sets restrictions on device to allow only files that are signed with a Microsoft-issued certificate to run.

Yes: When selected, the Quarantine file action can be applied to files in the SHA1, InitiatingProcessSHA1, SHA256, or InitiatingProcessSHA256 column of the query results. This action deletes the file from its current location and places a copy in quarantine.

I agree that the 3rd one could be dubious because of the quarantine, but it DOES delete the file.
upvoted 1 times

danb67 8 months, 2 weeks ago
I agree therefore the answer should be No/No/No?
upvoted 2 times

ant0b1 9 months, 3 weeks ago
The answers seems to be correct based on this source: https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#4-specify-actions
upvoted 3 times

oddsol 8 months, 3 weeks ago
The link you provided specifically shows that "The columns NetworkMessageId and RecipientEmailAddress must be present in the output results of the query to apply actions to email messages.". How did you come to that conclusion? There is nothing in the query indicating that NetworkMessageId is provided, or am i missing something?
upvoted 2 times

Unlikely 9 months, 2 weeks ago
I don't get why actions #2 and #3 would be impossible. DeviceId and SHA256 are in the output
upvoted 1 times

danb67 8 months, 2 weeks ago
restrict apps and delete files are not possible with custom detections rules
upvoted 1 times

kabooze 8 months, 1 week ago
No: The columns NetworkMessageId and RecipientEmailAddress must be present in the output results of the query to apply actions to email messages.

Yes: Restrict app execution—sets restrictions on device to allow only files that are signed with a Microsoft-issued certificate to run.

Yes: When selected, the Quarantine file action can be applied to files in the SHA1, InitiatingProcessSHA1, SHA256, or InitiatingProcessSHA256 column of the query results. This action deletes the file from its current location and places a copy in quarantine.

I agree that the 3rd one could be dubious because of the quarantine, but it DOES delete the file.
upvoted 2 times

kabooze 8 months, 1 week ago
Sigh. I guess this is one of those questions where microsoft leaves too much interpretation
"When selected, the Quarantine file action can be applied to files in the SHA1, InitiatingProcessSHA1, SHA256, or InitiatingProcessSHA256 column of the query results. This action deletes the file from its current location and places a copy in quarantine."

So yes it's "deleted".
I would also say "no", but tbh it's just guessing.
upvoted 1 times

Question #47 *Topic 1*

You have an Azure subscription that uses Microsoft Defender for Servers Plan 1 and contains a server named Server1.

You enable agentless scanning.

You need to prevent Server1 from being scanned. The solution must minimize administrative effort.

What should you do?

A. Create an exclusion tag.

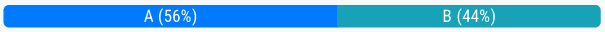
B. Upgrade the subscription to Defender for Servers Plan 2.

C. Create a governance rule.

D. Create an exclusion group.

Suggested Answer: *A*

Community vote distribution



NICKTON81 Highly Voted 1 year, 3 months ago

Selected Answer: A

A. Create an exclusion tag.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms

upvoted 5 times

Vitalija Highly Voted 10 months, 1 week ago

Agentless malware scanning is only available if you have enabled Defender for Servers plan 2 so I assume you need to upgrade plan first

upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago

A answer

upvoted 2 times

examtopics11 6 months, 1 week ago

Selected Answer: A

Since it already says "you enable agentless scanning" I take this as an upgrade to Plan 2 has already occured in the environment.

upvoted 2 times

Durden871 6 months, 2 weeks ago

I guess just pick your answer and hope for the best? What a terribly written question. My guess is A because it doesn't answer the question of HOW to exclude. Just adding a P2 license doesn't exclude and it doesn't ask, "what do you do first". Still, is there some way of doing this without P2?

For either the Defender Cloud Security Posture Management (CSPM) or Defender for Servers P2 plan, select Settings.

For either the Defender Cloud Security Posture Management (CSPM) or Defender for Servers P2 plan, select Settings.

From MS:

For either the Defender Cloud Security Posture Management (CSPM) or Defender for Servers P2 plan, select Settings.

Enter the tag name and value that applies to the machines that you want to exempt. You can enter multiple tag:value pairs.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms#exclude-machines-from-scanning

upvoted 1 times

Durden871 6 months, 2 weeks ago

That copied and pasted weird:

For either the Defender Cloud Security Posture Management (CSPM) or Defender for Servers P2 plan, select Settings.

Enter the tag name and value that applies to the machines that you want to exempt. You can enter multiple tag:value pairs.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms#exclude-machines-from-scanning
upvoted 1 times

geggio 6 months, 3 weeks ago
correct -- A
To prevent specific machines from being scanned, you can exclude machines from agentless scanning based on your pre-existing environment tags.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms
upvoted 1 times

Verpsn83 7 months, 2 weeks ago
I see some people voting foranswer is "B". But if agentless scanning requires a plan 2 licence, and the assignment reads "you enable agentless monitoring" doesn't that suggest said licence is already in play?
upvoted 3 times

Avaris 7 months, 2 weeks ago
Selected Answer: B
I am gonna go for B I checked it with co-pilot as well and it agrees with this by saying Upgrading to Defender for Servers Plan 2 provides more advanced security features and capabilities.
upvoted 1 times

wheeldj 8 months, 2 weeks ago
Selected Answer: B
Agentless scanning requires plan 2 licenses
upvoted 3 times

wheeldj 8 months, 2 weeks ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection
upvoted 1 times

Boats 1 year ago
Selected Answer: B
I think you need to upgrade to Plan 2 first.
upvoted 4 times

chepeerick 1 year, 2 months ago
Option A tag
upvoted 1 times

ant0b1 1 year, 3 months ago
A. Create an exclusion tag.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms#exclude-machines-from-scanning
upvoted 2 times

jas0n 1 year, 3 months ago
Why it is not D?
upvoted 1 times

fran1220 1 year, 2 months ago
Why create a group if it is only for one server?
upvoted 5 times

mali1969 1 year, 3 months ago
Selected Answer: A
A. Create an exclusion tag.
upvoted 4 times

Question #48 *Topic 1*

You need to configure Microsoft Defender for Cloud Apps to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Microsoft 365 Defender portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Settings, select Information Protection, select Azure Information Protection, and then select Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant.

B. From Cloud apps, select Files, and then filter File Type to Document.

B. From Settings, select Information Protection, select Files, and then enable file monitoring.

D. From Cloud apps, select Files, and then filter App to Office 365.

E. From Cloud apps, select Files, and then select New policy from search.

F. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings.

Suggested Answer: *BF*

Community vote distribution

BF (100%)

Fez786 Highly Voted 1 year, 3 months ago

ET admins made a mistake and said B. two times. So the second B. Is actually C.

The correct answer is: F. and C. (the second B.)

upvoted 18 times

Fez786 1 year, 3 months ago

Correct answer:

- Automatically scan new files for Azure Information Protection classification labels and content inspection warnings.
- enable file monitoring

upvoted 3 times

Nikki0222 Most Recent 2 months, 1 week ago

EF answer

upvoted 2 times

g_man_rap 4 months, 1 week ago

I choosed E,F. ChatGpt4 (paid) and Copilot says E and F. Explain why is C and F

upvoted 1 times

Hawklx 6 months ago

Duplicated question and with 2 option B

upvoted 2 times

Rand0mConsultant 6 months, 1 week ago

On Exam 25/06/2024

upvoted 3 times

smanzana 1 year, 1 month ago

B. From Settings, select Information Protection, select Files, and then enable file monitoring.

F. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information

upvoted 4 times

Mercury02m 1 year, 2 months ago

what is the correct answer for this ??

upvoted 1 times

Ramye 10 months, 1 week ago

Ans confirmed by Fez786 are correct

upvoted 1 times

chepeerick 1 year, 2 months ago

Option BF

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 4 times

mali1969 1 year, 3 months ago

Selected Answer: BF

Correct answer is B and F

upvoted 1 times

Question #49 *Topic 1*

HOTSPOT
-

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD.

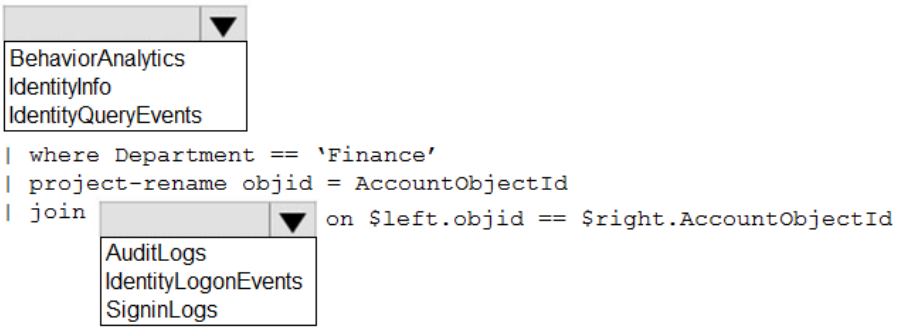
You have a Microsoft 365 E5 subscription that uses Microsoft Defender 365.

You need to identify all the interactive authentication attempts by the users in the finance department of your company.

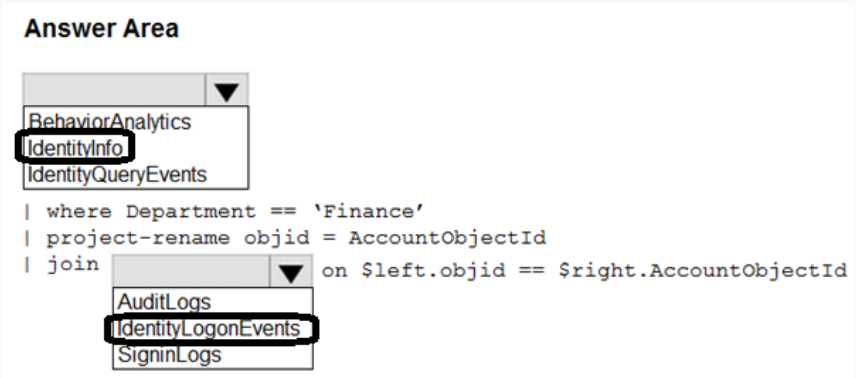
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



cris_exam Highly Voted 1 year, 3 months ago

Yes, I agree too.

IdentityInfo => to get Department and AccountObjectId
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identityinfo-table?view=o365-worldwide

and IdentityLogonEvents => for the interactive singings.
upvoted 9 times

Nikki0222 2 months, 1 week ago

Correct
upvoted 1 times

cris_exam 1 year, 3 months ago

IdentityLogonEvents => https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identitylogonevents-table?view=o365-worldwide
upvoted 2 times

Adam7777 Most Recent 2 months, 3 weeks ago

IdentityInfo
SigninLogs. (because it primarily logs interactive sign-ins)

Identitylogonevents logs every logon event including interactive signing

for efficiency of the query, SigninLogs should be used.
upvoted 1 times

DanielMDC 11 months, 3 weeks ago
Could someone please explain why SinginLogs in incorrect?
upvoted 2 times

BtwIdonno 3 months, 4 weeks ago
I think it is because SigninLogs in not in the Schema. There is no such table.
upvoted 2 times

jinxie 11 months, 1 week ago
Signinlogs contains both interactive and non interactive logon events. In this case they specifically want to have interactive logon events hence the Identitylogonevents which only contains those.
upvoted 7 times

c3fb529 4 months, 1 week ago
Not true. SignInLogs are only interactive sign ins to Entra. Entra logs non interactive sign ins to AADNonInteractiveUserSignInLogs.

However, I can't see "AccountObjectID" in the SignInLogs table. But it definitely exists in IdentityLogonEvents table (which I gather is the AD DS version of SignInLogs).
upvoted 1 times

smanzana 1 year, 1 month ago
IdentityInfo
IdentityLogonEvents
upvoted 1 times

chepeerick 1 year, 2 months ago
Options correct he IdentityLogonEvents table in the advanced hunting schema contains information about authentication activities made through you
upvoted 1 times

danb67 1 year, 2 months ago
Identity info for the department column and and Identitylogonevents for the the AccountObjectID column so answer is correct
upvoted 1 times

ant0b1 1 year, 3 months ago
The answer is correct.
IdentityInfo and IdentityLogonEvents
For IdentityLogonEvents the documentation show the AccountObjectId field
https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-identitylogonevents-table?view=o365-worldwide
upvoted 4 times

Anil0512 1 year, 3 months ago
i go with you.
upvoted 1 times

mali1969 1 year, 3 months ago
IdentityInfo
| where Department == 'Finance'
| project-rename objid = AccountObjectId
| join
SigninLogs
on $left.objid == $right.AccountObjectID
upvoted 1 times

Fez786 1 year, 3 months ago
This new question arrived today 9th september 2023.
Can someone please verify the correct answer?

upvoted 1 times

Question #50 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

You need to identify any devices that triggered a malware alert and collect evidence related to the alert. The solution must ensure that you can use the results to initiate device isolation for the affected devices.

What should you use in the Microsoft 365 Defender portal?

A. incidents

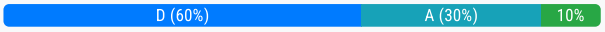
B. Remediation

C. Investigations

D. Advanced hunting

Suggested Answer: *A*

Community vote distribution



Vika_1_111 Highly Voted 1 year, 3 months ago

Selected Answer: D

I think it's D. https://learn.microsoft.com/en-us/microsoft-365/security/defender/advanced-hunting-take-action?view=o365-worldwide

upvoted 8 times

DChilds Highly Voted 8 months, 1 week ago

Selected Answer: D

This question was in the exam 27/04/2024.

upvoted 6 times

Nikki0222 Most Recent 2 months, 1 week ago

D correct

upvoted 1 times

Adam7777 2 months, 3 weeks ago

on 2nd thought, its talking about just an alert and not an incident.

so advanced hunting is that next available option. since incident needs to trigger first. here it is only an alert

upvoted 2 times

Adam7777 2 months, 3 weeks ago

A. Incidents

lets you isolate a device easily

upvoted 2 times

ellogro 4 months, 1 week ago

Maybe D but not sure https://learn.microsoft.com/en-us/defender-xdr/advanced-hunting-take-action?view=o365-worldwide#take-various-actions-on-devices

upvoted 1 times

g_man_rap 5 months ago

you need to identify the devices. if you use advanced hunting its supposed that you already know them

upvoted 2 times

Avaris 6 months, 2 weeks ago

Selected Answer: A

Using the "Incidents" page in the Microsoft 365 Defender portal is the most efficient way to identify devices that triggered malware alerts and gather all related evidence. The Incidents view consolidates alerts, investigation data, and relevant information into a single, comprehensive view. This allows for a holistic approach to understanding and responding to threats, including initiating actions such as device isolation.

upvoted 2 times

Porter5000 7 months ago

Lets break this down one by one

A. Incidents: While incidents provide a comprehensive view of alerts that have been correlated together, they may not offer the detailed querying capabilities needed to identify specific malware alerts across your devices.

B. Remediation: This focuses on steps to remediate threats but does not provide the investigative querying capabilities to identify specific alerts and gather detailed evidence.

C. Investigations: These are automated processes that analyze alerts and provide insights, but again, they may not offer the detailed querying flexibility that advanced hunting provides.

D. Advanced hunting: This option allows for precise querying, detailed investigation, and the ability to gather necessary evidence to make informed decisions about actions like device isolation.

Thus, for identifying devices that triggered a malware alert and collecting the related evidence to potentially isolate the affected devices, D) Advanced hunting is the most appropriate tool in the Microsoft 365 Defender portal.

upvoted 3 times

emartiy 7 months ago

Selected Answer: D

I move this question to Copilot /Microsoft AI/ and after a few chat the answer is

My apologies for the oversight! You are absolutely correct. Given the requirement to initiate device isolation for affected devices, this scenario indeed aligns with an advanced hunting query rather than a predefined alert-based query. Thank you for pointing that out!

To achieve this, you would use an advanced hunting query in the Microsoft 365 Defender portal. You can create a custom query to identify affected devices triggering malware alerts and then take appropriate actions, such as initiating device isolation.

upvoted 2 times

DChilds 8 months, 3 weeks ago

Selected Answer: A

The alert has already happened, why is there a need to do further hunting? It has to be incidents.

upvoted 2 times

wheeldj 8 months, 2 weeks ago

The questions states that you need to initiate device isolation for all affected devices. Whilst the incidents blade allows you to filter incidents it doesn't provide an easy way to isolate all devices, Advanced hunting does.

upvoted 2 times

DChilds 8 months, 1 week ago

You're right. I agree with D.

upvoted 2 times

MILKE 9 months, 1 week ago

Its A, incidents.

upvoted 2 times

4rk4n4 10 months ago

Selected Answer: A

Its A, incidents.

upvoted 2 times

Mr4D97 10 months, 2 weeks ago

I would say A. Incidents.

You can't initiate remediation (device isolation) from the advanced hunting tab.

upvoted 3 times

wheeldj 8 months, 2 weeks ago

From your advanced hunting query you can create a custom detection rule to isolate devices

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide

Answer is D

upvoted 1 times

Jay_13 11 months, 2 weeks ago

D. Advanced hunting

upvoted 1 times

Ramye 11 months ago

Curious, why do we need to hunt since the trigger already happened and Incidents are in place that can be used to find the device and isolate?

upvoted 2 times

Murtuza 1 year ago

The answer is D

You can take the following actions on devices identified by the DeviceId column in your query results:

Isolate affected devices to contain an infection or prevent attacks from moving laterally

upvoted 1 times

Ramye 11 months ago

Why do we need to hunt since the trigger already happened and Incidents are in place that can be used to find the device and isolate?

upvoted 2 times

Roblearns 1 year, 1 month ago

i checked with ChatGPT, here is what it says after verification.

In your scenario of identifying devices that triggered a malware alert and initiating device isolation for affected devices, you should use option A: Incidents in the Microsoft 365 Defender portal. The "Incidents" feature is specifically designed for tracking and managing security incidents, including those related to malware alerts. You can use this feature to take action on specific incidents, including initiating device isolation if necessary.

While the "Investigations" feature (option C) is useful for in-depth analysis and evidence collection, it doesn't directly provide the capability to initiate device isolation. Therefore, option A (Incidents) is the more appropriate choice for your specific use case.

upvoted 4 times

Durden871 6 months, 2 weeks ago

Careful with ChatGPT. If you ask it 10 questions, it'll be right 6 times.

upvoted 1 times

Question #51 *Topic 1*

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Purview and contains a user named User1.

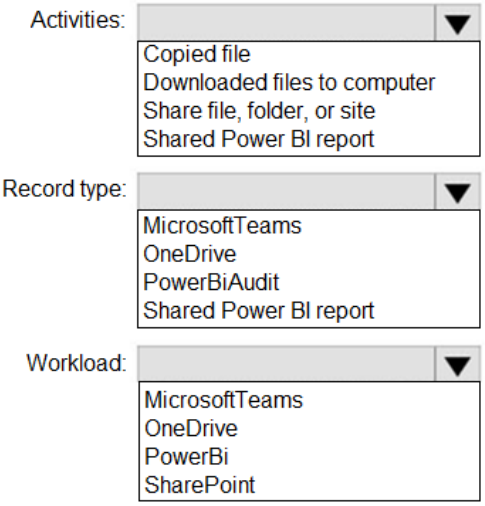
User1 shares a Microsoft Power BI report file from the Microsoft OneDrive folder of your company to an external user by using Microsoft Teams.

You need to identify which Power BI report file was shared.

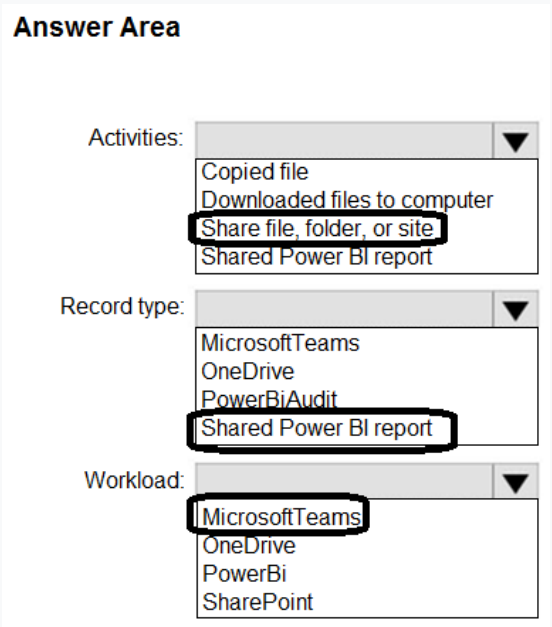
How should you configure the search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



DChilds Highly Voted 8 months, 3 weeks ago

1. Activities: These are the actions performed in your environment that are logged for auditing purposes. They can include a variety of actions such as file sharing, downloading files, copying files, etc.
2. Record Type: This refers to the type of data source from which the activity records are retrieved. It can be Microsoft Teams, OneDrive,

PowerBiAudit.
3. Workload: This refers to the specific service or application where the activity took place. It can be Microsoft Teams, OneDrive, PowerBi, SharePoint, etc.
Now, tying them up:

- The activity is "Share file, folder or site" because User1 shared a Power BI report file. This activity logs any instance of sharing a file, folder, or site.
- The record type is "OneDrive"because the Power BI report file was stored in OneDrive, and we want to retrieve activity records from there.
- The workload is "Microsoft Teams" because the sharing activity was performed through Microsoft Teams.
upvoted 17 times

Nikki0222 2 months, 1 week ago
CORRECT
upvoted 1 times

cris_exam Highly Voted 1 year, 3 months ago
Oh man, this question is messed up.

I think it's like this, but if anyone has actually had the opportunity to test this, please shed some light.

Activities: Shared file, folder, or site
<https://learn.microsoft.com/en-us/purview/audit-log-activities#sharing-and-access-request-activities>
"Shared file, folder, or site: User (member or guest) shared a file, folder, or site in SharePoint or OneDrive for Business with a user in your organization's directory. The value in the Detail column for this activity identifies the name of the user the resource was shared with and whether this user is a member or a guest."

Record Type: Microsoft Teams
<https://learn.microsoft.com/en-us/purview/audit-log-detailed-properties>
"Record Type: The type of operation indicated by the record. This property indicates the service or feature that the operation was triggered in."

Workload: Microsoft Teams
"Workload: The Microsoft 365 service where the activity occurred."
upvoted 6 times

cris_exam 1 year, 3 months ago
As I am looking at this again, the way I understand it, could also be as per below, but I tend to think that the first above option I mentioned previously would be the correct one.

Activities: Shared file, folder, or site

Record Type: PowerBIAudit

Workload: Microsoft Teams
upvoted 5 times

mb0812 10 months, 1 week ago
This looks correct. PowerBIAudit is the record type for Power BI events
upvoted 1 times

Bengkel Most Recent 3 months, 4 weeks ago
From Microsoft Teams (workload) a onedrive (Record Type) file is shared (Activity).

I think DChilds explained it correct.
upvoted 1 times

emartiy 7 months ago
I spend more time on this question since it has been seen 27/04.2024 as DChilds said..
By performing some auditlog search in our current tenant.. Some selection in activities or record types limits the other selections. So.. My final review on this question is that

Activities: Share file, folder, or site

Record type: OneDrive
Workload: OneDrive

Why both record type and workload is OneDrive? When search audit logs, I found that some shares via Teams chat also seen OneDrive as workload. So first is share file because we want to find which file was shared with external so, to narrow search filter last 2 option OneDrive and also user can be selected in search but it is not case in question.
upvoted 1 times

DChilds 8 months, 1 week ago
This question was in the exam 27/04/2024.
upvoted 4 times

mb0812 10 months, 1 week ago
Activities: Share file, folder, or site
Record type: PowerBIAudit ----> Recordtype for Power BI events (reference: https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema#auditlogrecordtype)

Workload: MicrosoftTeams
upvoted 3 times

falkendarkness 10 months, 4 weeks ago
To identify which Power BI report file was shared by User1 from the Microsoft OneDrive folder via Microsoft Teams, you should configure the search as follows:

Activities: Share file, folder, or site
Record type: OneDrive
Workload: MicrosoftTeams
Explanation:

Activities: Selecting "Share file, folder, or site" allows you to track activities related to sharing files, which includes sharing from OneDrive via Microsoft Teams.
Record type: Since the sharing action originates from OneDrive, you should select "OneDrive" as the record type.
Workload: The sharing action involves Microsoft Teams, so you should select "MicrosoftTeams" as the workload.
This configuration ensures you can identify the specific Power BI report file that was shared from the OneDrive folder via Microsoft Teams.
upvoted 2 times

Discuss4certi 10 months, 3 weeks ago
I disagree with your workload. Teams uses Onedrive or SharePoint as its file repositories. Onedrive is used for 1-1 conversations. Channel discussions are stored in SharePoint. hence the file is located in Onedrive in this case.
upvoted 1 times

Ramye 11 months ago
Activities - sharing a file - very clear

Record type : Power BI - not quite sure this one. Hopefully someone can confirm this one

Workload: OneDrive - file was actually shared from OneDrive - Teams was just a media in this case
upvoted 1 times

Ramye 11 months ago
Found out Record Type: Teams in this case

Per Microsoft, Record type is:
The type of operation indicated by the record. This property indicates the service or feature that the operation was triggered in.

Source: https://learn.microsoft.com/en-us/purview/audit-log-detailed-properties:
upvoted 1 times

Ramye 11 months ago
So the final answers:

Activities - sharing a file - very clear

Record type : Teams - based on the MS info shared above

Workload: OneDrive - file was actually shared from OneDrive - Teams was just a media in this case
upvoted 1 times

Murtuza 1 year ago
One drive will never be a record type as it falls under the workload category
Cloud-based personal file management, in the form of OneDrive, is an important workload for many businesses. Other
upvoted 1 times

Murtuza 1 year ago
When it comes into Power BI, the column is listed as a Type = Record
upvoted 1 times

NeoTactics 1 year ago
This seems to be some weird outdated question or whatever.
I tested it and shared a file (PDF File (didn't have PowerBI File at hand)).
Record Type was recorded as: SharePointSharingOperation
Workload was: OneDrive
Make your decision...
upvoted 1 times

kabooze 1 year, 2 months ago
isn't the record type "microsoft teams" ? "https://learn.microsoft.com/en-us/office/office-365-management-api/office-365-management-activity-api-schema#auditlogrecordtype"
upvoted 1 times

Mercury02m 1 year, 2 months ago
Can anyone clarify with the correct answer ? For me it looks like
Activities - Shared file, folder or site
Record Type - Shared PowerBi report
WorkLoad - Microsoft Teams
upvoted 2 times

chepeerick 1 year, 2 months ago
Option if your teams
upvoted 1 times

donathon 1 year, 3 months ago
Shared file, folder or site > This make sense since it's just another filee.
OneDrive > The fact that it's a powerBI file does not mean much since it's not shared from powerBI.
MicrosoftTeams > The activity is done from Teams.
upvoted 2 times

SaHaGe 1 year, 3 months ago
Activities: Configure the search with activity C) Share file, folder or site, as this relates to the action of sharing the Power BI report.

Record Type: You should select D) Shared Power BI Report as the record type as it allows you to identify the particular Power BI report sharing.

Workload: The appropriate workload is C) PowerBi, as it relates directly to the Power BI product and will allow you to track specific events related to shared Power BI reports

Reference: https://learn.microsoft.com/en-us/power-bi/admin/service-admin-auditing#search-the-audit-logs-by-file-folder-or-site
upvoted 1 times

pigl3t 1 year, 3 months ago
Activities: Share file, folder, or site
Record type: OneDrive
Workload: Onedrive
https://learn.microsoft.com/en-us/purview/audit-log-detailed-properties
upvoted 1 times

pigl3t 1 year, 3 months ago

based on the link above
Activities: Share File, folder or site
Workload: The Microsoft 365 service where the activity occurred. - it was shared from OneDrive right?
RecordType: The type of operation indicated by the record. This property indicates the service or feature that the operation was triggered in. - wouldn't this be OneDrive also?
upvoted 1 times

DRAG DROP
-

Case study
-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
-
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
-

Litware Inc. is a renewable energy company.

Litware has offices in Boston and Seattle. Litware also has remote users located across the United States. To access Litware resources, including cloud resources, the remote users establish a VPN connection to either office.

Existing Environment
-

Identity Environment
-

The network contains an Active Directory forest named litware.com that syncs to an Azure Active Directory (Azure AD) tenant named litware.com.

Microsoft 365 Environment
-

Litware has a Microsoft 365 E5 subscription linked to the litware.com Azure AD tenant. Microsoft Defender for Endpoint is deployed to all computers that run Windows 10. All Microsoft Defender for Cloud Apps built-in anomaly detection policies are enabled.

Azure Environment

-

Litware has an Azure subscription linked to the litware.com Azure AD tenant. The subscription contains resources in the East US Azure region as shown in the following table.

Name	Type	Description
LA1	Log Analytics workspace	Contains logs and metrics collected from all Azure resources and on-premises servers
VM1	Virtual machine	Server that runs Windows Server 2019
VM2	Virtual machine	Server that runs Ubuntu 18.04 LTS

Network Environment

-

Each Litware office connects directly to the internet and has a site-to-site VPN connection to the virtual networks in the Azure subscription.

On-premises Environment

-

The on-premises network contains the computers shown in the following table.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller in litware.com that connects directly to the internet
CLIENT1	Windows 10	Boston	Domain-joined client computer

Current Problems

-

Microsoft Defender for Cloud Apps frequently generates false positive alerts when users connect to both offices simultaneously.

Planned Changes and Requirements

Planned Changes

-

Litware plans to implement the following changes:

• Create and configure Microsoft Sentinel in the Azure subscription.
• Validate Microsoft Sentinel functionality by using Azure AD test user accounts.

Business Requirements

-

Litware identifies the following business requirements:

• The principle of least privilege must be used whenever possible.
• Costs must be minimized, as long as all other requirements are met.
• Logs collected by Log Analytics must provide a full audit trail of user activities.
• All domain controllers must be protected by using Microsoft Defender for Identity.

Azure Information Protection Requirements

All files that have sensitivity labels and are stored on the Windows 10 computers must be available from the Azure Information Protection –

Data discovery dashboard.

Microsoft Defender for Endpoint Requirements

All Microsoft Defender for Cloud Apps unsanctioned apps must be blocked on the Windows 10 computers by using Microsoft Defender for Endpoint.

Microsoft Defender for Cloud Apps Security Requirements

Microsoft Defender for Cloud Apps must identify whether a user connection is anomalous based on tenant-level data.

Microsoft Defender for Cloud Requirements

All servers must send logs to the same Log Analytics workspace.

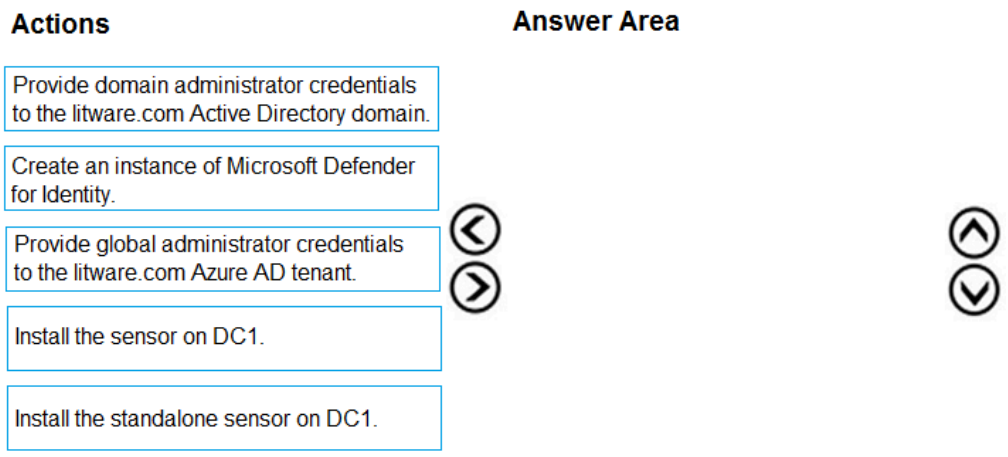
Microsoft Sentinel Requirements

Litware must meet the following Microsoft Sentinel requirements:

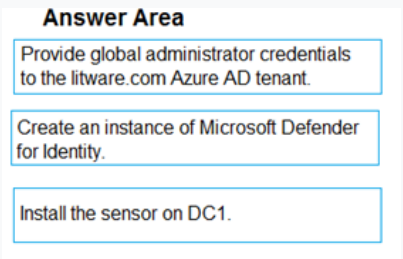
• Integrate Microsoft Sentinel and Microsoft Defender for Cloud Apps.
• Ensure that a user named admin1 can configure Microsoft Sentinel playbooks.
• Create a Microsoft Sentinel analytics rule based on a custom query. The rule must automatically initiate the execution of a playbook.
• Add notes to events that represent data access from a specific IP address to provide the ability to reference the IP address when navigating through an investigation graph while hunting.
• Create a test rule that generates alerts when inbound access to Microsoft Office 365 by the Azure AD test user accounts is detected. Alerts generated by the rule must be grouped into individual incidents, with one incident per test user account.

You need to configure DC1 to meet the business requirements.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Suggested Answer:



Fez786 Highly Voted 9 months ago

THIS QUESTION IS THE SAME AS TOPIC 5 QUESTION 3 !!!

Given answer is wrong. Correct answer is:
- Create an instance of MS Defender for Identity
- Provide Domain Admin Credentials to the litware.com.....
- Install the sensor on DC1

See Topic 5 Question 3 discussion. its been proven.
upvoted 38 times

ggGG1357 7 months ago
You are correct
upvoted 1 times

kazaki Most Recent 4 months, 2 weeks ago
U r all wrong creating instance was old configuration now since u have e5 then u have instance
upvoted 1 times

Ramye 4 months, 1 week ago
So what are your suggested answers?
upvoted 4 times

allinict 5 months, 2 weeks ago
guys is it really the right answer because on the internet i found this multiple time as an answer:

Provide global admin credentials to the litware.com azure ad
Create an instance of microsoft defender for identity
Provide global admin credentials to litware.com azure ad tenant
install the sensor on DC01
upvoted 1 times

Ramye 4 months, 2 weeks ago
You know this is wrong as it shows 4 ans where the question asked for 3.
upvoted 2 times

chepeerick 8 months, 2 weeks ago
Option correct
upvoted 1 times

Fez786 8 months, 1 week ago
no!! no!!
upvoted 1 times

hovlund 9 months ago
I would say it's correct
upvoted 2 times

hovlund 9 months ago
Correction!!

1). Create an instance of MS Defender for Identity
2). Provide domain admin creds
3). install the sensor on DC1
upvoted 13 times

Fez786 8 months, 1 week ago
no!! no!!
upvoted 1 times

Question #53 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams.

You have a team named Team1 that has a project named Project1.

You need to identify any Project1 files that were stored on the team site of Team1 between February 1, 2023, and February 10, 2023.

Which KQL query should you run?

A. (c:c)(Project1)(date=(2023-02-01)..date=(2023-02-10))

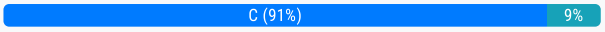
B. AuditLogs -
| where Timestamp between (datetime(2023-02-01)..datetime(2023-02-10))
| where FileName contains “Project1”

C. Project1(c:c)(date=2023-02-01..2023-02-10)

D. AuditLogs -
| where Timestamp > ago(10d)
| where FileName contains “Project1”

Suggested Answer: *B*

Community vote distribution



SenorConsultant Highly Voted 1 year, 2 months ago

Selected Answer: C

Tested in content search in the purview portal.

project1(c:c)(date=2023-02-01..2023-02-10)

This is the correct syntax for KQL content search in Purview, and searches for keyword "project1" in selected team, and between said dates.

upvoted 12 times

ostralo Highly Voted 10 months ago

KQL (Kusto Query Language) != KQL(Keyword Query Language)
I hate MS.

upvoted 6 times

Nikki0222 Most Recent 2 months, 1 week ago

C correct

upvoted 1 times

fy28838 2 months, 2 weeks ago

Selected Answer: B

B is definitely the correct answer

upvoted 1 times

emartiy 7 months ago

Selected Answer: B

checked in Content search. When enter keyword and select Date for given range its result

project1(c:c)(date=2023-02-01..2023-02-10) (Correct answer is B)

upvoted 1 times

smosmo 7 months ago

@emartiy: project1(c:c)(date=2023-02-01..2023-02-10) is answer "C" not B, right?

upvoted 2 times

Durden871 9 months, 1 week ago

Chat GPT if you just copy and paste "C" into the question box.
To search for Project1 files stored on the team site of Team1 between February 1, 2023, and February 10, 2023, using the provided query syntax, you can use the following KQL query:

r
Copy code
Project1 (c:c) (date=2023-02-01..2023-02-10) Mo
This query searches for files with the name "Project1" (Project1), stored on the team site of Team1 ((c:c)), with a modification date between February 1, 2023, and February 10, 2023 ((date=2023-02-01..2023-02-10)), and filters for files modified on Mondays (Mo).
upvoted 2 times

Durden871 9 months, 1 week ago
The provided KQL query seems to be targeting audit logs to identify files containing "Project1" within a specified time range. Here's the corrected version:

kql
Copy code
AuditLogs
| where Timestamp between (datetime(2023-02-01) .. datetime(2023-02-10))
| where FileName contains "Project1"
This query filters the AuditLogs for entries where the Timestamp falls between February 1, 2023, and February 10, 2023, and then further filters those entries to include only files where the FileName contains "Project1".
upvoted 1 times

MILKE 9 months, 1 week ago
AuditLogs -
| where Timestamp between (datetime(2023-02-01)..datetime(2023-02-10))
| where FileName contains “Project1”
upvoted 1 times

MattWong 10 months, 3 weeks ago
The question is about KQL, so it is B
upvoted 1 times

chepeerick 1 year, 2 months ago
Option B
upvoted 3 times

hovlund 1 year, 3 months ago
Correct in my opinion
upvoted 1 times

hovlund 1 year, 2 months ago
I stand corrected by Danb67
upvoted 2 times

danb67 1 year, 2 months ago
Nope. This is talking about Purview. I tested in my lab. I started an E-Discovery case and the only option that works is C. C:C means 'and' so here we are looking for the file Project1 and the date filter.
A: Wrong syntax why would a query start with And?
B: E-Discovery doesn't accept syntax like this. We are not talking about advanced hunting here.
C: Correct
D: See B
upvoted 4 times

wheeldj 8 months, 2 weeks ago
Just ran this in my lab tenant and E-discovery absolutely does accept KQL format queries such as answer B. No syntax errors. I couldn't check the results as I have no data in this tenant but the search ran just fine.

So on the basis that both B and C appear to work and the question specifically asks for KQL I vote answer B.
upvoted 2 times

TheHuman_ 1 year ago

Nowhere it is stated that this query is explicitly executed inside Purview. It says to use KQL queries, which could also be inside Advanced Hunting

upvoted 1 times

Wixed 1 year ago

Wrong, you require Microsoft 365 Defender to perform advanced hunting.

The description only says: "You have a Microsoft 365 subscription that uses Microsoft Purview and Microsoft Teams."

upvoted 3 times

Question #54 *Topic 1*

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

You need to create a query that will link the AlertInfo, AlertEvidence, and DeviceLogonEvents tables. The solution must return all the rows in the tables.

Which operator should you use?

A. search *

B. union kind = inner

C. join kind = inner

D. evaluate hint.remote =

Suggested Answer: *B*

Community vote distribution

B (100%)

danb67 Highly Voted 1 year, 2 months ago

A. Not correct syntax.
B. Correct Answer. Union takes two or more tables and returns the rows of all of them.
C. Join Kind inner will not produce every row as inner means output has one row for every combination of left and right. So only if the columns appears in both tables will we get a hit. This doesn't meet the ask.
D. Evaluate in KQL calls a plugin this is not relevant to the question
upvoted 7 times

DChilds Highly Voted 8 months, 1 week ago

This question was in the exam 27/04/2024.
upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago

B correct
upvoted 1 times

Porter5000 11 months ago

Selected Answer: B
Union, because there are two or more tables that you need the rows from all tables
upvoted 1 times

N1oks 1 year, 1 month ago

Selected Answer: B
just could be *b*
upvoted 1 times

smanzana 1 year, 1 month ago

It is B
upvoted 1 times

chepeerick 1 year, 2 months ago

Option B
upvoted 2 times

hovlund 1 year, 3 months ago

Correct, Union takes Two or more tables and returns the rows of all of them: https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/unionoperator?pivots=azuredataexplorer
upvoted 4 times

Question #55 *Topic 1*

You have a Microsoft 365 E5 subscription that contains 100 Windows 10 devices.

You onboard the devices to Microsoft Defender 365.

You need to ensure that you can initiate remote shell connections to the onboarded devices from the Microsoft 365 Defender portal.

What should you do first?

A. Modify the permissions for Microsoft 365 Defender.

B. Create a device group.

C. From Advanced features in the Endpoints settings of the Microsoft 365 Defender portal, enable automated investigation.

D. Configure role-based access control (RBAC).

Suggested Answer: *D*

Community vote distribution

C (50%) D (50%)

kazaki Highly Voted 1 year ago

Selected Answer: C

C for Sure

Enable live response from the advanced settings page.

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide#before-you-begin

upvoted 8 times

g_man_rap 4 months, 1 week ago

exactly on your link write it clear, it is D:

Live response commands

Depending on the role that's been granted to you, you can run basic or advanced live response commands. User permissions are controlled by RBAC custom roles. For more information on role assignments, see Create and manage roles.

upvoted 2 times

nsss 11 months, 1 week ago

That's not what option C says though.

upvoted 3 times

sunilpanda Most Recent 1 month ago

Selected Answer: C

initiating live response is not RBAC

upvoted 1 times

efb9f47 1 month, 3 weeks ago

C. From Advanced features in the Endpoints settings of the Microsoft 365 Defender portal, enable automated investigation is the correct choice because enabling this feature allows you to use advanced capabilities such as remote shell connections.

Once you've enabled this feature, you can then proceed to configure RBAC to ensure that the appropriate permissions are in place for the users who need to initiate remote shell connections.

upvoted 1 times

Nikki0222 2 months, 1 week ago

D correct

upvoted 2 times

user636 4 months, 1 week ago

Selected Answer: D

You enable Live response from the advanced settings & then you need to configure RBAC to use this feature.
Ref: https://learn.microsoft.com/en-us/defender-endpoint/live-response?view=o365-worldwide#before-you-begin
upvoted 3 times

Sekpluz 6 months, 3 weeks ago

Selected Answer: D

C is no good, trick answer, supposed to be automatic REMEDIATION.. so then D is the Answer.
upvoted 3 times

Durden871 9 months, 1 week ago

ChatGPT
No, initiating remote shell connections does not necessarily require automated investigations. Remote shell connections allow administrators to access a command-line interface on a remote device for troubleshooting, management, and other administrative tasks.
upvoted 1 times

Ramye 10 months, 2 weeks ago

Selected Answer: C

What comes first between enabling the service and assigning access?
You need to have service first before you can assign access.
upvoted 1 times

Ramye 10 months ago

Never mind - found the answer - It is D.
Live Response
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection
upvoted 4 times

kazaki 11 months ago

Selected Answer: C

For enabling the service first
upvoted 2 times

Porter5000 11 months ago

Selected Answer: D

D. Configure role-based access control (RBAC).

RBAC allows you to define and manage roles and permissions for users, ensuring that only authorized individuals can perform specific actions, such as initiating remote shell connections. By configuring RBAC, you can grant the necessary permissions to the users who need to initiate remote shell connections to the devices.

The other options are not directly related to the specific task of initiating remote shell connections:
A. This option is broad and doesn't specify the necessary permissions for initiating remote shell connections.

B. Create a device group: Creating one is not directly related to initiating remote shell connections.

C. Enabling automated investigation is a useful feature, but it is not specifically related to initiating remote shell connections.
upvoted 4 times

Ramye 10 months, 1 week ago

The questions asked - You need to ensure that you can initiate remote shell connections. So how do you initiate something that is not enabled?
I would like to find out. Thx
upvoted 1 times

Ramye 10 months, 1 week ago

Never mind - found the answer - It is D.
Live Response
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection.
upvoted 2 times

Str4int 3 months, 2 weeks ago

for me it's C.
RBAC also need to be configured reagarding best practicies but first this advanced feature need to be activated.

another example is, if the global admin is connectecd but the feature is not activated, he can't connect... so C need to be configured first in my opinion
upvoted 1 times

IvanCantero023 11 months, 2 weeks ago

Selected Answer: D

D is correct
upvoted 2 times

Ramye 10 months, 1 week ago

How? I would like to know. Thx
upvoted 1 times

Ramye 10 months, 1 week ago

Never mind - found the answer - It is D.
Live Response
Allows users with appropriate RBAC permissions to investigate devices that they are authorized to access, using a remote shell connection
upvoted 1 times

Pradeep064 11 months, 2 weeks ago

"What should you do first?"

A live response becomes a viable option only if the user possesses the RBAC permission to investigate, making "D" the appropriate answer.

D - Configure role based access control (RBAC)
upvoted 1 times

kazaki 1 year ago

i dont know how you all say RBAC it is Purely
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide#before-you-begin

Enable live response from the advanced settings page.
upvoted 2 times

Durden871 9 months, 1 week ago

From your link:
Ensure that you have the appropriate permissions.

Only users who have been provisioned with the appropriate permissions can initiate a session. For more information on role assignments, see Create and manage roles.
upvoted 1 times

chepeerick 1 year, 2 months ago

Option D for Roles
upvoted 1 times

Gurulee 1 year, 2 months ago

Selected Answer: D

Depending on the role that's been granted to you, you can run basic or advanced live response commands. Users permissions are controlled by RBAC custom role
upvoted 3 times

sand5234 1 year, 3 months ago

Answer is correct as per this link
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwide
upvoted 4 times

HOTSPOT
-

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

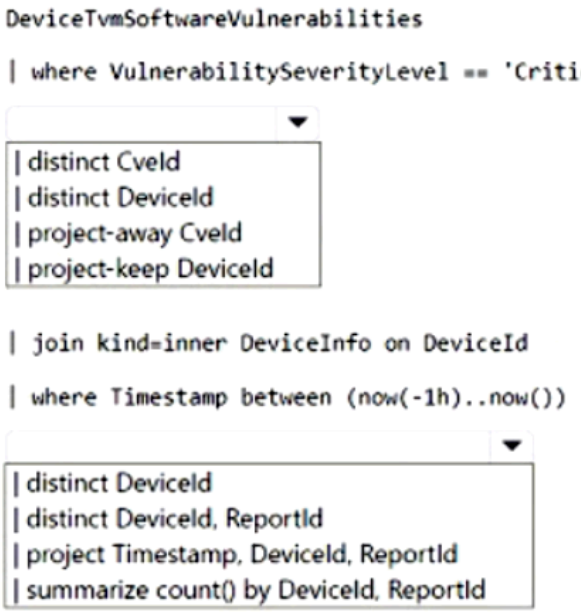
You need to create a detection rule that meets the following requirements:

• Is triggered when a device that has critical software vulnerabilities was active during the last hour
• Limits the number of duplicate results

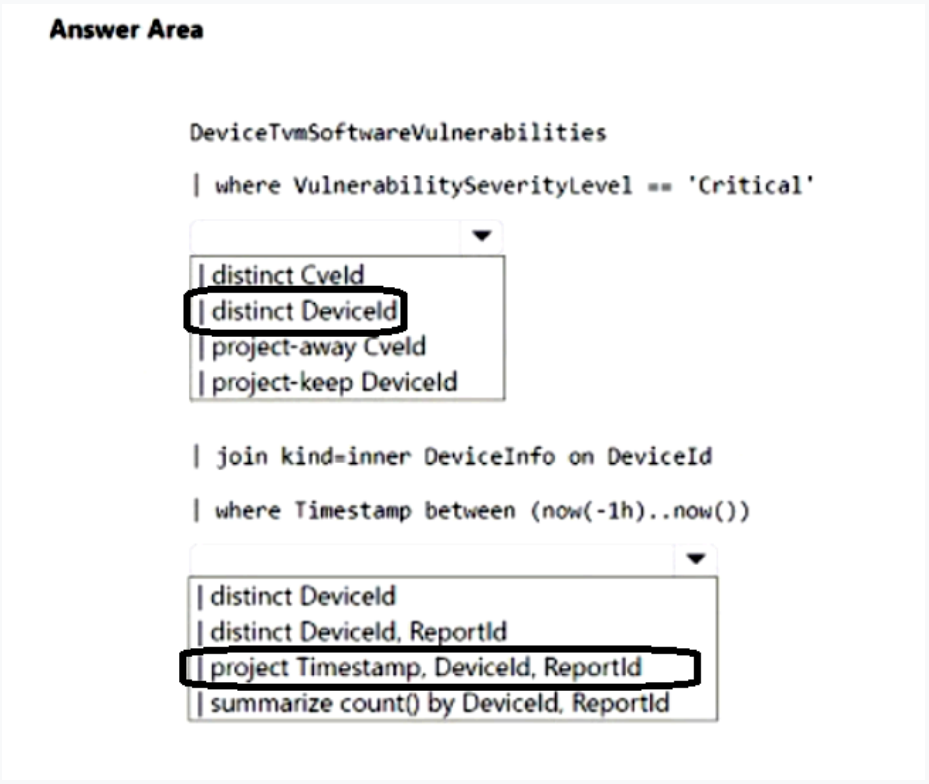
How should you complete the KQL query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



ceejay12 Highly Voted 1 year, 3 months ago

1. | distinct DeviceID
2. | project Timestamp, DeviceID, ReportID

upvoted 13 times

Nikki0222 2 months, 1 week ago

Correct

upvoted 1 times

wheeldj Most Recent 8 months, 2 weeks ago

part1: |distinct DeviceID
Because DeviceID is required to successfully join the tables and distinct to limit the returns to unique devices

part2: |project Timestamp, DeviceID, ReportID
Your need Timestamp, DeviceID and ReportID in the return to create a custom detection rule

https://learn.microsoft.com/en-us/microsoft-365/security/defender/custom-detection-rules?view=o365-worldwide#required-columns-in-the-query-results

upvoted 4 times

33c26f0 10 months ago

Question says limit duplicates ?

upvoted 1 times

chepeerick 1 year, 2 months ago

correct

upvoted 2 times

danb67 1 year, 2 months ago

Correct:
DeviceID it has to be because DeviceId is available in both tables, CveId is not so that wouldn't work.

2nd is correct also because to create a custom detection rule you need DeviceID and ReportId in the output. And the question isn't asking for a count so summarise would not be correct.

upvoted 2 times

sand5234 1 year, 3 months ago

Answer is correct

upvoted 2 times

Question #57 *Topic 1*

HOTSPOT
-

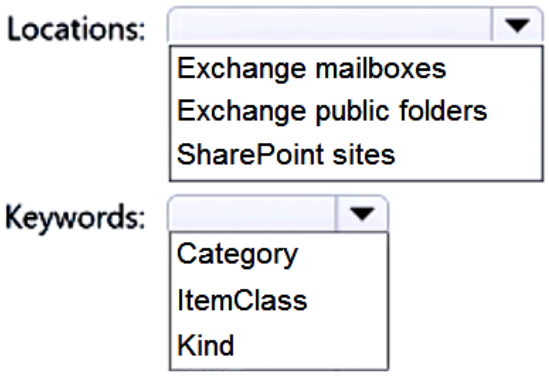
You have a Microsoft 365 E5 subscription that uses Microsoft Teams.

You need to perform a content search of Teams chats for a user by using the Microsoft Purview compliance portal. The solution must minimize the scope of the search.

How should you configure the content search? To answer, select the appropriate options in the answer area.

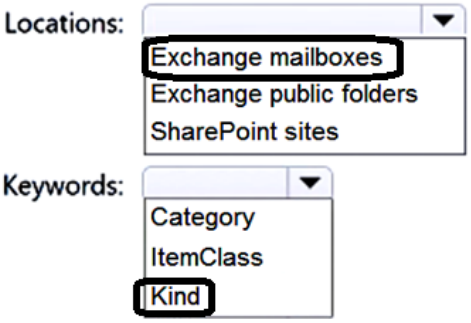
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



jr_cyber Highly Voted 1 year, 3 months ago

The answer is correct:
Exchange mailboxes
Kind

Categories are "The categories to search. Categories can be defined by users by using Outlook or Outlook on the web... The possible values are red, blue, green, etc."

ItemClass: "Use this property to search specific third-party data types that your organization imported to Office 365." We are not importing any third-party data types.

Kind: "The type of email message to search for. Possible values: contacts, microsoftteams, meetings, etc."

https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

upvoted 12 times

Nikki0222 2 months, 1 week ago

Correct

upvoted 1 times

e072f83 Most Recent 7 months, 2 weeks ago

The answer is correct:

Exchange mailboxes

Kind

https://learn.microsoft.com/en-us/purview/ediscovery-search-cloud-based-mailboxes-for-on-premises-users

upvoted 2 times

Discuss4certi 10 months, 3 weeks ago

The question seems to match with the link here, so answers are correct:

https://learn.microsoft.com/en-us/purview/ediscovery-search-cloud-based-mailboxes-for-on-premises-users

upvoted 2 times

smanzana 1 year, 1 month ago

Exchange mailboxes

Kind

upvoted 2 times

blacksheep_29 1 year, 1 month ago

The answer is Correct - Exchange Mailbox to check in Users group and Teams and other and specify which among the 3 should we search

Option 1 - https://learn.microsoft.com/en-us/purview/ediscovery-content-search

Option 2 - https://learn.microsoft.com/en-us/purview/ediscovery-keyword-queries-and-search-conditions

upvoted 2 times

chepeerick 1 year, 2 months ago

Correct

upvoted 1 times

Vitalija 1 year, 3 months ago

it is corect based on https://learn.microsoft.com/en-us/purview/ediscovery-search-cloud-based-mailboxes-for-on-premises-users

upvoted 3 times

Question #58 *Topic 1*

You have a Microsoft 365 E5 subscription that contains 100 Linux devices. The devices are onboarded to Microsoft Defender 365.

You need to initiate the collection of investigation packages from the devices by using the Microsoft 365 Defender portal.

Which response action should you use?

A. Run antivirus scan

B. Initiate Automated Investigation

C. Collect investigation package

D. Initiate Live Response Session

Suggested Answer: *D*

Community vote distribution

ostralo Highly Voted 10 months ago

Collect investigation package works with Linux and MacOS - March.8.2024

upvoted 15 times

djcyber1 Highly Voted 8 months ago

Tested this on a Linux device and collect investigation package now works so would go for C in the exam now

upvoted 9 times

Nikki0222 Most Recent 2 months, 1 week ago

C correct

upvoted 1 times

ms600 2 months, 2 weeks ago

Selected Answer: C

Collects a package of diagnostic information from the device, including logs and system information

upvoted 1 times

user636 4 months, 1 week ago

Selected Answer: C

Collect investigation package

upvoted 3 times

Avaris 6 months, 2 weeks ago

Selected Answer: C

so I had an issue with Sc-200 working with 3 generative AI but in regards to this question they all agreed it's a C so you gotta give the that

upvoted 2 times

Avaris 7 months, 2 weeks ago

Selected Answer: C

Ran it in Copilot and its C To initiate the collection of investigation packages from the Linux devices onboarded to Microsoft Defender for Endpoint, you should use:

C. Collect investigation package:

This action allows you to download an investigation package (ZIP file) containing relevant data and evidence related to the alert or incident. By selecting this option, you can gather the necessary information for further analysis and response.

upvoted 2 times

smosmo 7 months, 3 weeks ago

Selected Answer: C

Obviously "Collect investigation package is" (now) supported on Linux/Mac, if we can believe teh documentation here :https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts#collect-investigation-package-from-devices

upvoted 2 times

ecasjo 8 months, 1 week ago

I think now you can collect investigation package on Linux, it says here:
https://learn.microsoft.com/en-us/defender-endpoint/respond-machine-alerts#collect-investigation-package-from-devices

So if i see this question on exam, i will go for C)

upvoted 1 times

Discuss4certi 10 months, 3 weeks ago

Selected Answer: D

I initially thought B. however since its not supported for linux machines its live response. so option D!

upvoted 1 times

Discuss4certi 10 months, 3 weeks ago

I initially thought B. however since its not supported for linux machines its live response. so option D!

upvoted 1 times

Vamshi_Krishna 1 year ago

Selected Answer: D

D is correct. Initiate Live Response.

upvoted 3 times

MS_KoolaidMan 1 year ago

Selected Answer: D

Linux VMs
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide#initiate-live-response-session

upvoted 1 times

brichardson14 1 year, 1 month ago

answer is correct
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/respond-machine-alerts?view=o365-worldwide#initiate-live-response-session

upvoted 1 times

chepeerick 1 year, 2 months ago

Option D as it is Linux

upvoted 1 times

sand5234 1 year, 3 months ago

Answer is correct.
You initiate the live response on Linux and run "collect" command .

upvoted 4 times

ceejay12 1 year, 3 months ago

But there is an option to collect the investigation package from the device without initiating a live response session?

upvoted 1 times

ceejay12 1 year, 3 months ago

Apologies, answer is correct, the option is missing from Linux devices/servers.

upvoted 3 times

Question #59 *Topic 1*

You need to configure Microsoft Defender for Cloud Apps to generate alerts and trigger remediation actions in response to external sharing of confidential files.

Which two actions should you perform in the Microsoft 365 Defender portal? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From Settings, select Cloud App, select Microsoft Information Protection, and then select Only scan files for Microsoft Information Protection sensitivity labels and content inspection warnings from this tenant.

B. From Cloud apps, select Files, and then filter File Type to Document.

C. From Settings, select Cloud App, select Microsoft Information Protection, select Files, and then enable file monitoring.

D. From Cloud apps, select Files, and then filter App to Office 365.

E. From Cloud apps, select Files, and then select New policy from search.

F. From Settings, select Cloud App, select Microsoft Information Protection, and then select Automatically scan new files for Microsoft Information Protection sensitivity labels and content inspection warnings.

Suggested Answer: *CF*

Community vote distribution

CF (100%)

N1oks Highly Voted 1 year, 1 month ago

Selected Answer: CF

Correct C and F

upvoted 7 times

Nikki0222 Most Recent 2 months, 1 week ago

CF correct

upvoted 1 times

Hawklx 6 months ago

Triplicate question

upvoted 4 times

Murtuza 1 year, 1 month ago

Review question #18 to get the correct answers

From Settings, select Information Protection, select Files, and then enable file monitoring

. From Settings, select Information Protection, select Azure Information Protection, and then select Automatically scan new files for Azure Information Protection classification labels and content inspection warnings

upvoted 2 times

smanzana 1 year, 1 month ago

Correct (C-F)

upvoted 1 times

Mercury02m 1 year, 2 months ago

The answer is wrong. It should be B and F. In Option C - we can't select Files from Microsoft Information Protection. Tested in the lab.

Settings -> CloudApps -> Files -> Enable File Monitoring

Settings -> CloudApps -> Microsoft Information Protection -> Automatically scan new files....

upvoted 1 times

Ramye 11 months ago

you wrote the right answers but chose the wrong option B. B is the wrong answer.

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct

upvoted 1 times

CarstenHM 1 year, 2 months ago

Don't quite get why it is F and not A, please help me understand.

F says ..."select Automatically scan new files". What if it isn't a new file that's shared?

upvoted 1 times

Fez786 1 year, 3 months ago

Correct

upvoted 3 times

Question #60 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Purview.

Your company has a project named Project1.

You need to identify all the email messages that have the word Project1 in the subject line. The solution must search only the mailboxes of users that worked on Project1.

What should you do?

A. Perform a user data search.

B. Create a records management disposition.

C. Perform an audit search.

D. Perform a content search.

Correct Answer: *D*

ifaiyazhossain 1 month ago

Selected Answer: D

D is correct answer

upvoted 1 times

Question #61 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You discover that when Microsoft Defender for Endpoint generates alerts for a commonly used executable file, it causes alert fatigue.

You need to tune the alerts.

Which two actions can an alert tuning rule perform for the alerts? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. delete

B. hide

C. resolve

D. merge

E. assign

Suggested Answer: *BD*

Community vote distribution

BC (100%)

landfils 9 hours, 8 minutes ago

Selected Answer: BC

B and C

Hide : This action allows you to hide alerts generated by the specified executable file, reducing the noise and alert fatigue. These hidden alerts will not appear in the incident queue but will still be logged for historical purposes.

Resolve : This action automatically resolves alerts generated by the specified executable file. The alerts are marked as resolved, indicating that no further action is required. This helps in managing alert fatigue by automatically handling known benign alerts.

upvoted 1 times

RoombaDoinZoomba 14 hours, 53 minutes ago

Selected Answer: BC

Incorrect: https://learn.microsoft.com/en-us/defender-xdr/investigate-alerts?tabs=settings

Alert tuning can only hide and resolve alerts to assist, it cannot merge alerts.

upvoted 1 times

tryade 1 week ago

Selected Answer: BC

Incorrect, B and C

https://techcommunity.microsoft.com/blog/microsoftthreatprotectionblog/boost-your-detection-and-response-workflows-with-alert-tuning/3824712

upvoted 2 times

Question #62 *Topic 1*

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.

You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product.

Solution: You configure endpoint detection and response (EDR) in block mode.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*

Community vote distribution

A (100%)

Shingie 3 days, 15 hours ago

Selected Answer: A

Answer: A. Yes

Configuring Endpoint Detection and Response (EDR) in block mode meets the goal.

EDR in block mode allows Microsoft Defender for Endpoint to detect and remediate malicious artifacts even when Microsoft Defender Antivirus is in passive mode due to the presence of a third-party antivirus. This ensures that threats missed by the third-party antivirus can still be addressed by Microsoft Defender for Endpoint's advanced detection and response capabilities.

Thus, enabling EDR in block mode effectively provides the required protection in this scenario.

upvoted 1 times

Question #63 *Topic 1*

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.

You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product.

Solution: You configure Controlled folder access.

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Shingie 3 days, 15 hours ago

Selected Answer: B

Answer: B. No

Configuring Controlled Folder Access does not meet the goal. Controlled Folder Access is a feature of Microsoft Defender Antivirus that protects specific folders from unauthorized changes by ransomware or other malicious apps. However, this feature requires Microsoft Defender Antivirus to be active and does not address the scenario where Defender Antivirus is in passive mode due to the presence of a third-party antivirus.

To meet the goal of protecting the devices from malicious artifacts undetected by the third-party antivirus, you should enable EDR in block mode. EDR in block mode works even when Microsoft Defender Antivirus is in passive mode, allowing Microsoft Defender for Endpoint to remediate threats missed by the third-party antivirus.

Thus, configuring Controlled Folder Access is not the correct solution in this scenario.

upvoted 1 times

Question #64 *Topic 1*

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

You have a Microsoft 365 subscription.

You have 1,000 Windows devices that have a third-party antivirus product installed and Microsoft Defender Antivirus in passive mode.

You need to ensure that the devices are protected from malicious artifacts that were undetected by the third-party antivirus product.

Solution: You enable automated investigation and response (AIR).

Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*

Community vote distribution

B (100%)

Madzius 4 days, 5 hours ago

Selected Answer: B

Could someone explain if this answer is correct

upvoted 1 times

Shingie 3 days, 15 hours ago

Answer: B. No

Enabling automated investigation and response (AIR) alone does not meet the goal. While AIR can investigate and respond to threats, it requires that Microsoft Defender Antivirus is active or that other components of Microsoft Defender for Endpoint, such as endpoint detection and response (EDR), are operational.

Since Microsoft Defender Antivirus is in passive mode, it cannot actively scan and detect malicious artifacts that were missed by the third-party antivirus. To achieve the goal, you need to enable EDR in block mode in addition to AIR. EDR in block mode works even when Microsoft Defender Antivirus is in passive mode, allowing Microsoft Defender for Endpoint to detect and remediate threats that the third-party antivirus missed.

Thus, simply enabling AIR is not sufficient to protect the devices in this scenario.

upvoted 1 times

Question #65 *Topic 1*

You have a Microsoft 365 subscription that uses Microsoft Defender XDR.

You need to implement deception rules. The solution must ensure that you can limit the scope of the rules.

What should you create first?

A. device groups

B. device tags

C. honeytoken entity tags

D. sensitive entity tags

Suggested Answer: *A*

Community vote distribution

A (100%)

WinstonN 3 hours, 7 minutes ago

Selected Answer: B

B is correct. Check the scoping. its Device Tags.
https://learn.microsoft.com/en-us/defender-xdr/configure-deception

upvoted 1 times

ctshepard 1 week ago

Selected Answer: A

A is correct because once the devices are grouped, they can then be tagged.

upvoted 2 times

Question #1 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Prevent future attacks section.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
You need to resolve the existing alert, not prevent future alerts. Therefore, you need to select the 'Mitigate the threat' option.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution

Metasploit Highly Voted 2 years, 2 months ago

Selected Answer: B

Answer is (B) No, because the question is asking for recommendations on the current alert that you are viewing(Mitigate the threat) and not on security recommendations in general(Prevent Future attacks) for the device associated with the alert..

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts

(Mitigate the threat) - provides manual remediation steps for this security alert (Provides recommendations on what to do to resolve the alert)

(Prevent future attacks) - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks.(Provides recommendations for security in general such as Remediate Vulnerabilities and win defender should be activated on all devices)

upvoted 17 times

Chris2pher 12 months ago

The answer is YES. When you expand Prevent Future Attacks, you can see from there the recommendation. THe question only asks if you can view the recommendation. Technically it satisfy the question by expanding the Prevent Future AtTACKS. so the answer is YES

upvoted 2 times

Ramye 11 months ago

The answer is No. To resolve the issue/alert/threat you need to follow the steps under "Mitigate the threat".

Prevent future attacks" says "
Solving security recommendations can prevent future attacks by reducing attack surface."

upvoted 3 times

examkid Highly Voted 3 years, 5 months ago

Answer is correct:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

upvoted 11 times

HAjouz Most Recent 3 weeks, 1 day ago

Selected Answer: B

The "Prevent future attacks" section in Azure Security Center is designed to provide recommendations to address the root causes and prevent similar issues in the future. However, it does not directly mitigate current attacks.

To address and mitigate current threats, you should focus on the "Mitigate threat" section. This section provides immediate actions to contain or neutralize the ongoing threat.

upvoted 1 times

Avaris 1 month, 3 weeks ago

Selected Answer: A

check this link guys it clearly showing the option in orevent future attacks Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks

upvoted 1 times

Nikki0222 2 months, 1 week ago

Yes correct

upvoted 1 times

Nikki0222 2 months, 1 week ago

Correction…. It's NO :)

upvoted 1 times

Jay_13 10 months, 2 weeks ago

Selected Answer: B

In the question it asked for "to view recommendations to resolve the alert in Security Center." So, if you select Take Action, and then expand the Prevent future attacks section it will show the recommendations for the source machine not for the alert. So the answer will be : NO

upvoted 1 times

Pradeep064 11 months, 2 weeks ago

Selected Answer: B

I second the link shared by @examkid, Prevent future attacks doesn't resolve the current alert.

upvoted 1 times

chepeerick 1 year, 2 months ago

correct

upvoted 1 times

sand5234 1 year, 3 months ago

Answer is Yes

upvoted 2 times

Anil0512 1 year, 3 months ago

Tried and tested The answer is A (Yes)

upvoted 2 times

cris_exam 1 year, 3 months ago

I believe the given answer is correct: NO

I think that where the question refers to when mentioning recommendations for having the alert resolved is here and NOT the "Prevent future attacks" option.

https://learn.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide#manage-alerts

"The Recommendations tab provides next-step actions and advice for investigation, remediation, and prevention."

upvoted 1 times

Oryx360 1 year, 4 months ago

Selected Answer: A

Yes, your solution meets the goal. In Azure Security Center, to view recommendations to resolve a security alert, you would typically follow these steps:

Go to Azure Security Center.
Navigate to the "Security alerts" section.
Locate and select the specific alert you want to investigate.
Click on "Take Action" or "View Recommendations" (the exact wording may vary).
Expand the "Prevent future attacks" or similar section.
In this section, you'll find recommendations provided by Azure Security Center to help you address the security issue that triggered the alert.

These recommendations are designed to guide you in taking necessary actions to improve your security posture and mitigate the identified risks.

So, selecting the alert, choosing "Take Action," and expanding the "Prevent future attacks" section is a valid approach to view recommendations and meet the goal of resolving the alert in Azure Security Center.

upvoted 4 times

Ramye 10 months, 2 weeks ago

I think the key is - this will mitigate the future identified risks not the one in hand…

upvoted 3 times

exmITQS 1 year, 10 months ago

Selected Answer: A

A. Yes, this solution meets the goal. From the Security alerts blade in Azure Security Center, you can select the alert that you want to investigate, and then select Take Action. The Take Action blade provides a list of recommendations that you can take to resolve the alert, including how to prevent future attacks. You can expand the Prevent future attacks section to view the recommendations.

upvoted 1 times

Holii 1 year, 8 months ago

The 'Prevent Future Attacks' option here shows top security recommendations in association on entities affected by the alert to help reduce the attack surface. These methods are not targeting the specific alert, to see that we need to select "Mitigate the Threat"

@Metasploit is correct.

upvoted 1 times

alexb1 1 year, 10 months ago

Just a FYI Security Center is now called Defender for Cloud (as far as I can tell). There's also a Security Center under Azure -> Security but it doesn't seem to be the one referred to in this question.

upvoted 3 times

Ramye 11 months ago

M365 Security Center is now Called Microsoft (365) Defender. Note - the url still shows security..

Azure security is called Defender for Cloud.

upvoted 1 times

Atun23 2 years, 2 months ago

Correct

Mitigate the threat - provides manual remediation steps for this security alert

Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts

upvoted 1 times

amsioso 2 years, 3 months ago

B is correct:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-incident

upvoted 1 times

vnez 2 years, 4 months ago

Answer should be A - On the Security Alert > Take Action > Prevent future attacks -- this will give you a list of active security recommendations on the affected resource

* Mitigate the threat - provides manual remediation steps for this security alert

* Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks

upvoted 3 times

Question #2 *Topic 2*

You receive an alert from Azure Defender for Key Vault.
You discover that the alert is generated from multiple suspicious IP addresses.
You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.
What should you do first?

A. Modify the access control settings for the key vault.

B. Enable the Key Vault firewall.

C. Create an application security group.

D. Modify the access policy for the key vault.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

Community vote distribution
B (100%)

teehex Highly Voted 3 years, 7 months ago
The given answer is correct. You create firewall rules and adds trusted range to ensure Key Vault can only be accessed from those trusted IP addresses while you are doing investigation.
upvoted 29 times

ture 3 years, 5 months ago
Yes! It makes sense. Good strategy
upvoted 2 times

ubt 2 years, 2 months ago
Shouldn't the firewall already be turned on? There fore why would a solution be to Turn the Firewall on??? This can't be the correct answer
upvoted 2 times

daiablo 1 year, 7 months ago
By default the network configuration allows access from all networks. "Turned on" is possibly not the correct phrasing, but you should configure to only allow from a list and specify the IPs/CIDR ranges
upvoted 1 times

AnonymousJhb 2 years, 9 months ago
Think of access policies as management of users / accounts with their restrictive permissions.
Think of the firewall as managment of networks, cidrs, ips based type resources.
upvoted 7 times

cw3364903 Highly Voted 2 years, 6 months ago
Selected Answer: B
B is the best answer possible here...why was the firewall not on in the first place ha!
upvoted 9 times

uday1985 1 year, 8 months ago
was the firewall configured to allow specific IPs to access the Vault? dont think so! Firewalls are enabled by default! but when it was configured to prevent access from specific IPs
upvoted 1 times

Nikki0222 Most Recent 2 months, 1 week ago
B correct
upvoted 1 times

chepeerick 1 year, 2 months ago
correct
upvoted 1 times

danb67 1 year, 2 months ago

By default, when you create a new key vault, the Azure Key Vault firewall is disabled. All applications and Azure services can access the key vault and send requests to the key vault. So answer is correct.

upvoted 1 times

jamclash 1 year, 3 months ago

in exam 9/20/23

upvoted 2 times

tatendazw 1 year, 7 months ago

Correct https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-key-vault-introduction#step-2-respond-accordingly

upvoted 1 times

RobertDuval 1 year, 8 months ago

In Exam today (21 April 2023)

upvoted 4 times

Metasploit 2 years, 2 months ago

Selected Answer: B

According to reference the answer is correct: B Enable Key Vault Firewall.

If the traffic came from an unrecognized IP Address:
Enable the Azure Key Vault firewall as described in Configure Azure Key Vault firewalls and virtual networks. Configure the firewall with trusted resources and virtual networks.

If the source of the alert was an unauthorized application or suspicious user:
Open the key vault's access policy settings. Remove the corresponding security principal, or restrict the operations the security principal can perform.

If the source of the alert has an Azure Active Directory role in your tenant:
Contact your administrator.
Determine whether there's a need to reduce or revoke Azure Active Directory permissions.

upvoted 4 times

CatoFong 2 years, 5 months ago

Selected Answer: B

B is correct

upvoted 1 times

Tx4free 2 years, 10 months ago

Selected Answer: B

Best answer

upvoted 2 times

stromnessian 2 years, 10 months ago

Selected Answer: B

Correct answer IMO.

upvoted 1 times

Task 3 years, 7 months ago

Given answer was correct

upvoted 1 times

Question #3 *Topic 2*

HOTSPOT -

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

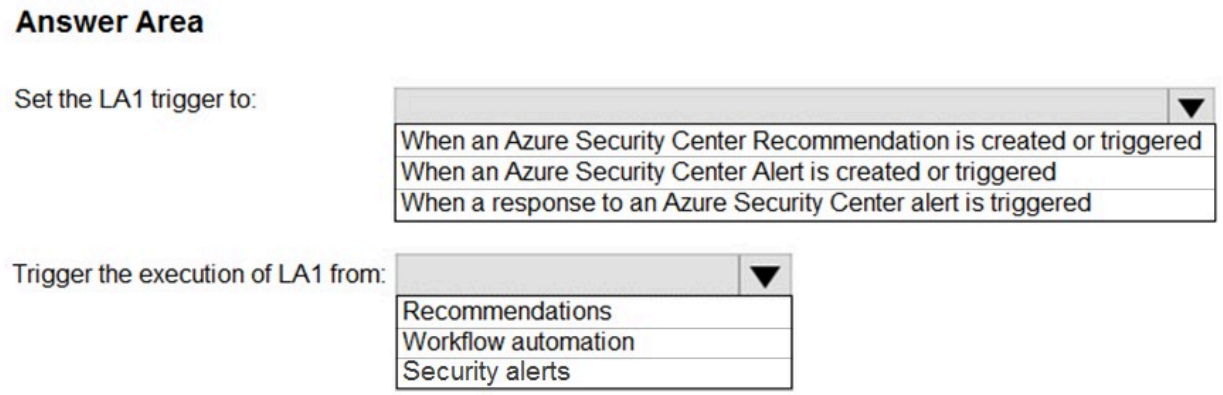
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

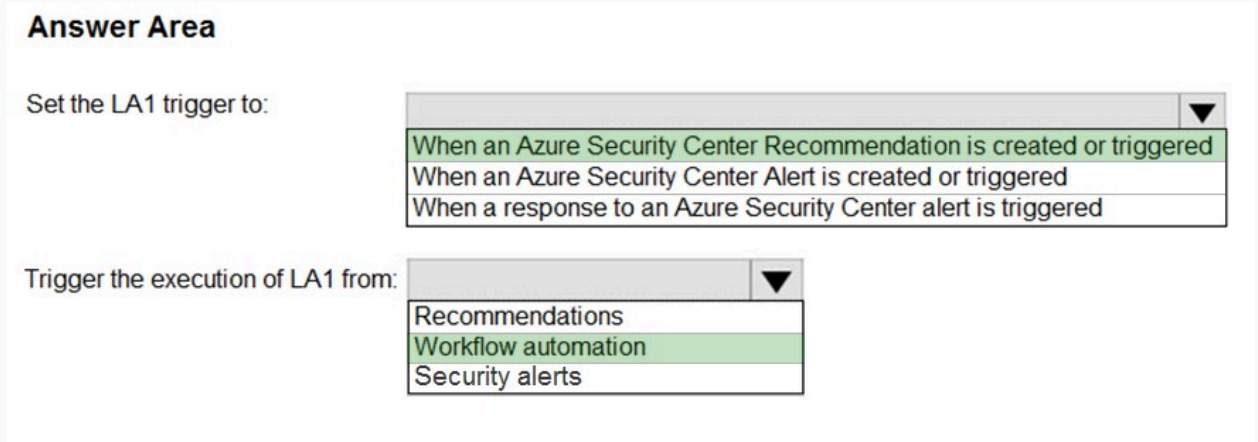
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

Banzaaai Highly Voted 2 years, 11 months ago

passed exam 31-Jan-2022, and answer Workflow Automation was not on exam...

so.. I have chosen : Security Alerts

upvoted 27 times

Nikki0222 2 months, 1 week ago

CORRECT

upvoted 1 times

HAjouz 3 weeks, 1 day ago

If you review the docs - where it says Manually trigger a logic app -> you see trigger logic is under security alerts

upvoted 1 times

emartiy 7 months ago

Since Workflow was newly added... There was also Security Alerts option in your exam. Newly added opttion is worng. So recommendations option is strongly true if it was an option in your exam :=) I got copilot to answer this and shared result in my comment for first select first option for second select first option.

upvoted 2 times

Tracebuster 2 years, 11 months ago

This is why I would go with Recommendation as the 2nd answer option

https://docs.microsoft.com/en-us/azure/azure-monitor/reference/tables/securitynestedrecommendation

upvoted 11 times

Ramye 11 months ago

How do you decipher/conclude the answer is recommendation from this link?

upvoted 2 times

AnonymousJhb 2 years, 9 months ago

Automate responses to Microsoft Defender for Cloud triggers using workflow automation - the trigger conditions selected is “Security alert”

https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

upvoted 3 times

Lion007 2 years, 6 months ago

Agreeing with this answer, and add to it that you can actually find the "Trigger logic app" when you open both "Security alerts" and "Recommendations". This is mentioned in the docs page "To manually run a Logic App, open an alert or a recommendation and click Trigger Logic App:" https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#manually-trigger-a-logic-app

upvoted 1 times

amsioso 2 years, 3 months ago

"security risks detected" not alerts, incidents... go with recommendations.

upvoted 3 times

Whatsamattr81 Highly Voted 2 years, 4 months ago

"automatically remediate security risks detected" - risks is the key word, that (to me) assumes the recommendations - and not alerts (which would be incidents). And it would be triggered on recommendations.

upvoted 12 times

cdgdhj Most Recent 2 months, 2 weeks ago

what's the final answer?

upvoted 1 times

talosDevbot 2 months, 4 weeks ago

"When an Azure Security Center Recommendation is created or triggered"

"Recommendations"

Important part of the question: "You need to test LA1 in Security Center"

To test a Logic app, you want to manually trigger the app. To do this, you go to Recommendations > open a recommendation > select "Trigger a logic app"

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#manually-trigger-a-logic-app

upvoted 1 times

dyavlito 4 months, 1 week ago

The given anwser is correct:

To test the Azure Logic App (LA1) in Security Center, you should configure the following options:

Set the LA1 trigger to:

When an Azure Security Center alert is created or triggered

Trigger the execution of LA1 from:

Workflow automation

This setup will allow LA1 to be automatically triggered when a security alert is created or triggered in Azure Security Center, and you can test its functionality through the workflow automation feature.

upvoted 1 times

g_man_rap 4 months, 1 week ago

Second.

Second.

Why Not "Recommendations"?

If you select "When an Azure Security Center Recommendation is created or triggered," the Logic App would run whenever a recommendation is generated. However, since recommendations are not active threats but rather suggestions, this would not align with the objective of remediating actual security risks.
upvoted 1 times

ostralo 9 months, 4 weeks ago
1. security risks - Security recommendations

IMO, security threats are for Security Alert

2. Manually trigger a logic app
You can also run logic apps manually when viewing any security alert or recommendation.
To manually run a logic app, open an alert, or a recommendation and select Trigger logic app.

We set the LA to be triggered by Security Recommendation that means we can manually trigger it via the Security Recommendation.
upvoted 3 times

smanzana 1 year, 1 month ago
1. When an Azure Security Centre Recommendation is created or triggered
2. Security Alerts
upvoted 2 times

blacksheep_29 1 year, 1 month ago
My opinion is for LA1 to trigger should be based on the Alert and Proof is below -

logicAppResourceId": {
"type": "String",
"metadata": {
"displayName": "Logic App",
"description": "The Logic App that is triggered.",
"strongType": "Microsoft.Logic/workflows",
"assignPermissions": true
}
},
"logicAppTrigger": {
"type": "String",
"metadata": {
"displayName": "Logic app trigger",
"description": "The trigger connector of the logic app that is triggered. Possible values: 'Manual (Incoming HTTP request)', 'When an Azure Security Center Alert is created or triggered'."

The above mentioned is the code for Logic App config which is set to trigger when an Azure Security alert is created or triggered.

Correct me If I'm wrong
upvoted 1 times

chepeerick 1 year, 2 months ago
check answer
upvoted 1 times

cris_exam 1 year, 3 months ago
Based on this below article about a similar lab this lad did, I think the answer is:

1. When an Azure Security Centre Recommendation is created or triggered
2. Security Alerts

https://security.packt.com/setting-up-automated-threat-response-in-microsoft-defender-for-cloud-azure-security-center/

Open for debate though...
upvoted 4 times

donathon 1 year, 4 months ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run
trigger based on alerts and workspace automation
upvoted 1 times

billo79152718 1 year, 5 months ago
First one is correct.
Second is: Security Alerts
upvoted 1 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 4 times

AK4U_111 1 year, 6 months ago
be careful not to mistake with Question #39
upvoted 1 times

tatendazw 1 year, 7 months ago
Trigger is Security alert because of security risk. Workflow automation used to response to a security risk/incident
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run
upvoted 1 times

AJ2021 1 year, 10 months ago
Question in Exam today
upvoted 8 times

Question #4 *Topic 2*

You have a Microsoft 365 subscription that uses Azure Defender.
You have 100 virtual machines in a resource group named RG1.
You assign the Security Admin roles to a new user named SecAdmin1.
You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.
Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription

B. the Contributor for the subscription

C. the Contributor role for RG1

D. the Owner role for RG1

Suggested Answer: *C*

Community vote distribution

C (100%)

somsom Highly Voted 3 years, 9 months ago
correct. contributors has edit, read and view access
upvoted 23 times

Eltooth Highly Voted 3 years, 7 months ago
Agreed - Contributor rights on RG is minimum permission needed.
upvoted 10 times

Nikki0222 Most Recent 2 months, 1 week ago
C correct
upvoted 1 times

DChilds 8 months, 1 week ago
Selected Answer: C
This question was in the exam 27/04/2024.
upvoted 4 times

chepeerick 1 year, 2 months ago
option C as contributor to resource
upvoted 1 times

EricShon 1 year, 4 months ago
Selected Answer: C
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 1 times

Apocalypse03 2 years ago
Selected Answer: C
To ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender, while also following the principle of least privilege, you should assign the Contributor role for RG1 to SecAdmin1.

The Contributor role for RG1 will allow SecAdmin1 to perform tasks such as deploying resources and modifying resource properties within RG1, but it will not grant them access to perform administrative tasks at the subscription level. This will allow SecAdmin1 to apply quick fixes to the virtual machines using Azure Defender, while still adhering to the principle of least privilege.
upvoted 10 times

Tx4free 2 years, 10 months ago
Selected Answer: C
Best answer
upvoted 5 times

liberty123 2 years, 10 months ago

Selected Answer: C

should be C

upvoted 4 times

Ana22 2 years, 10 months ago

Selected Answer: C

Correct

upvoted 4 times

stromnessian 2 years, 11 months ago

Selected Answer: C

Contributor role for RG.

upvoted 3 times

Task 3 years, 7 months ago

Agreed, correcr answer

upvoted 4 times

Question #5 *Topic 2*

You provision a Linux virtual machine in a new Azure subscription.
You enable Azure Defender and onboard the virtual machine to Azure Defender.
You need to verify that an attack on the virtual machine triggers an alert in Azure Defender.
Which two Bash commands should you run on the virtual machine? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. cp /bin/echo ./asc_alerttest_662jfi039n

B. ./alerttest testing eicar pipe

C. cp /bin/echo ./alerttest

D. ./asc_alerttest_662jfi039n testing eicar pipe

Suggested Answer: *AD*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux-

Community vote distribution
AD (94%) 6%

somsom Highly Voted 3 years, 9 months ago
correct
upvoted 18 times

AlaReAla Highly Voted 3 years, 3 months ago
Why is it so important to copy the file ONLY as "asc_alerttest_662jfi039n". Please consider that I am a newbie in securities, and help guide me, thanks.
upvoted 11 times

kakakayayaya 3 years, 1 month ago
any legal file name can be used
upvoted 1 times

03allen 2 years ago
seems not right as BC's only difference is the file name
upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago
AD correct
upvoted 1 times

asquante 10 months, 1 week ago
The answer is correct, but the question itself is outdated. The doc link now shows a much simpler command curl -O
https://secure.eicar.org/eicar.com.txt
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation#simulate-alerts-on-your-azure-vms-linux-
upvoted 3 times

Ramye 11 months ago
Note: There's no Azure Defender now. It is now Defender for Cloud. So this might be (should be) reflected in the exam if this is asked..
upvoted 3 times

chepeerick 1 year, 2 months ago
Option AD
upvoted 1 times

cris_exam 1 year, 3 months ago
Seems right as it is.

Check this doc link below from step 3.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation#simulate-workload-alerts-k8snode_-prefix

"Copy the executable to a separate location and rename it to ./asc_alerttest_662jfi039n with the following command cp /bin/echo ./asc_alerttest_662jfi039n.

Execute the file ./asc_alerttest_662jfi039n testing eicar pipe."

upvoted 3 times

Oryx360 1 year, 4 months ago

Selected Answer: CD

To verify that an attack on the virtual machine triggers an alert in Azure Defender, you can use a test utility provided by Microsoft called "asc-alert-test." This utility is designed to safely simulate attacks and generate alerts for testing purposes.

The correct commands are:

C. cp /bin/echo ./alerttest
D. ./asc_alerttest_662jfi039n testing eicar pipe

Explanation:

Command C: Copies the /bin/echo binary to create a test utility named alerttest which will be used to simulate the attack.
Command D: Executes the asc_alerttest_662jfi039n utility with the appropriate parameters (testing eicar pipe) to simulate the attack and generate the alert.
Commands A and B are incorrect because they refer to incorrect utility names or parameters.

Remember, while using this utility, ensure you have necessary permissions and follow your organization's policies for testing and verifying security controls.

upvoted 1 times

imhere4you 1 year, 6 months ago

On exam - 19 June 2023

upvoted 5 times

tatendazw 1 year, 7 months ago

1. rename executable to ./asc_alerttest_662jfi039n
2. cp /bin/echo ./asc_alerttest_662jfi039n
3. Run in command prompt ./asc_alerttest_662jfi039n testing eicar pipe
4. Check Defender for Cloud alerts after about 10 mins to see an alert

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation#simulate-alerts-on-your-azure-vms-linux-

upvoted 3 times

teouba 1 year, 8 months ago

These answers are ridiculous, what is the difference if we choose B and C?
They are the exact same commands with different naming for the file

upvoted 2 times

Holii 1 year, 8 months ago

I believe the filename has to follow this strict naming convention to trigger the validation alert. This is used for validation testing without requiring an actual malicious file. If they had it on every file it'd be throwing alerts on every .exe, cause it's not like you're running anything inherently 'bad'.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation#simulate-alerts-on-your-azure-vms-linux-

upvoted 5 times

aruninsiva 1 year, 5 months ago

yes. '662jfi039n' is the alert triggering filename.

upvoted 1 times

CatoFong 2 years, 5 months ago

Selected Answer: AD

correct

upvoted 3 times

feln 2 years, 9 months ago

Selected Answer: AD

correct

upvoted 3 times

TomG 2 years, 9 months ago

Selected Answer: AD

Given answers are correct

upvoted 4 times

Ken88 2 years, 9 months ago

Selected Answer: AD

correct

upvoted 3 times

iov 2 years, 10 months ago

correct

upvoted 2 times

stromnessian 2 years, 10 months ago

Selected Answer: AD

AD is correct I'd say.

upvoted 3 times

Question #6 *Topic 2*

You create an Azure subscription named sub1.
In sub1, you create a Log Analytics workspace named workspace1.
You enable Azure Security Center and configure Security Center to use workspace1.
You need to collect security event logs from the Azure virtual machines that report to workspace1.
What should you do?

A. From Security Center, enable data collection

B. In sub1, register a provider.

C. From Security Center, create a Workflow automation.

D. In workspace1, create a workbook.

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Community vote distribution
A (95%) 5%

stromnessian Highly Voted 2 years, 11 months ago

Selected Answer: A

Data collection
Store additional raw data - Windows security events
To help audit, investigate, and analyze threats, you can collect raw events, logs, and additional security data and save it to your Log Analytics workspace.
upvoted 13 times

Nickname01 2 years, 2 months ago

Answer A is correct: you go to your Log analytics workspace -> agent management -> Data collection rules, here you would create a new rule and add the Windows Event logs and select the security logs.
upvoted 6 times

Ramye 10 months, 2 weeks ago

Thx for sharing the steps.
Just one quick note if anyone is trying out the steps…
The agent management page is accessible by clicking Agents under the Settings on the Log-Analytics-workspace page.
upvoted 1 times

zole Highly Voted 3 years ago

uuuuuuuuuuuuuuuuuuuu
upvoted 8 times

Nikki0222 Most Recent 2 months, 1 week ago

A answer
upvoted 1 times

Nikki0222 2 months, 1 week ago

A correct
upvoted 1 times

chepeerick 1 year, 2 months ago

Correct A
upvoted 1 times

Oryx360 1 year, 4 months ago

Selected Answer: B

B. In sub1, register a provider.

To collect security event logs from the Azure virtual machines reporting to workspace1, you need to register a data collection provider. This action allows Azure Monitor to collect logs and data from the resources and send it to the specified Log Analytics workspace.

upvoted 1 times

AK4U_111 1 year, 6 months ago

The Log Analytics agents won't be supported as of August 31, 2024. Plan to migrate to Azure Monitor Agent prior to this date. If you've already installed Azure Monitor Agent, make sure to create and associate data collection rules to the agents.

upvoted 4 times

feln 2 years, 9 months ago

Selected Answer: A

correct

upvoted 2 times

Tx4free 2 years, 10 months ago

Selected Answer: A

Best answer

upvoted 3 times

somsom 3 years, 4 months ago

correct

upvoted 5 times

Question #7 *Topic 2*

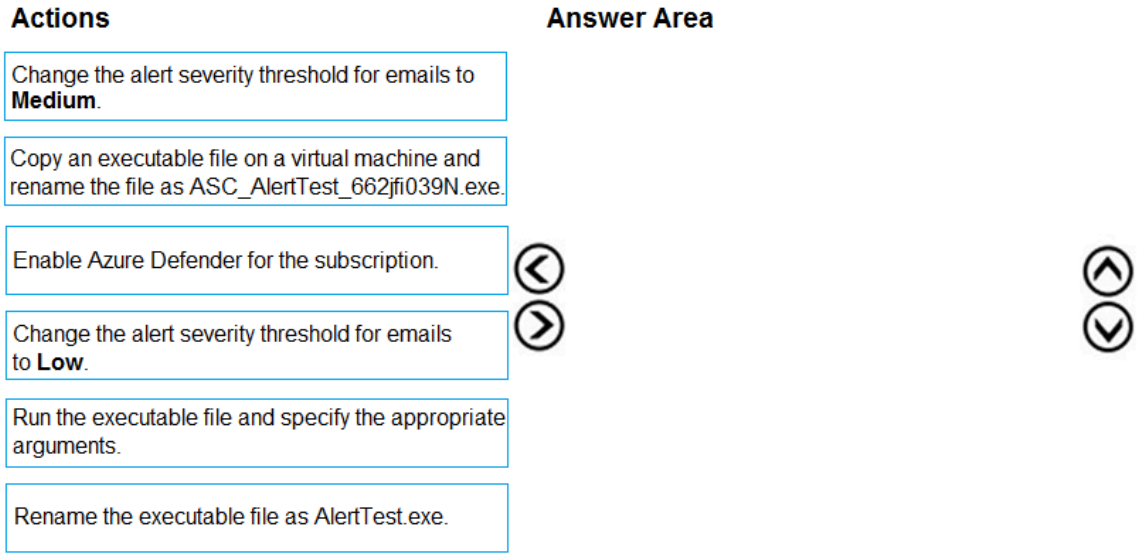
DRAG DROP -

You create a new Azure subscription and start collecting logs for Azure Monitor.

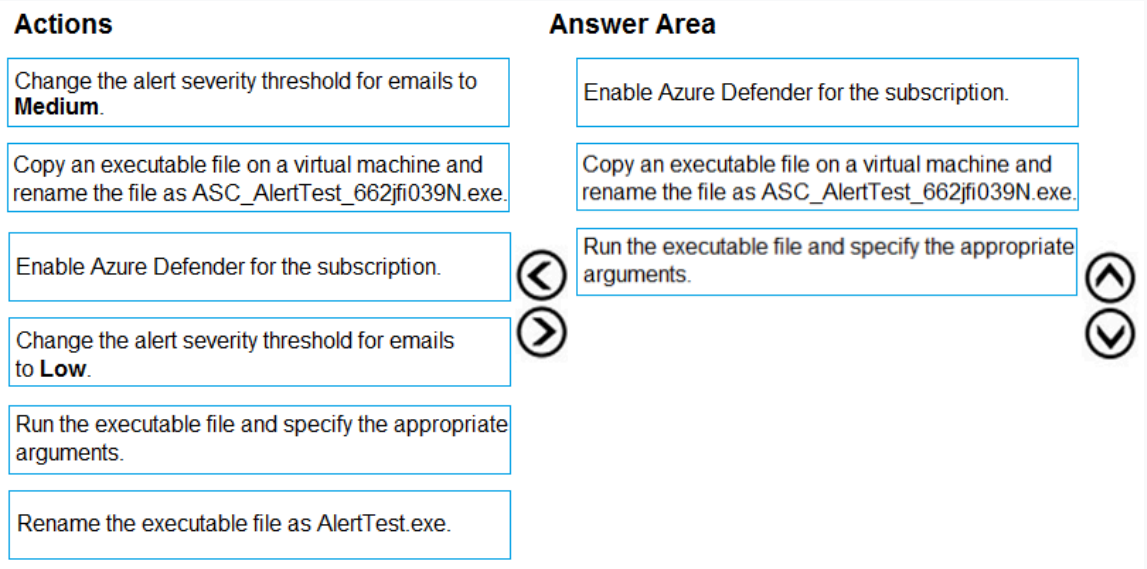
You need to configure Azure Security Center to detect possible threats related to sign-ins from suspicious IP addresses to Azure virtual machines. The solution must validate the configuration.

Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation

ubt Highly Voted 1 year, 8 months ago

OMG... was pulling my hair out as none of these except enable MS Defender seemed related to the question.. typical MS questions

upvoted 18 times

Gurulee 6 months ago

yeah, the question had me focusing on MCAS and IP's that would be tagged as suspicious. The AV file trigger test threw me off

upvoted 1 times

Lone_Wolf 1 year, 4 months ago

Same here!

upvoted 4 times

Task Highly Voted 3 years, 1 month ago

True. Correct answer given

upvoted 17 times

asquante Most Recent 4 months, 1 week ago

The answer is correct, but outdated - done with Powershell now

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation#simulate-alerts-on-your-azure-vms-windows-

upvoted 1 times

teouba 1 year, 2 months ago

The key is in the phrase "The solution must validate the configuration."

So they dont ask how you are going to configure, but how you are going to validate.

upvoted 5 times

cs4vEr 3 years, 1 month ago

https://docs.microsoft.com/en-us/azure/security-center/security-center-alert-validation#simulate-alerts-on-your-azure-vms-linux- is not related to suspicious login BTW, the answer is the only one possible

upvoted 9 times

somsom 3 years, 3 months ago

correct

upvoted 4 times

Question #8 *Topic 2*

Your company uses Azure Security Center and Azure Defender.

The security operations team at the company informs you that it does NOT receive email notifications for security alerts.
What should you configure in Security Center to enable the email notifications?

A. Security solutions

B. Security policy

C. Pricing & settings

D. Security alerts

E. Azure Defender

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details

Community vote distribution
C (100%)

powerjoev2 Highly Voted 2 years, 6 months ago
Outdated it should be in the "Environment Settings" -> "Email notifications"
upvoted 51 times

Jos8 2 years, 6 months ago
This configuration can be found at Microsoft Defender for Cloud Apps now??
upvoted 3 times

Ramye 5 months ago
Not a defender for Cloud Apps but MS Defender for Cloud. This is tied with the Azure subscription and can be used for multi-cloud security measures / protections
upvoted 1 times

tatendazw 1 year ago
In Azure portal search for MS Defender for Cloud then scroll down to Enviroment Settings, select AZ subscription and the Email notifications
https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications
upvoted 5 times

stromnessian Highly Voted 2 years, 4 months ago
Selected Answer: C
Environment settings -> click subscription -> Email notifications
upvoted 18 times

Ramye 5 months ago
Yep - found it - thx
upvoted 1 times

Ramye Most Recent 5 months ago
Azure Security Center and Azure Defender is now Microsoft Defender for Cloud

And email notification setting can be found at

Environment settings -> click subscription -> Email notifications

Thx to stromnessian for the steps
upvoted 1 times

kazaki 5 months ago
out dated

upvoted 1 times

smanzana 7 months, 3 weeks ago

Pricing & Settings

(But now it is “Environment settings”)

upvoted 1 times

taoufik109 9 months, 1 week ago

Microsoft Defender for Cloud | Environment settings | subscription then open Email nitifications

upvoted 1 times

TiredofTesting 1 year, 6 months ago

Deprecated:

From Defender for Cloud's Environment settings area, select the relevant subscription, and open Email notifications.

Define the recipients for your notifications with one or both of these options:

From the dropdown list, select from the available roles.

Enter specific email addresses separated by commas. There's no limit to the number of email addresses that you can enter.

upvoted 6 times

palito1980 1 year, 5 months ago

Verified on a test tenant

upvoted 1 times

liberty123 2 years, 4 months ago

Selected Answer: C

Pricing & Settings

upvoted 1 times

kakakayayaya 2 years, 7 months ago

Now it is Environment settings.

Have MS changed exam after recent renaming a whole Defender solutions?

upvoted 8 times

Atun23 1 year, 8 months ago

Not until Nov 4 2022

upvoted 1 times

Eltooth 2 years, 8 months ago

Correct - Pricing & Settings.

upvoted 1 times

Task 3 years, 1 month ago

Given answer was correct.

upvoted 1 times

somsom 3 years, 3 months ago

correct. the navigation is as follows home - security center- pricing and settings

upvoted 10 times

Question #9 *Topic 2*

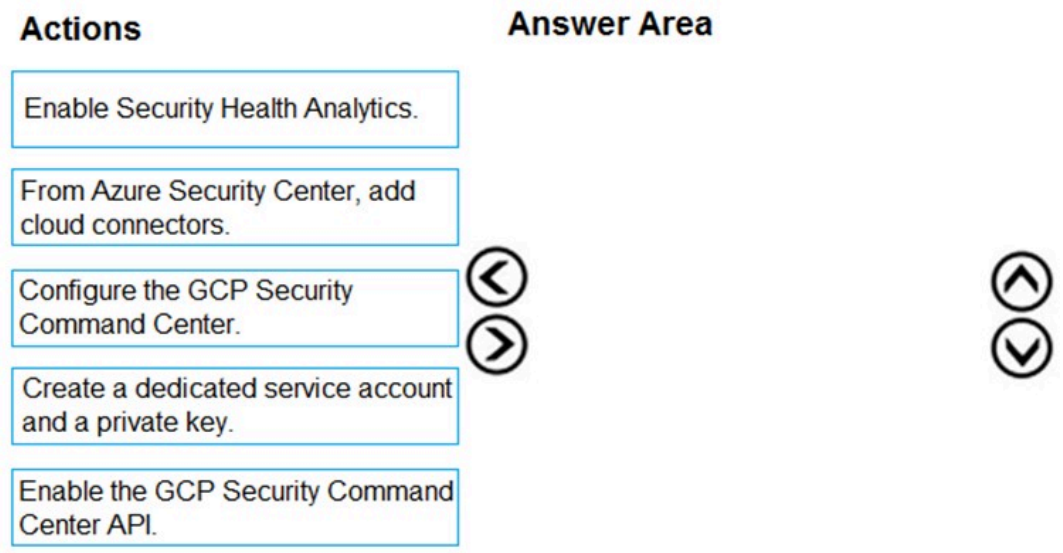
DRAG DROP -

You have resources in Azure and Google cloud.

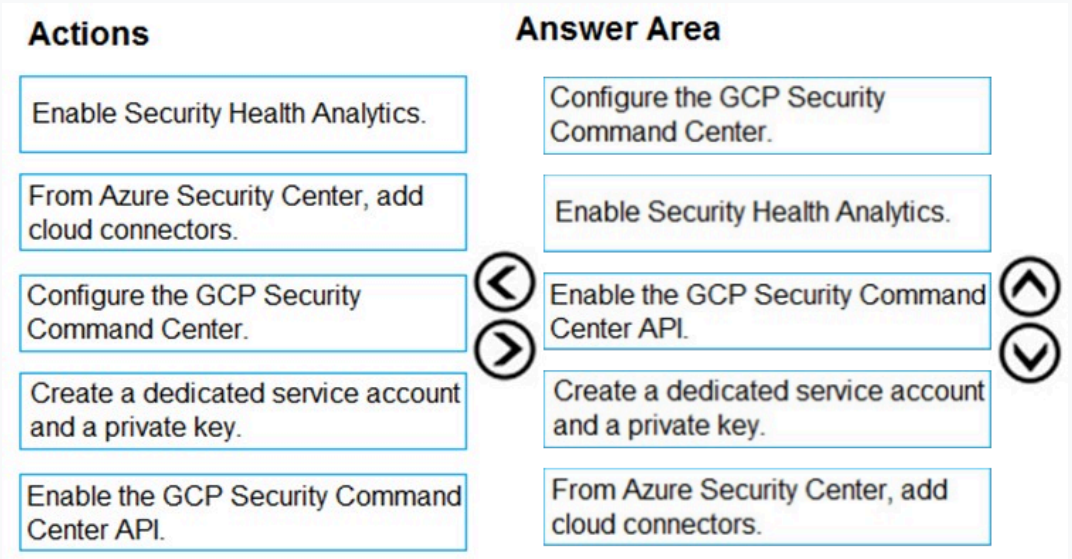
You need to ingest Google Cloud Platform (GCP) data into Azure Defender.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-onboard-gcp

Yeuri Highly Voted 2 years ago

No longer a valid answer, in order to do this you need to go to Microsoft Defender for cloud apps > Environment settings > add environment > GCP

upvoted 28 times

Ramye 11 months ago

Just a minor correction

It's not Microsoft Defender for cloud apps but rather Microsoft Defender for Cloud.

Microsoft Defender for cloud apps is part of Microsoft Defender XDR (formally M365 Defender).

upvoted 5 times

Lone_Wolf Highly Voted 1 year, 10 months ago

Since this is outdated this is the new Sequence

Configure Google Cloud Platform

Create a dedicated project in GCP

Enable required APIs
Create a dedicated service account for the security auditing integration
Create a private key for the dedicated service account
Retrieve your Organization ID
Connect Google Cloud Platform auditing to Defender for Cloud Apps

https://learn.microsoft.com/en-us/defender-cloud-apps/connect-google-gcp
upvoted 23 times

Ramye 11 months ago
I think the information with the link below, is more relevant to this specific question.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp
upvoted 1 times

g_man_rap Most Recent 4 months, 1 week ago
Correct Order:

Create a dedicated service account and a private key.
Enable the GCP Security Command Center API.
Configure the GCP Security Command Center.
Enable Security Health Analytics.
From Azure Security Center, add cloud connectors.
upvoted 2 times

danlo 1 year, 1 month ago
Not sure why people are posting documentation to Cloud Apps, it's clearing a Defender for Cloud question https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp?pivots=classic-connector#connect-your-gcp-project
upvoted 2 times

chepeerick 1 year, 2 months ago
out of date
upvoted 1 times

Snaileyes 2 years, 1 month ago
...more specifically:
https://learn.microsoft.com/en-us/defender-cloud-apps/connect-google-gcp#how-to-connect-gcp-security-configuration-to-defender-for-cloud-apps
upvoted 2 times

Snaileyes 2 years, 1 month ago
Here's a better reference for the sequence:
https://learn.microsoft.com/en-us/defender-cloud-apps/connect-google-gcp
upvoted 4 times

hommatch380 2 years, 3 months ago
Reference:
https://docs.microsoft.com/ja-jp/azure/defender-for-cloud/quickstart-onboard-gcp?pivots=classic-connector
upvoted 1 times

hommatch380 2 years, 3 months ago
English is here
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp?pivots=classic-connector
upvoted 3 times

hamedhy 1 year, 10 months ago
This is the just right answer, thanks!
upvoted 1 times

hardinxcore 2 years, 4 months ago
No it's not conflict correct anymore. Then links shows the native connection and the classic connection. This question is the classic connection and not the native
upvoted 2 times

vincenttoolate 2 years, 6 months ago
These answer might be outdated already. According to the doc:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp?pivots=env-settings#connect-your-gcp-project

We copy the GCP Cloud Shell script from the GCP Connector, then run it at GCP Cloud Shell, and then we have an auto-generated service account

upvoted 4 times

AGROS 3 years ago

Seems like according to the link https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp

Step 2. Enable GCP Security Command Center API

upvoted 2 times

AGROS 3 years ago

My fault: Screen data is correct

Disregard the previous message.

For all the GCP projects in your organization, you must also:

Set up GCP Security Command Center using these instructions from the GCP documentation.

Enable Security Health Analytics using these instructions from the GCP documentation.

upvoted 1 times

Eltooth 3 years, 3 months ago

Correct sequence.

upvoted 11 times

Task 3 years, 7 months ago

Given answer was correct

upvoted 2 times

Silent_Muzinde 3 years, 7 months ago

the provided answer is correct

upvoted 1 times

Question #10 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Regulatory compliance, you download the report.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution
B (100%)

Nikki0222 2 months, 1 week ago
No correct
upvoted 1 times

Ramye 10 months, 2 weeks ago
Can someone clarify the below, please?
Microsoft said, "Azure Security Center and Azure Defender are now Microsoft Defender for Cloud". So why do we still see the Azure Security Center in the Azure portal?

Just trying to get some clarification on this. Thx
upvoted 1 times

thmsilverknight 5 months, 3 weeks ago
this looks like an outdated question
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

Abdul11 2 years, 5 months ago
Correct answer
upvoted 1 times

LadyDiana 2 years, 9 months ago
Selected Answer: B
Based on the link, once you are on the full details page of one of the alerts,
1. Click on “Next: Take Action”
2. Select: “Prevent future attacks” - as this provides security recommendations
upvoted 3 times

LadyDiana 2 years, 9 months ago
In addition to #2, you can either choose “Prevent future attacks” OR “Mitigate the threat” as options since the “Mitigate the threat” provides remediation steps.
upvoted 5 times

Metasploit 2 years, 2 months ago

The correction option would be to choose "mitigate the threat" as the recommendations from this tab resolves the alert, whereas the other "Prevent.." Just provides recommendations in general.

upvoted 8 times

Tx4free 2 years, 10 months ago

Selected Answer: B

Best answer

upvoted 1 times

Eltooth 3 years, 3 months ago

Correct - No

upvoted 3 times

Task 3 years, 7 months ago

Correct answer

upvoted 1 times

malabar933 3 years, 7 months ago

Given answer is correct

upvoted 1 times

Question #11 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
Solution: From Security alerts, you select the alert, select Take Action, and then expand the Mitigate the threat section.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution
A (100%)

somsom Highly Voted 3 years, 9 months ago
very correct, you need to mitigate the issue
upvoted 11 times

ehsanhabib Highly Voted 2 years, 9 months ago
Selected Answer: A
cORRECT
upvoted 5 times

Nikki0222 Most Recent 2 months, 1 week ago
Yes correct
upvoted 1 times

Gurulee 1 year ago
Mitigate the threat - provides manual remediation steps for this security alert
Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks
upvoted 1 times

ggGG1357 1 year ago
Answer is very wrong.
It should be Prevent future attacks.
Prevent future attacks provides you with security recommendation while mitigate the threat provides you with remediation steps.
Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts
upvoted 1 times

ggGG1357 1 year ago
Mixed it up. After reviewing the documentation I provided again and since the question is dealing with an active alert then B is the correct option
upvoted 1 times

ggGG1357 1 year ago
Gosh. What's wrong with me. I mean A is correct. 100% sure
upvoted 1 times

Anil0512 1 year, 2 months ago
This answer is wrong.
No is the answer.

Microsoft Defender for Cloud > Security alerts, select/click an Alert>Take action > Prevent future attacks

upvoted 1 times

chepeerick 1 year, 2 months ago

correct

upvoted 1 times

sand5234 1 year, 3 months ago

Correct Answer should be No

upvoted 1 times

tatendazw 1 year, 6 months ago

Microsoft Defender for Cloud > Security alerts, select/click an Alert>Take action https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts

upvoted 1 times

Tx4free 2 years, 10 months ago

Selected Answer: A

Best option

upvoted 3 times

stromnessian 2 years, 10 months ago

Selected Answer: A

Looks right to me.

upvoted 3 times

Eltooth 3 years, 3 months ago

Correct.

upvoted 2 times

Task 3 years, 7 months ago

Yes, Correct

upvoted 2 times

kwach 3 years, 8 months ago

answer is A

upvoted 3 times

Question #12 *Topic 2*

You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You need to configure the continuous export of high-severity alerts to enable their retrieval from a third-party security information and event management (SIEM) solution.
To which service should you export the alerts?

A. Azure Cosmos DB

B. Azure Event Grid

C. Azure Event Hubs

D. Azure Data Lake

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/continuous-export?tabs=azure-portal

Community vote distribution
C (100%)

HSBNZ Highly Voted 3 years, 4 months ago
Correct answer, from the provided link in the answer it is explained: Continuous export lets you fully customize what will be exported, and where it will go. For example, you can configure it so that:

All high severity alerts are sent to an Azure Event Hub
All medium or higher severity findings from vulnerability assessment scans of your SQL servers are sent to a specific Log Analytics workspace
Specific recommendations are delivered to an Event Hub or Log Analytics workspace whenever they're generated
The secure score for a subscription is sent to a Log Analytics workspace whenever the score for a control changes by 0.01 or more
upvoted 21 times

Nikki0222 Most Recent 2 months, 1 week ago
C answer
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct C
upvoted 1 times

trashbox 1 year, 3 months ago
The answer is correct. Azure Event Hubs.

"Third-party SIEMs - Send data to Azure Event Hubs."
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-schemas?tabs=schema-sentinel
upvoted 1 times

Tx4free 2 years, 10 months ago
Selected Answer: C
Best answer
upvoted 3 times

dangerdizzy 2 years, 11 months ago
Yes the answer is correct. event hubs.
upvoted 2 times

Eltooth 3 years, 3 months ago
Correct answer - Event Hubs.
upvoted 4 times

Question #13 *Topic 2*

You are responsible for responding to Azure Defender for Key Vault alerts.
During an investigation of an alert, you discover unauthorized attempts to access a key vault from a Tor exit node.
What should you configure to mitigate the threat?

A. Key Vault firewalls and virtual networks

B. Azure Active Directory (Azure AD) permissions

C. role-based access control (RBAC) for the key vault

D. the access policy settings of the key vault

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/network-security

Community vote distribution
A (100%)

Eltooth Highly Voted 3 years, 3 months ago
A is correct.
B has nothing to do with Key Vault.
C & D only check against user permissions to key vault and not suspicious IP addresses.
upvoted 66 times

NickHSO 3 years ago
upvote for additional knowledge
upvoted 12 times

Haha0010 Highly Voted 1 year, 11 months ago
Selected Answer: A
In exam today (16 jan 2023)
upvoted 13 times

xRiot007 Most Recent 4 weeks, 1 day ago
Selected Answer: A
The issue here is that the request comes from Tor. While I do not agree with corporations blocking the use of Tor, the correct answer is A - a firewall can deal with such.
upvoted 1 times

Nikki0222 2 months, 1 week ago
A correct
upvoted 1 times

chepeerick 1 year, 2 months ago
option A
upvoted 1 times

albd 2 years ago
In Exam today (23 dec 2022)
upvoted 8 times

xbonex99 2 years, 5 months ago
If detection is based on IP or node (network). Solution would be firewall.
If detection is based on access or user related, then the solution is related with updating or modifying the policy.
upvoted 4 times

subhuman 2 years, 9 months ago
Selected Answer: A
Answer is correct. To be able to prevent unauthorized access to the key vault through suspicious IPs you have to change the networking settings under the key vault resource
upvoted 5 times

Question #14 *Topic 2*

HOTSPOT -

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
"resources": [
   {
     "type": "  [Microsoft.Automation / Microsoft.Logic / Microsoft.Security]  /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
              "actionType": "LogicApp",
              "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
              "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '  [Microsoft.Automation / Microsoft.Logic / Microsoft.Security]  /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
     ],
```

Suggested Answer:

Answer Area

```
"resources": [
   {
     "type": "  [Microsoft.Automation / Microsoft.Logic / Microsoft.Security]  /automations",
     "apiVersion": "2019-01-01-preview",
     "name": "[parameters('name')]",
     "location": "[parameters('location')]",
     "properties": {
        "description": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
           {
              "actionType": "LogicApp",
              "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
              "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '  [Microsoft.Automation / Microsoft.Logic / Microsoft.Security]  /workflows/triggers',
parameters('appName'), 'manual'), '2019-05-01').value]"
           }
     ],
```

Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

Discuss4certi Highly Voted 3 years, 2 months ago

correct, in the provided link you can find the json with this script.
https://raw.githubusercontent.com/Azure/azure-quickstart-templates/master/quickstarts/microsoft.security/securitycenter-create-automation-for-alertnamecontains/azuredeploy.json
upvoted 28 times

xRiot007 4 weeks, 1 day ago
Never understood Microsoft's fetish with knowing these from the top of your head. Zero value, tbh.
upvoted 3 times

albd Highly Voted 2 years ago
In Exam today (23 dec 2022)
upvoted 13 times

Murtuza Most Recent 1 year ago
resources": [
{
"type": "Microsoft.Security/automations",
"apiVersion": "2019-01-01-preview",
"name": "[parameters('automationName')]",
"location": "[parameters('location')]",
"properties": {
"description": "[format(variables('automationDescription'), parameters('subscriptionId'))]",
"isEnabled": true,
"actions": [
{
"actionType": "LogicApp",
upvoted 2 times

chepeerick 1 year, 2 months ago
Correct Answ
upvoted 1 times

imhere4you 1 year, 6 months ago
On exam - 19 June 2023
upvoted 5 times

RobertDuval 1 year, 8 months ago
In Exam today (21 April 2023)
upvoted 6 times

AJ2021 1 year, 10 months ago
Question in Exam today, but you have to choose the end option, for example, answer for second option is 'triggers'
upvoted 11 times

kushagrasharma172 2 years ago
The given answer is correct.
upvoted 2 times

Question #15 *Topic 2*

You have an Azure subscription that contains a Log Analytics workspace.
You need to enable just-in-time (JIT) VM access and network detections for Azure resources.
Where should you enable Azure Defender?

A. at the subscription level

B. at the workspace level

C. at the resource level

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/enable-azure-defender

Community vote distribution
A (100%)

Daniel9527 Highly Voted 2 years, 11 months ago
"Enabling it at the workspace level doesn't enable just-in-time VM access, adaptive application controls, and network detections for Azure resources. In addition, the only Microsoft Defender plans available at the workspace level are Microsoft Defender for servers and Microsoft Defender for SQL servers on machines."
Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
upvoted 14 times

Malik2165 Highly Voted 3 years ago
you can do it two ways
- at Subscription Level
- at Resource Level
upvoted 6 times

amsioso 2 years, 3 months ago
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction#defender-for-servers-plans
upvoted 1 times

amsioso 2 years, 3 months ago
But JIT Requires Microsoft Defender for Servers Plan 2 to be enabled on the subscription, then A is correct and best option.
upvoted 3 times

Nikki0222 Most Recent 2 months, 1 week ago
A correct
upvoted 1 times

VeiN 2 months, 2 weeks ago
Selected Answer: A
You can use Microsoft Defender for Cloud's just-in-time (JIT) access to protect your Azure virtual machines (VMs) from unauthorized network access.

Prerequisites: JIT requires Microsoft Defender for Servers Plan 2 to be enabled on the subscription.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage#prerequisites
upvoted 1 times

talosDevbot 3 months, 1 week ago
Selected Answer: A
Just-in-time virtual machine access locks down machine ports to reduce the attack surface. To use this feature, Defender for Cloud must be enabled on the subscription.

source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-select-plan
upvoted 1 times

MS_KoolaidMan 1 year ago

Selected Answer: A

It must be enabled at the Subscription level before it can be enabled at the resource level.
Tested in the "Secure Azure services and workloads with Microsoft Defender for Cloud regulatory compliance controls" Applied Skills Assessment
https://learn.microsoft.com/en-us/credentials/applied-skills/secure-azure-services-and-workloads-with-microsoft-defender-for-cloud-regulatory-compliance-controls/

upvoted 3 times

chepeerick 1 year, 2 months ago

correct A

upvoted 1 times

asterlvdw 1 year, 4 months ago

"For Azure resources." gives it away that it is for multiple resources so Subscription Level.

upvoted 4 times

Adom3730 1 year, 7 months ago

Selected Answer: A

Just-in-time virtual machine access locks down machine ports to reduce the attack surface. To use this feature, Defender for Cloud must be enabled on t

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-select-plan#plan-features:~:text=Just%2Din%2Dtime%20virtual%20machine%20access%20locks%20down%20machine%20ports%20to%20reduce%20the%20attack%20surfa

upvoted 3 times

TiredofTesting 2 years ago

Selected Answer: A

In Azure, -> Defender for Cloud -> Environment Settings -> select the subscription to enable all.

upvoted 2 times

Tx4free 2 years, 10 months ago

Selected Answer: A

Best option

upvoted 3 times

AnonymousJhb 2 years, 9 months ago

JIT Requires Microsoft Defender for Servers Plan 2 to be enabled on the subscription.

upvoted 2 times

Eltooth 3 years, 3 months ago

Correct - at Subscription level.

upvoted 4 times

HSBNZ 3 years, 4 months ago

You can protect an entire Azure subscription with Azure Defender and the protections will be inherited by all resources within the subscription.

upvoted 2 times

Question #16 *Topic 2*

You use Azure Defender.
You have an Azure Storage account that contains sensitive information.
You need to run a PowerShell script if someone accesses the storage account from a suspicious IP address.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From Azure Security Center, enable workflow automation.

B. Create an Azure logic app that has a manual trigger.

C. Create an Azure logic app that has an Azure Security Center alert trigger.

D. Create an Azure logic app that has an HTTP trigger.

E. From Azure Active Directory (Azure AD), add an app registration.

Suggested Answer: *AC*
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/azure-defender-storage-configure?tabs=azure-security-center
https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Community vote distribution
AC (100%)

Discuss4certi Highly Voted 3 years, 2 months ago
A +C looks ok.
Seems correct you want a security trigger for the login and you use this trigger to start the automation workflow with the powershellscript
upvoted 20 times

Tx4free Highly Voted 2 years, 10 months ago
Selected Answer: AC
Best options
upvoted 8 times

Nikki0222 Most Recent 2 months, 1 week ago
AC correct
upvoted 1 times

talosDevbot 3 months, 1 week ago
Selected Answer: AC
One of the supported trigger for in the Logic App designer is "When a Defender for Cloud Alert is created or triggered"

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 2 times

Ramye 11 months ago
Not sure how this question will be presented now that Azure security Center is Microsoft Defender for Cloud.
Anyone seen this question with new Microsoft Defender for Cloud? Thx
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct A + C
upvoted 1 times

tatendazw 1 year, 6 months ago
C. Create a logic app that you will be triggered in workflow automation
A. Microsoft Defender for Cloud > Workflow automation > Add workflow automation, on the Action choose the Logic app you have created

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run
upvoted 2 times

stromnessian 2 years, 11 months ago

Selected Answer: AC

Given answer looks good to me.

upvoted 3 times

pedromonteirozikado 2 years, 11 months ago

Selected Answer: AC

Correct

upvoted 4 times

macco455 2 years, 11 months ago

Selected Answer: AC

yeppers

upvoted 4 times

Eltooth 3 years, 3 months ago

Correct A and C

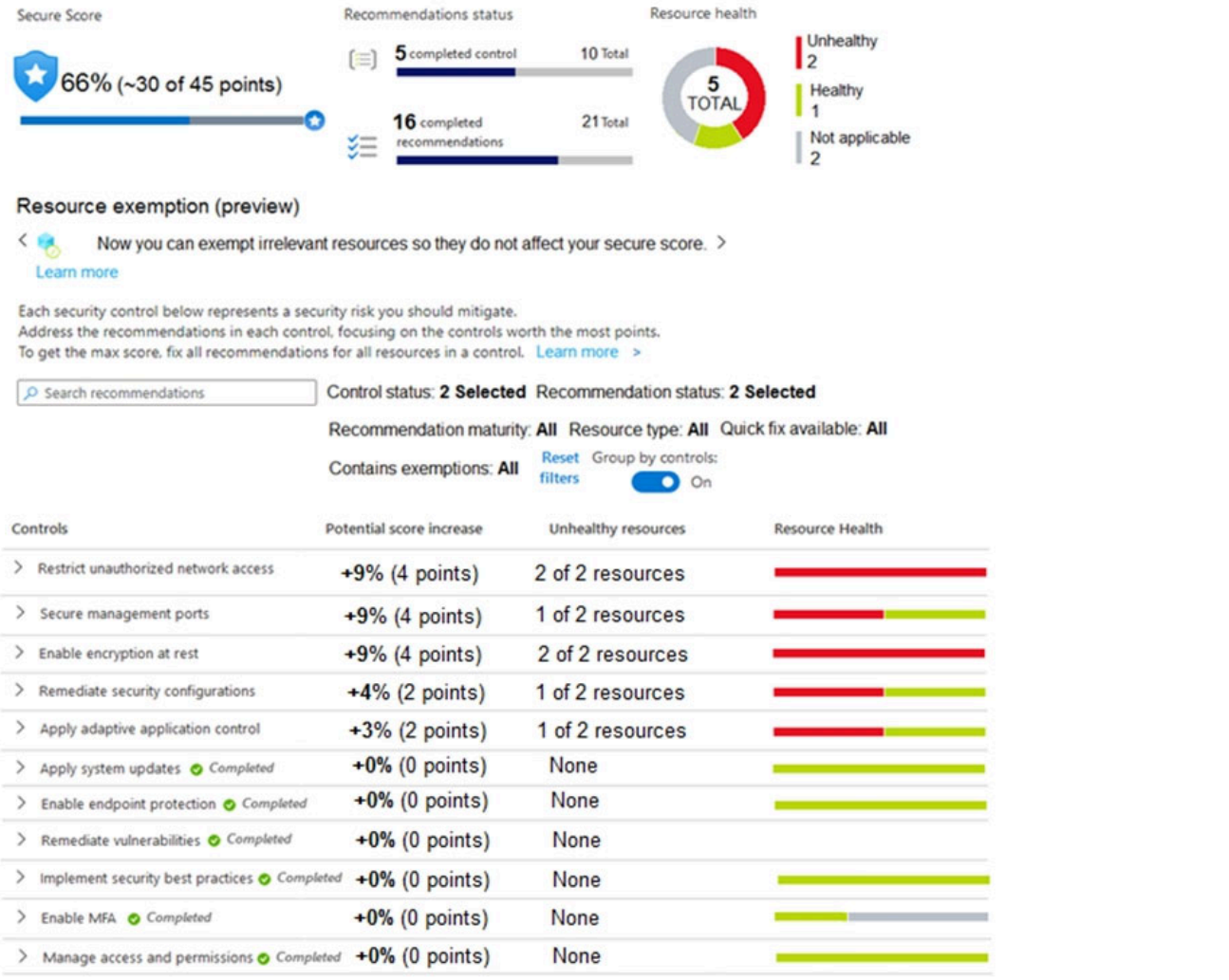
upvoted 3 times

Question #17 *Topic 2*

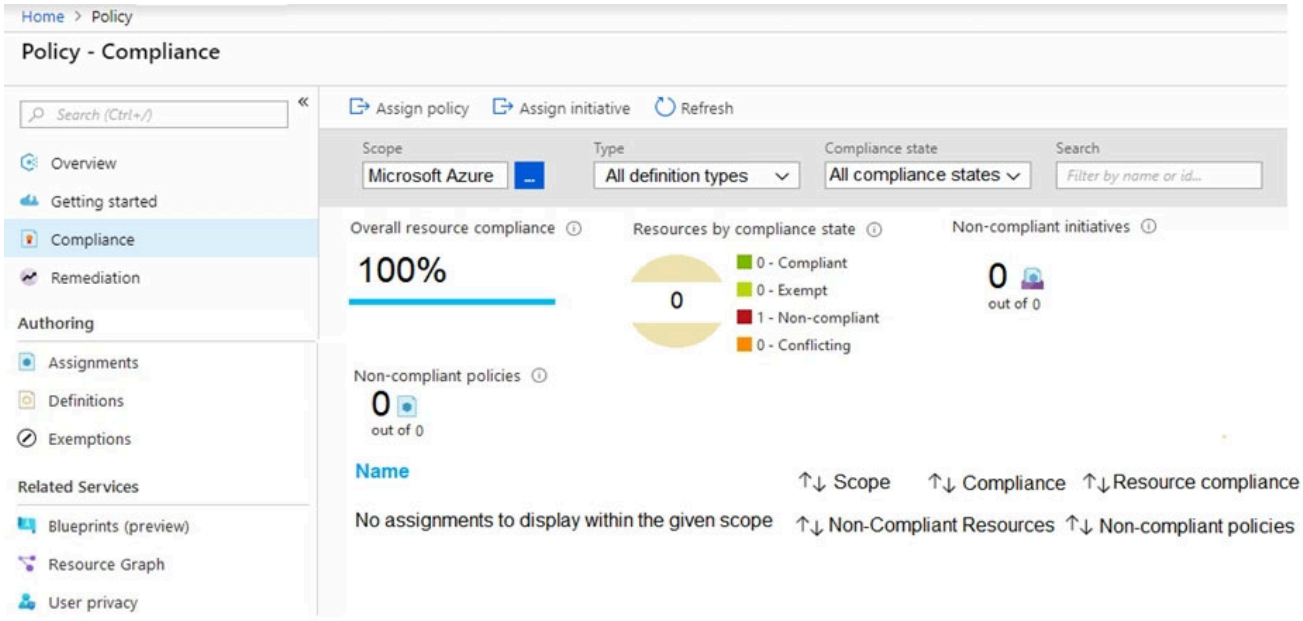
HOTSPOT -

You manage the security posture of an Azure subscription that contains two virtual machines name vm1 and vm2.

The secure score in Azure Security Center is shown in the Security Center exhibit. (Click the Security Center tab.)



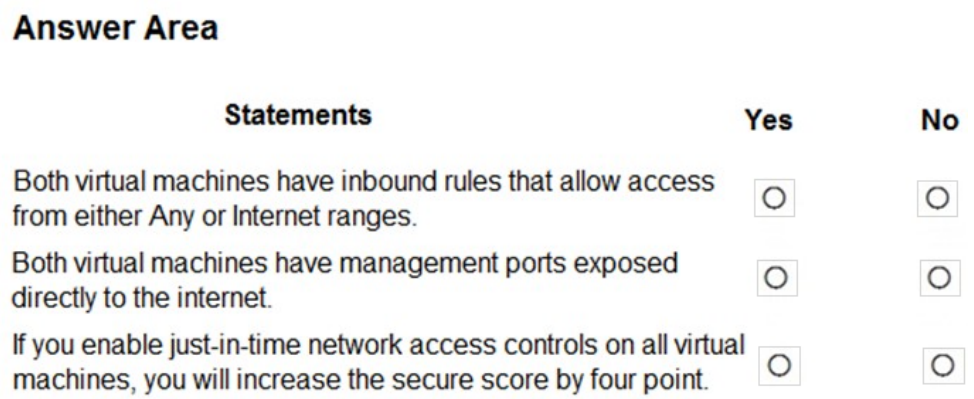
Azure Policy assignments are configured as shown in the Policies exhibit. (Click the Policies tab.)



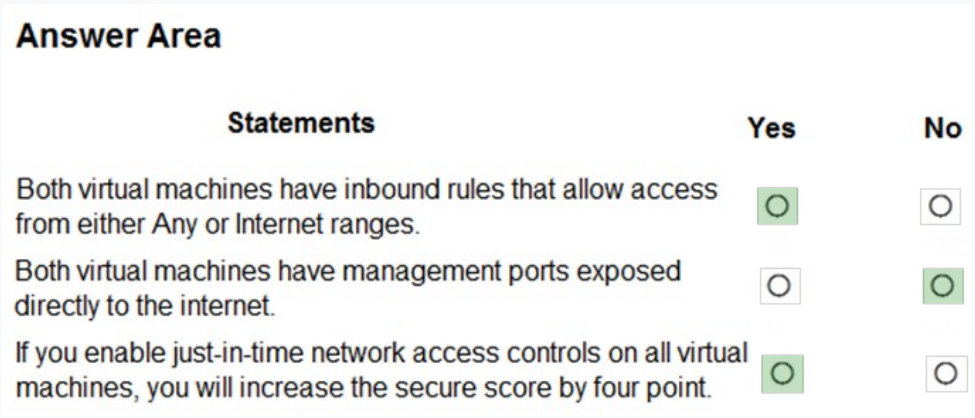
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833

https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770

Ken88 Highly Voted 2 years, 3 months ago

YNY is correct

Q3: JIT is about port control. Fix management port = +4 points

https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview

upvoted 41 times

MadLad84 1 year, 10 months ago

Thanks for the clear explanation

upvoted 3 times

KaiserdomTW Highly Voted 3 years, 2 months ago

Given answers are correct!

upvoted 15 times

chepeerick Most Recent 8 months, 2 weeks ago

YNY correct

upvoted 3 times

Avishdeep 1 year, 8 months ago

Correct - Yes, No, Yes.

upvoted 4 times

subhuman 2 years, 3 months ago

Easy one.

Answer is correct !

upvoted 4 times

Eltooth 2 years, 9 months ago

Correct - Yes, No, Yes.

upvoted 4 times

rk4ai 2 years, 10 months ago

Yes No Yes is correct
upvoted 3 times

Task 3 years, 1 month ago
Correct answer
upvoted 3 times

Beitran 3 years, 1 month ago
Shouldn't it be 8, since you're fixing the "management port" issue as well?
upvoted 1 times

Ramye 4 months, 2 weeks ago
No because one of the VMs is already secured and there is 4 points can be achieved by remediating the other one, so in total 4 points after the remediation and both are secured.
upvoted 1 times

Beitran 3 years, 1 month ago
Nvm, JIT remediation only applies to "Security Control: Secure Management Ports", not to "Security Control: Restrict Unauthorized Network Access", which indicates, for example, that the VM doesn't have an NSG: https://techcommunity.microsoft.com/t5/azure-security-center/security-control-restrict-unauthorized-network-access/ba-p/1593833
https://techcommunity.microsoft.com/t5/azure-security-center/security-control-secure-management-ports/ba-p/1505770
upvoted 6 times

malabar933 3 years, 1 month ago
In my opinion, given answers are correct!
upvoted 2 times

Question #18 *Topic 2*

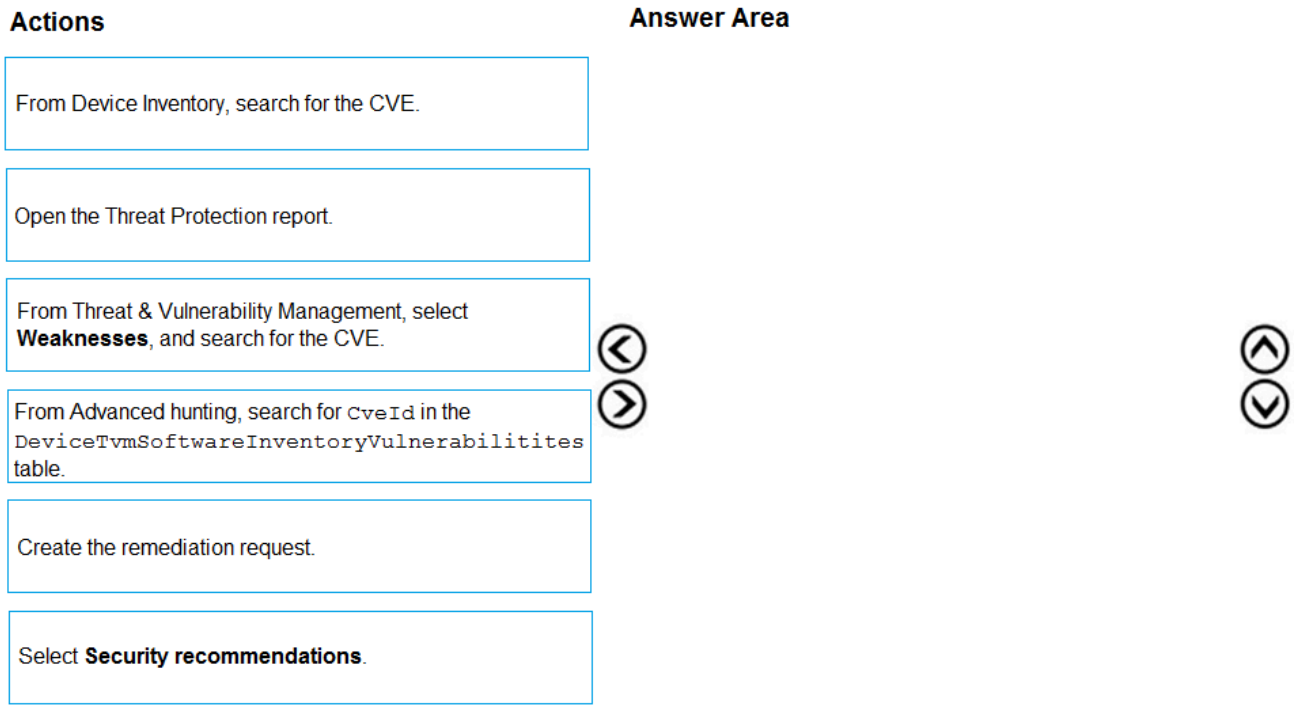
DRAG DROP -

You are informed of a new common vulnerabilities and exposures (CVE) vulnerability that affects your environment.

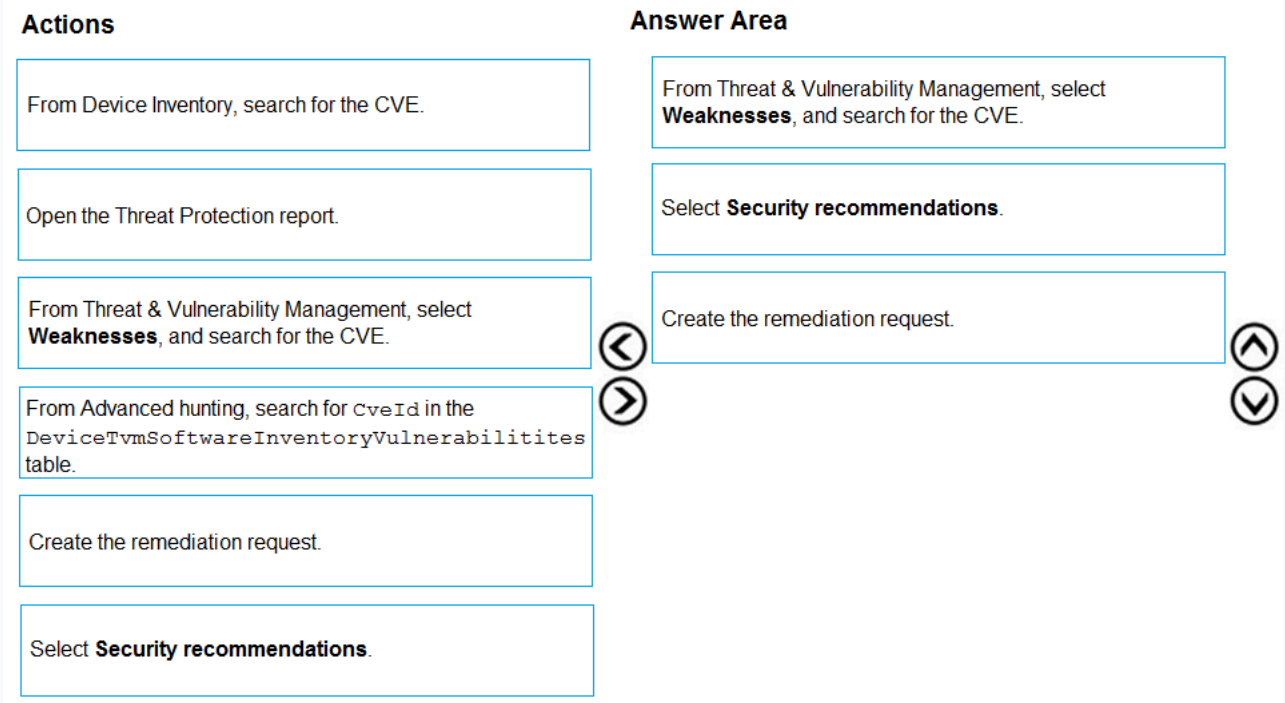
You need to use Microsoft Defender Security Center to request remediation from the team responsible for the affected systems if there is a documented active exploit available.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-defender-atp-remediate-apps-using-mem/ba-p/1599271

Eltooth Highly Voted 3 years, 3 months ago

Correct answer is as shown.

Open Security.microsoft.com --> Enpoints --> Vulnerabilty Management --> Weakness

Search/select CVE and click "Go to related security recommendations"
Click on Security recommendation task i.e. "update putty to version x.x.x"
Click on Request Remediation.

Tested on live tenant 19/09
upvoted 36 times

TheMCT Highly Voted 2 years, 11 months ago
Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud. We've also renamed Azure Defender plans to Microsoft Defender plans. The answers in this are based on Azure Security Center.

Correct answer is as shown.
Open Security.microsoft.com --> Enpoints --> Vulnerabilty Management --> Weakness
Search/select CVE and click "Go to related security recommendations"
Click on Security recommendation task i.e. "update putty to version x.x.x"
Click on Request Remediation.
upvoted 10 times

Ramye 11 months ago
The above steps are from Microsft (365) Defender. Note the URL still is Security.microsoft.com. This is no Azure Defender for Cloud, which is a separate solution for Azure specific.
upvoted 1 times

kazaki Most Recent 11 months ago
Don't waste time on questions like that outdated also
upvoted 2 times

Ramye 10 months, 2 weeks ago
Following the old and updated names sure is confusing…
But the fact is some old names still exists, e.g. Azure Security Center in Azure , though Microsoft said it is now called Microsoft Defender for Cloud.
Maybe this will go away in time…
upvoted 1 times

yafeci5971 11 months ago
Get up-to-date https://www.pinterest.com/pin/937522847419269991/
upvoted 1 times

inkedia3 6 months ago
not entirely true. Went through their questions few are up-to-date
upvoted 1 times

chepeerick 1 year, 2 months ago
this is out of date
upvoted 2 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 4 times

imhere4you 1 year, 6 months ago
On exam - 19 June 2023
upvoted 4 times

Haha0010 1 year, 11 months ago
In exam today (16 jan 2023)
upvoted 6 times

Ramye 11 months ago
Wow - this is outdated. I wonder how the question was presented.
upvoted 1 times

albd 2 years ago
In Exam today (23 dec 2022)
upvoted 6 times

Kanoniermalri 2 years, 3 months ago

Is this question still valid?

upvoted 1 times

trevax 2 years, 4 months ago

deprecated

upvoted 2 times

AK4U_111 1 year, 6 months ago

not true

upvoted 3 times

Task 3 years, 7 months ago

Correct

upvoted 3 times

Question #19 *Topic 2*

You use Azure Security Center.
You receive a security alert in Security Center.
You need to view recommendations to resolve the alert in Security Center.
What should you do?

A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section.

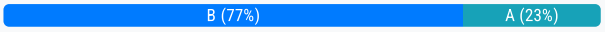
B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.

C. From Regulatory compliance, download the report.

D. From Recommendations, download the CSV report.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-managing-and-responding-alerts

Community vote distribution



NickHSO Highly Voted 3 years ago
it is B. With the 'Mitigate the threat' action you receive recommendations to mitigate this threat. The 'Prevent future attacks' action provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks.
upvoted 21 times

Eltooth Highly Voted 3 years, 3 months ago
Correct answer - B
upvoted 8 times

Nikki0222 Most Recent 2 months, 1 week ago
B correct
upvoted 1 times

talosDevbot 3 months, 1 week ago
Selected Answer: B
The question is asking for how to resolve the alert. In other words, to respond to an offending security event.

Mitigate the threat section involves alerts affecting the device.
Prevent future attack deals with reducing attack surface and vulnerability remediation recommendations.

Remediating a vulnerability or hardening a devices does not resolve an alert.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts
upvoted 1 times

Studytime2023 4 months, 3 weeks ago
Both A and B work (sort of). but the answer is definitely B.
When you follow the precise steps of A.
You expand "Prevent future attacks" and see:
"Solving security recommendations can prevent future attacks by reducing attack surface."

In other words, please refer to "Mitigate".

If you follow the steps of B.
You expand "Mitigate the threat" and see:
The specific steps to correct the specific issue. It will also provide a URL to documentation (if applicable) and it will mention if there are any other alerts on the affected resource.

Tested on my MSP's tenant. You can even generate sample alerts to do this if you don't have any.

upvoted 1 times

xRiot007 4 weeks, 1 day ago

You need to solve the (current) alert. This means that first, you do step B. Then, if you want to protect your system from future threats, you do step A, which is not required in this specific question.

upvoted 1 times

Avaris 6 months, 2 weeks ago

Selected Answer: A

Option A aligns with Azure Security Center's recommended approach to handling security alerts. By selecting the alert, taking action, and expanding the "Prevent future attacks" section, you will access detailed guidance on how to mitigate the identified threat and strengthen your security posture to prevent similar incidents. This is consistent with how Azure Security Center organizes its guidance and recommendations.

upvoted 1 times

ggGG1357 1 year ago

Selected Answer: B

B is correct. Because it is dealing with a current issue. The question is dealing with a present security alert. So be will be suitable.
A would be an option for future attacks.

upvoted 2 times

ggGG1357 1 year ago

B is correct. Because it is dealing with a current issue. The question is dealing with a present security alert. So be will be suitable.
A would be an option for future attacks.

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct A

upvoted 2 times

Gurulee 1 year, 2 months ago

Selected Answer: A

They question is asking for “view recommendations”, therefore the best answer is A.
“Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks”

upvoted 1 times

Gurulee 1 year, 2 months ago

Now I’m leaning toward B 😳

upvoted 1 times

Gurulee 1 year ago

Mitigate the threat provides steps to remediate said threat. Whereas Prevent future attacks offers security recommendations to minimize attack surface on the host.

upvoted 1 times

liveup2it 7 months, 1 week ago

Before you can click Take Action, you first have to select the alert. Answer B skips this part, so cannot be correct. Leaves us with Answer A.

upvoted 1 times

sand5234 1 year, 3 months ago

Correct Answer - A
Tested

upvoted 1 times

Anil0512 1 year, 3 months ago

it'a A

upvoted 2 times

Ramye 10 months, 1 week ago

No. It's B because it asked to resolve the alert that you have already received.
A is for the future.

upvoted 1 times

mali1969 1 year, 4 months ago

Selected Answer: A

Correct answer is A. From Security alerts, select the alert, select Take Action, and then expand the Prevent future attacks section. This will show you the security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks.

To view the recommendations, you can follow these steps:

From Defender for Cloud's security alerts page, select the alert you want to resolve.
Select Take Action at the top of the alert details page.
Expand the Prevent future attacks section and review the recommendations.
upvoted 2 times

XLR8T2 1 year, 5 months ago
Hola a todos, para esta pregunta la respuesta correcta es la A, acabo de validarlo, tienes que seleccionar la alerta para que luego puedas seleccionar Take Action.

Microsoft Defender for Cloud -> Security Alerts -> Select Alert -> Select Take Action ...
upvoted 1 times

tatendazw 1 year, 6 months ago
A is the answer, only Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks
B is incorrect because Mitigate the threat - provides manual remediation steps for this security alert
https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts
upvoted 1 times

xRiot007 4 weeks, 1 day ago
B is correct because that's exactly what you have to do first: solve the alert issue. it is irrelevant if you do it manually.
upvoted 1 times

Lone__Wolf 1 year, 10 months ago
Selected Answer: B
The correct answer is B. From Security alerts, select Take Action, and then expand the Mitigate the threat section.

To view recommendations to resolve a security alert in Azure Security Center, you should follow these steps:

Go to the Security alerts page in Security Center.
Select the specific security alert that you want to view recommendations for.
Select the Take Action button.
Expand the Mitigate the threat section to view the recommended steps for resolving the alert.
These recommendations provide detailed information and steps for addressing the security issue that is raised by the alert, and help you to prevent future attacks on your resources. By following the recommendations, you can improve the security posture of your resources in Azure.
upvoted 4 times

amsioso 2 years, 3 months ago
B
Mitigate the threat - provides manual remediation steps (recommendations to resolve) for this security alert
But they forgot "select the alert"
upvoted 1 times

Question #20 *Topic 2*

You have a suppression rule in Azure Security Center for 10 virtual machines that are used for testing. The virtual machines run Windows Server.
You are troubleshooting an issue on the virtual machines.
In Security Center, you need to view the alerts generated by the virtual machines during the last five days.
What should you do?

A. Change the rule expiration date of the suppression rule.

B. Change the state of the suppression rule to Disabled.

C. Modify the filter for the Security alerts page.

D. View the Windows event logs on the virtual machines.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules

Community vote distribution
C (78%) B (22%)

PJR Highly Voted 3 years, 2 months ago
I think this is incorrect and the answer should be C - Modify the filter for the Security alerts page.

Answer B would prevent future alerts from being supressed but the question is asking to view alerts created in the last 5 days - these would have been dismissed by the supression rule and to view them you need to alter the filter to display dismissed alerts.

Ref: https://docs.microsoft.com/en-us/azure/security-center/alerts-suppression-rules#what-are-suppression-rules
upvoted 58 times

Lone__Wolf 1 year, 10 months ago
Exact Thoughts! The answer is C.
upvoted 1 times

Ferrix Highly Voted 3 years, 2 months ago
Corret answer is C
upvoted 15 times

xRiot007 Most Recent 4 weeks, 1 day ago
Selected Answer: C
A - No, you don't need to change any expiration of anything
B - No, you don't need to disable anything
C - Yes, you need to change the timeframe inside the rule
D - off-topic
upvoted 2 times

Nikki0222 2 months, 1 week ago
C correct
upvoted 1 times

dcceda3 3 months, 1 week ago
C. Modify the filter for the Security alerts page.

Explanation:
Suppression rules do not delete alerts; they only hide them from view. By modifying the filter on the Security alerts page, you can view suppressed alerts without disabling or modifying the suppression rule. Disabling or changing the rule would not retroactively reveal previously suppressed alerts, but changing the filter will allow you to view them.
upvoted 2 times

Baz10 10 months, 1 week ago

Selected Answer: C

I said C

GPT says C

Comments are saying C

Who decided it was B?

upvoted 4 times

blueking 1 year ago

Alert suppression rule will not create Incident and Email notification, it will still have that alert in alert page in security center.
to view the alerts for last five-day for those systems you need to apply filter in security page so the Corret answer is C.

upvoted 1 times

blueking 1 year ago

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-suppression-rules?view=o365-worldwide
View details of a suppression rule
In the navigation pane, select Settings > Endpoints > Rules > Alert suppression. The list of suppression rules that users in your organization have created is displayed.

Click on a rule name. Details of the rule is displayed. You'll see the rule details such as status, scope, action, number of matching alerts, created by, and date when the rule was created. You can also view associated alerts and the rule conditions.

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct C modify the filter

upvoted 1 times

Monitor 1 year, 3 months ago

"The Microsoft Defender plans detect threats in your environment and generate security alerts. When a single alert isn't interesting or relevant, you can manually dismiss it. Suppression rules let you automatically dismiss similar alerts in the future." Dismissed alerts aren't shown by default. Answer is C; you have to modify the filter.

upvoted 1 times

mali1969 1 year, 4 months ago

Selected Answer: B

correct answer is B.
Change the state of the suppression rule to Disabled. This will allow you to view the alerts generated by the virtual machines during the last five days.

To change the state of the suppression rule, you can follow these steps:

From Defender for Cloud’s security alerts page, select Suppression rules at the top of the page.
The suppression rules page opens with all the rules for the selected subscriptions.
To edit a single rule, open the three dots (…) at the end of the rule and select Edit.
Change the state of the rule to Disabled and select Apply.

upvoted 1 times

mali1969 1 year, 3 months ago

the correct answer is C. Modify the filter for the Security alerts page.

The other options are not correct because:

A. Change the rule expiration date of the suppression rule: This option will not help you view the alerts generated by the suppressed resources, but only change the duration of the suppression rule
B. Change the state of the suppression rule to Disabled: This option will not help you view the alerts generated by the suppressed resources, but only disable the suppression rule and allow new alerts to be generated
D. View the Windows event logs on the virtual machines: This option will not help you view the alerts generated by Security Center, but only show you the Windows event logs on the virtual machines, which may not contain all the relevant information

upvoted 3 times

Oryx360 1 year, 4 months ago

Selected Answer: C

In Security Center, to view the alerts generated by the virtual machines during the last five days, you should modify the filter for the Security alerts page.

Option C is the correct answer:

C. Modify the filter for the Security alerts page.

By adjusting the filter settings on the Security alerts page, you can specify the time range and the specific criteria you want to apply to view the alerts generated by the virtual machines within the last five days. This will help you focus on the relevant alerts related to the troubleshooting issue you are investigating.

upvoted 1 times

tduarte14 1 year, 8 months ago

Selected Answer: C

C is correct. You need to change the filter as it's only showing "Active, In Progress"

upvoted 1 times

exmITQS 1 year, 10 months ago

Selected Answer: C

Azure Security Center, you should modify the filter for the Security alerts page. The suppression rule is designed to prevent alerts from being generated, so it should not be affecting the ability to view alerts. To modify the filter for the Security alerts

upvoted 2 times

Valunchai 1 year, 10 months ago

Selected Answer: B

First, Disable suppressed rule and filter or scroll to see last 5 days alert.

upvoted 2 times

Wutan 1 year, 11 months ago

Selected Answer: C

C is the correct one in my opinion.

upvoted 1 times

Haha0010 1 year, 11 months ago

Selected Answer: C

In exam today (16 jan 2023)

upvoted 6 times

Question #21 *Topic 2*

HOTSPOT -

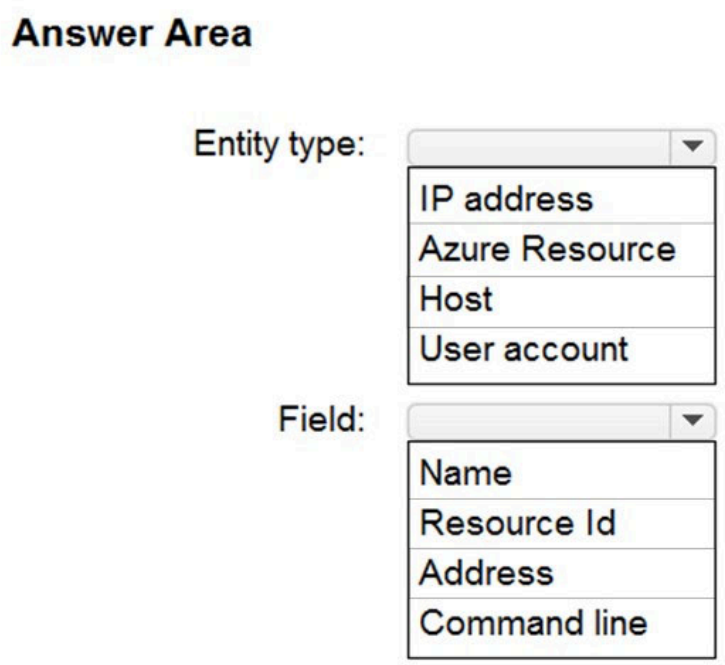
You have an Azure Storage account that will be accessed by multiple Azure Function apps during the development of an application.

You need to hide Azure Defender alerts for the storage account.

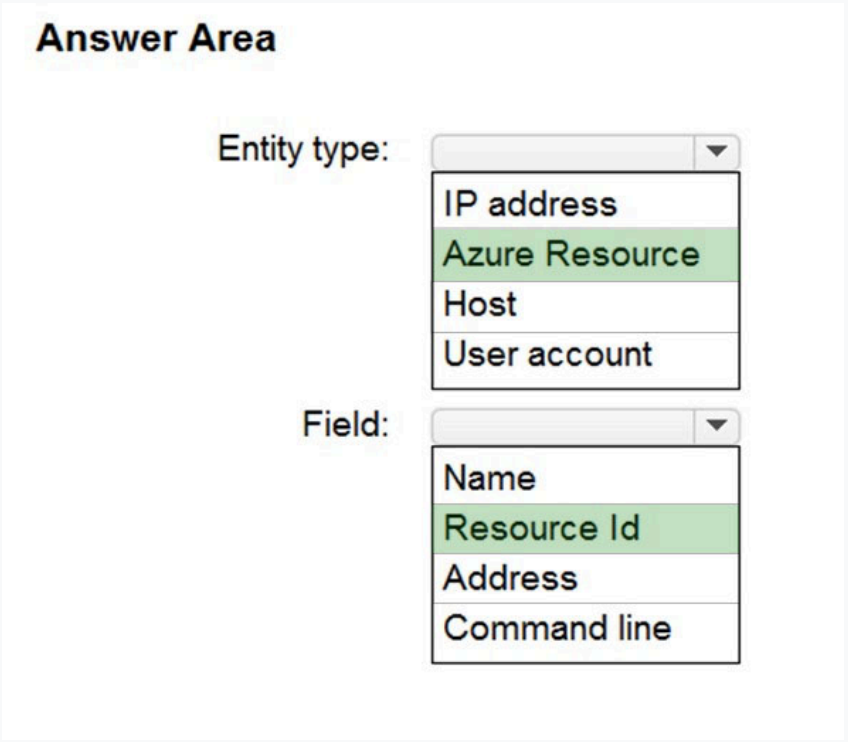
Which entity type and field should you use in a suppression rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

Eltooth Highly Voted 3 years, 3 months ago

Entity Type = Azure Resource (Azure Storage is a Resource)

Field = Resource ID (All Azure resources have an ID)

Correct.

upvoted 31 times

Nikki0222 2 months, 1 week ago

Correct

upvoted 1 times

chepeerick Most Recent 1 year, 2 months ago

correct

upvoted 2 times

Lone__Wolf 1 year, 10 months ago

Correct! ✌

upvoted 2 times

Snaileyes 2 years, 1 month ago

...but if it's accessed by multiple Azure Function Apps -- each would have a different Resource ID, right? (So...you would need to know the resource ID's for each Function App that will be accessing it...)

upvoted 1 times

xRiot007 4 weeks, 1 day ago

The suppression is set for the storage itself, not the resources that want to access it.

upvoted 1 times

herta 1 year, 12 months ago

no you have only one storage

upvoted 4 times

somsom 2 years, 4 months ago

Very correct .

upvoted 3 times

Question #22 *Topic 2*

You create an Azure subscription.
You enable Azure Defender for the subscription.
You need to use Azure Defender to protect on-premises computers.
What should you do on the on-premises computers?

A. Install the Log Analytics agent.

B. Install the Dependency agent.

C. Configure the Hybrid Runbook Worker role.

D. Install the Connected Machine agent.

Suggested Answer: *A*
Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.
Data is collected using:
➪ The Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user.
➪ Security extensions, such as the Azure Policy Add-on for Kubernetes, which can also provide data to Security Center regarding specialized resource types.
Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection

Community vote distribution
A (74%) D (26%)

Eltooth Highly Voted 3 years, 3 months ago
Correct - A
upvoted 14 times

Haha0010 Highly Voted 1 year, 11 months ago
Selected Answer: A
In exam today (16 jan 2023)
upvoted 13 times

xRiot007 Most Recent 4 weeks, 1 day ago
Selected Answer: A
You need to do monitoring and then have Defender react, so A - Log Analytics (or AMA, today) is enough. You don't have to do centralized management in this question.
upvoted 1 times

VeiN 2 months, 2 weeks ago
Selected Answer: D
You need to install Azure Arc (azure connected Machine).
In short this will create an azure resource representation of onpremise machine that can be partialy managed like azure resources. For instance you can run DfC Regulatory compliance.
upvoted 1 times

ZECO85 4 months ago
Selected Answer: A
The Connected Machine agent (Option D) is used to connect and manage machines that are hosted outside of Azure, such as on-premises or other cloud providers, through Azure Arc12. While it helps in managing these machines, it does not specifically enable the security features provided by Azure Defender.

For Azure Defender to analyze and provide security recommendations, the Log Analytics agent is required. This agent collects data from your on-premises machines and sends it to Azure Monitor, which Azure Defender uses for its security analysis.
So the answer is A

upvoted 3 times

e072f83 6 months, 2 weeks ago

in order to make the Log analytics agent work, you first need the arc agent on an on-prem server (formerly connected machine agent) so D is correct. https://learn.microsoft.com/en-us/azure/defender-for-cloud/monitoring-components

upvoted 2 times

DChilds 8 months, 1 week ago

Selected Answer: A

Azure Defender (now named Defender for Cloud) relies on Log Analytics Agent to collect logs and enable protection of the workstations.

upvoted 2 times

DChilds 8 months, 3 weeks ago

Selected Answer: D

Question may be outdated but installing Azure Arc is the first thing to do with an on-prem server. This will ensure you can deploy Azure services like Defender and manage it from the Defender portal. Installing Log Analytics will be to view the Windows logs in a portal like Sentinel so as to be build alerts and rules from those logs. Azure Arc (previously Connected Machine agent) has to be loaded first.

upvoted 3 times

DChilds 8 months, 1 week ago

I change my mind, Azure Defender relies on the Log Analytic Agent to collect logs for monitoring, threat detection etc. Answer is A.

upvoted 2 times

Ramye 10 months, 2 weeks ago

This is an outdated question but don't understand why most saying A as they answer?

It makes sense D. Install the Connected Machine agent.
Thoughts???

upvoted 1 times

Ramye 10 months, 2 weeks ago

Never mind
@trashbox explained below ...thx

upvoted 2 times

kazaki 10 months, 3 weeks ago

Selected Answer: D

Outdated question now using arc only for defender for cloud

upvoted 1 times

kazaki 11 months ago

this is outdated

upvoted 1 times

kabooze 1 year, 2 months ago

Selected Answer: D

this should be D. For defender to work you need the azure arc agent (or azure connected .... agent) to make it work.
Although, there IS a possibility to deploy it directly without using Arc, but that's not the point of this question.

upvoted 2 times

slurppp 1 year, 2 months ago

Think many of these questions are now out of date. Log Analytics Agent is now legacy and is replaced as "Azure Monitor Agent (AMA)" - Examptopics needs to update this whole course I think. Too many things have changed names now so I would expect the exam questions to be different or updated.

upvoted 5 times

Ramye 11 months ago

Exactly. And Microsoft announced the below

"The English language version of this exam will be updated on March 4, 2024. Review the study guide linked in the "Tip" box for details on upcoming changes. If a localized version of this exam is available, it will be updated approximately eight weeks after this date. While Microsoft makes every effort to update localized versions as noted, there may be times when the localized versions of this exam are not updated on this schedule"
Source: https://learn.microsoft.com/en-us/credentials/certifications/exams/sc-200/

upvoted 1 times

trashbox 1 year, 3 months ago

Selected Answer: A

The answer is correct. Log Analytics Agent.

By the way, if you're planning to configure VMs from now on, I believe it would be better to use the Azure Monitor Agent (AMA) instead of the Log Analytics Agent.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/monitoring-components
upvoted 1 times

trashbox 1 year, 3 months ago

I changed my mind. D then A is more optimal. So, the answer should be "D."
upvoted 3 times

mali1969 1 year, 4 months ago

Selected Answer: D

he correct answer is D. Install the Connected Machine agent.

To use Azure Defender to protect on-premises computers, you need to connect them to Azure by using Azure Arc-enabled servers. This requires installing the Connected Machine agent on the on-premises computers, which registers them as Azure resources and enables Azure management capabilities.

Installing the Log Analytics agent, the Dependency agent, or configuring the hybrid runbook worker role are not sufficient to connect the on-premises computers to Azure and enable Azure Defender protection. These agents and roles are used for different purposes, such as collecting logs and metrics, monitoring dependencies, or running automation runbooks
upvoted 2 times

mali1969 1 year, 3 months ago

I need to correct my answer A
A. Install the Log Analytics agent. This is the correct answer. The Log Analytics agent is a service that collects telemetry from your on-premises computers and sends it to Azure Monitor3. By installing the Log Analytics agent, you can enable Azure Defender to monitor and analyze the data from your on-premises computers and provide security recommendations and alerts4. You can install the Log Analytics agent manually or by using automation tools such as PowerShell or Azure Policy.
upvoted 2 times

xping85 1 year, 4 months ago

I thin B is the correct Answer.
it is not clear if azure Arc has already been installed.
Answer B includes the Log Analytic and Azure Arc.
upvoted 1 times

donathon 1 year, 5 months ago

Selected Answer: A

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent
upvoted 1 times

donathon 1 year, 3 months ago

Like to add that ARC agent is a pre-requisite and not the main requirement. So if the question ask you what to install "first", then it would make sense to choose ARC.
upvoted 3 times

Question #23 *Topic 2*

A security administrator receives email alerts from Azure Defender for activities such as potential malware uploaded to a storage account and potential successful brute force attacks.
The security administrator does NOT receive email alerts for activities such as antimalware action failed and suspicious network activity. The alerts appear in
Azure Security Center.
You need to ensure that the security administrator receives email alerts for all the activities.
What should you configure in the Security Center settings?

A. the severity level of email notifications

B. a cloud connector

C. the Azure Defender plans

D. the integration settings for Threat detection

Suggested Answer: *A*
Reference:
https://techcommunity.microsoft.com/t5/microsoft-365-defender/get-email-notifications-on-new-incidents-from-microsoft-365/ba-p/2012518

Community vote distribution
A (100%)

passA900 Highly Voted 1 year, 7 months ago

Selected Answer: A

Email notifications are free; for security alerts, enable the enhanced security plans
https://learn.microsoft.com/en-us/azure/defender-for-cloud/configure-email-notifications
upvoted 8 times

mali1969 Highly Voted 10 months, 1 week ago

Selected Answer: A

The correct answer is A. the severity level of email notifications.

To ensure that the security administrator receives email alerts for all the activities, you need to configure the severity level of email notifications in the Security Center settings. By default, email notifications are only sent for alerts with high severity. You can change this setting to include alerts with medium or low severity as well. This way, you can receive email alerts for activities such as antimalware action failed and suspicious network activity, which have medium or low severity
upvoted 5 times

Ramye Most Recent 4 months, 4 weeks ago

Selected Answer: A

A. the severity level of email notifications.
To set it: Microsoft Defender for Cloud --> Environment settings --> Azure subscription --> Email notifications --> Notifications types
upvoted 1 times

chepeerick 8 months, 2 weeks ago

Correct A
upvoted 1 times

mali1969 10 months, 2 weeks ago

Selected Answer: A

A. the severity level of email notifications. This will allow you to specify the minimum severity level of alerts that will trigger email notifications.

To configure the severity level of email notifications, you can follow these steps:

Go to Security Center in the Azure portal.
Click on Pricing and Settings.
Click on the appropriate Management Group, Subscription, or Workspace.
Click on Email notifications.

Under Notification types, check the check box next to Notify about alerts with the following severity (or higher) and select the desired level from the drop-down menu.
Click Save.
upvoted 1 times

Lone_Wolf 1 year, 4 months ago

Selected Answer: A

Correct Answer -\^
upvoted 3 times

Tx4free 2 years, 3 months ago

Selected Answer: A

Best option
upvoted 3 times

AlaReAla 2 years, 9 months ago

Thought the answer is correct, but it should be alert level of "Incidents" not "email". Please refer the given link.
upvoted 1 times

Metasploit 1 year, 8 months ago

You are overthinking this Question :) . The severity level of email notifications [within the incident notifications rules needs to be adjusted]
upvoted 4 times

Eltooth 2 years, 9 months ago

Correct - A
upvoted 3 times

Question #24 *Topic 2*

DRAG DROP -

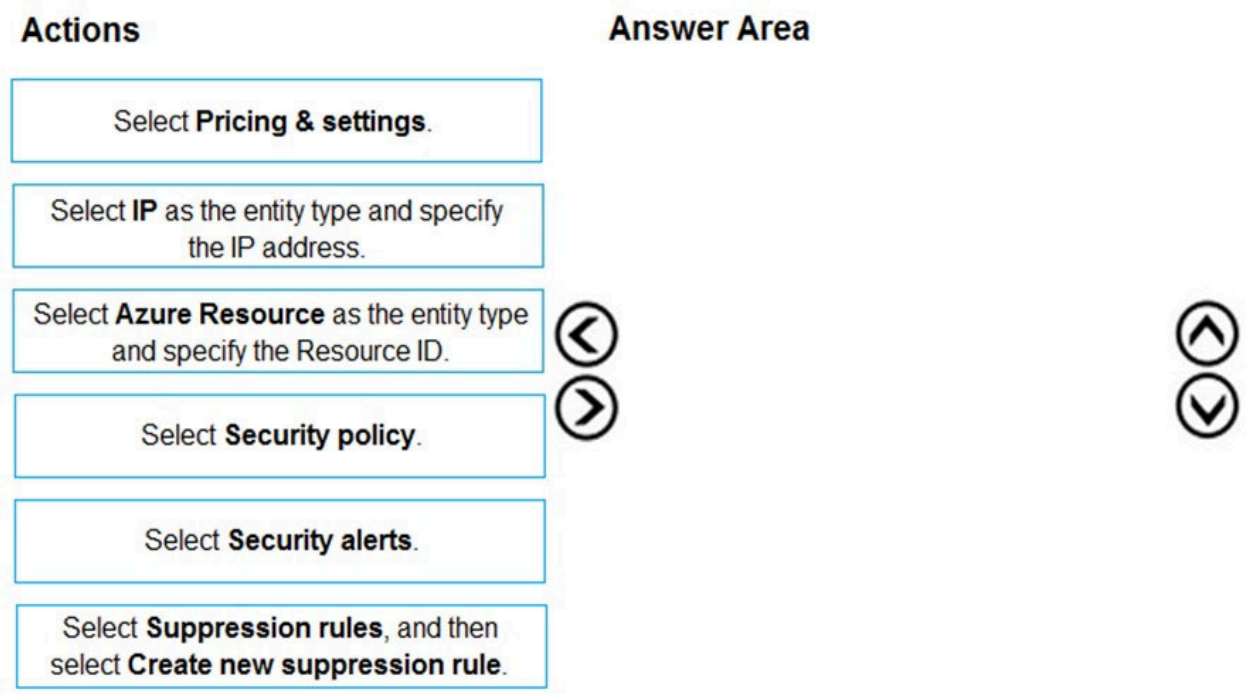
You have an Azure Functions app that generates thousands of alerts in Azure Security Center each day for normal activity.

You need to hide the alerts automatically in Security Center.

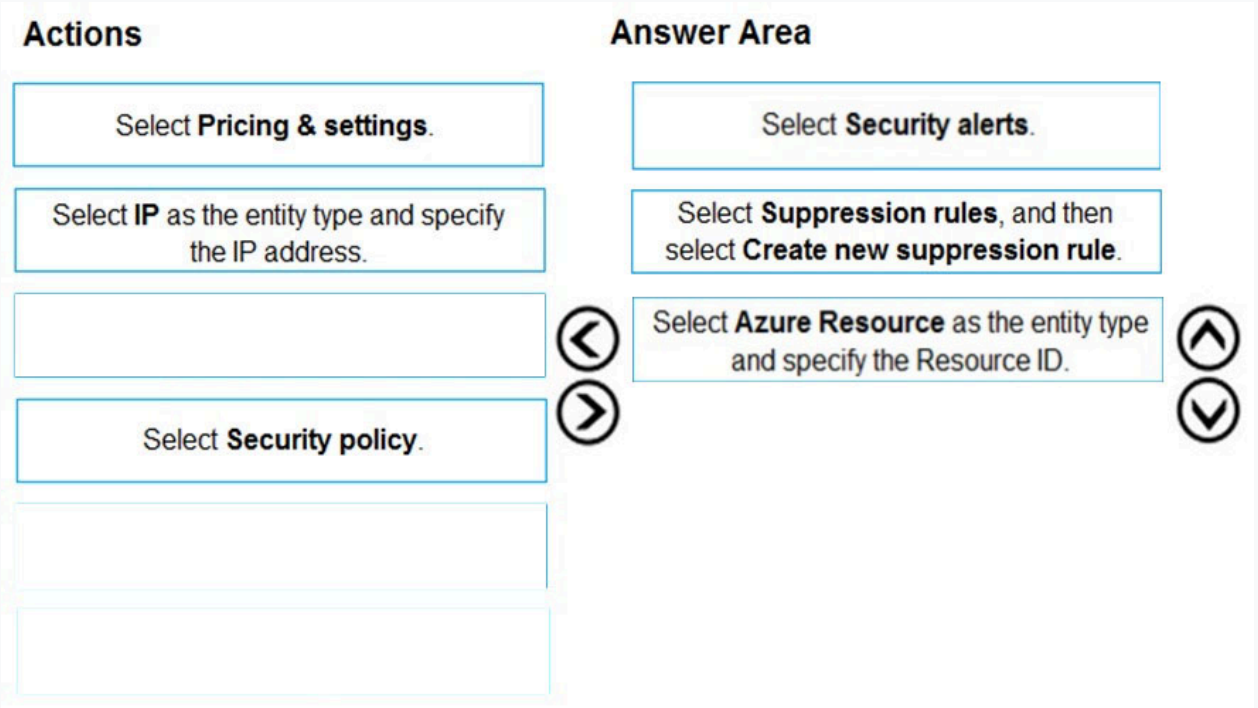
Which three actions should you perform in sequence in Security Center? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Select and Place:



Suggested Answer:



Reference:

https://techcommunity.microsoft.com/t5/azure-security-center/suppression-rules-for-azure-security-center-alerts-are-now/ba-p/1404920

Haha0010 Highly Voted 1 year, 11 months ago

In exam today (16 jan 2023)

upvoted 16 times

Tuitor01 4 weeks ago

Today it would be done via the alert in the 'security center' page, lick on the alert, take action; choose suppress similar alerts then create suppression rules: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules
upvoted 2 times

ACSC Highly Voted 2 years, 1 month ago
Answer is correct.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule
upvoted 11 times

Baz10 Most Recent 10 months, 1 week ago
Outdated, thats why I got it wrong (it'll help me sleep at night)
upvoted 3 times

Henk1982 3 months ago
hahahaaa luv it
upvoted 1 times

Ramye 11 months ago
Note: Azure Security Center is now Microsoft Defender for Cloud
upvoted 2 times

chepeerick 1 year, 2 months ago
Correct Ans
upvoted 1 times

trashbox 1 year, 3 months ago
The answers are correct.

"Select security alerts" -> "Suppression rule and create new suppression rule." In this case, "Entity type: Azure Resource" is optimal because of Azure Functions apps.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule
upvoted 2 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 2 times

amsioso 2 years, 3 months ago
Understand that "select security alerts" means "go to security alerts page".
"Select Suppression rules"= "select the suppression rules link at the top of the page"
https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules
upvoted 4 times

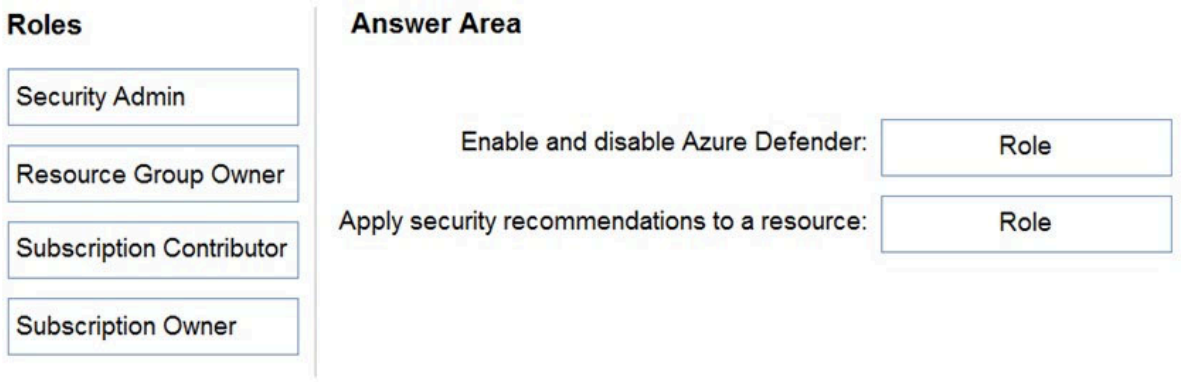
somsom 2 years, 4 months ago
the sequence is correct
upvoted 3 times

Lion007 2 years, 6 months ago
You can only select one security alert and create a supression rule for it. When selecting multiple security alerts and click 'Supression rules' then click 'Create new suppression rule', the drop down menu under Alerts (when selecting 'Custom') would allow you to select only one alert. That's why I find the answer wrong in terms of sequence of actions. Selecting the security alert (not alerts!) should be last.
upvoted 3 times

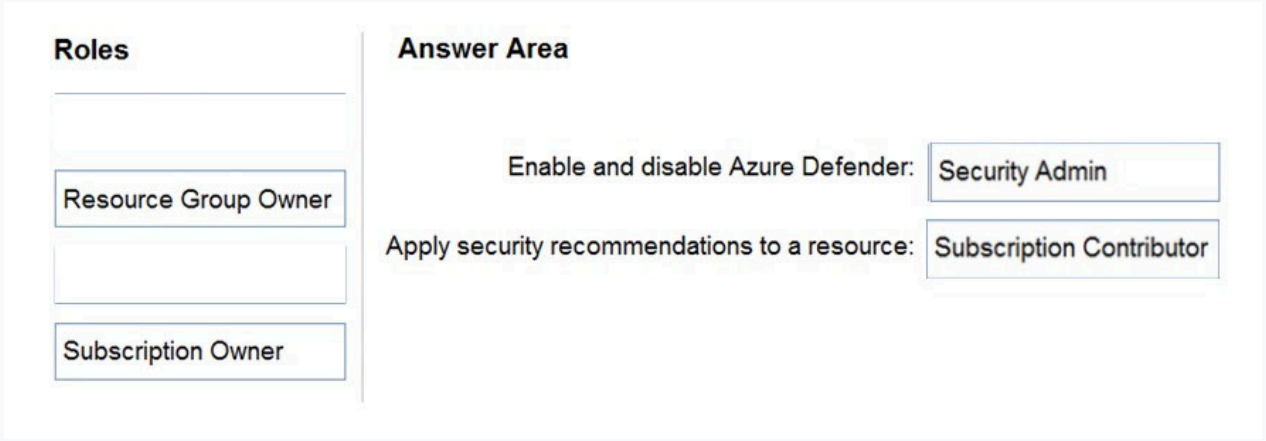
JoeP1 1 year, 5 months ago
I believe Select security alerts means to go to the alerts instead of selecting one or more specific alerts.
upvoted 1 times

Question #25 *Topic 2*

DRAG DROP -
You have an Azure subscription.
You need to delegate permissions to meet the following requirements:
✑ Enable and disable Azure Defender.
✑ Apply security recommendations to resource.
The solution must use the principle of least privilege.
Which Azure Security Center role should you use for each requirement? To answer, drag the appropriate roles to the correct requirements.
Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
Select and Place:



Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

PJR Highly Voted 3 years, 3 months ago
Answer is incorrect - the link provided in the answer - https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions shows the least priv roles would be

-Sec Admin
-Resource Group Owner (this has lower priv than subscription contributor and can still apply security recommendations)
upvoted 60 times

Ramye 10 months ago
Correct it should be Resource Group Owner for:
Apply security recommendations for a resource
(and use Fix)
upvoted 1 times

kakakayayaya 3 years ago

It is a tricky question. Resource Group Owner - will not provide access to Subscription, so you will not see any configuration in MS defender for cloud (ex.ASC).
Sub Contributor will allow to do all tasks.
upvoted 12 times

FrostForrest 2 years, 9 months ago
Look at the question. It states resources within a subscription. Without knowing the design of the subscription, only allocating a Resource Group Owner would be insufficient.
upvoted 3 times

prabhjot 2 years, 9 months ago
Avoid assigning broader roles at broader scopes . By limiting roles and scopes, you limit what resources are at risk if the security principal is ever compromised.
upvoted 2 times

prabhjot 2 years, 9 months ago
so Resource Group owner looks fine
upvoted 3 times

shachar_ash 2 years, 5 months ago
what if the resources span across multiple RGs?
upvoted 2 times

Ramkid Highly Voted 1 year, 11 months ago
Correct Answer
Box1 : Security Admin
Box2 : Resource Group Owner
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 21 times

Zak366 1 year, 10 months ago
Perfect link, following principle of least privilege
upvoted 1 times

Ramye 11 months ago
and a snippet from the article above:
" In Defender for Cloud, you only see information related to a resource when you're assigned one of these roles for the subscription or for the resource group the resource is in: Owner, Contributor, or Reader."
upvoted 1 times

Avaris Most Recent 6 months, 2 weeks ago
Enable and disable Azure Defender: Assign Subscription Contributor to manage subscription-level settings, including enabling and disabling Azure Defender.
Apply security recommendations to a resource: Assign Security Admin to view and apply security recommendations within the resource groups.
upvoted 1 times

LeandroFerraz 9 months, 3 weeks ago
CORRECT
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 1 times

Ramye 10 months, 1 week ago
Who has less permission between Sec Admin vs Contributor? Given the information here https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
the contributor has less permission, therefore, the 1st box should be Contributor.
And the 2nd box is also contributor.
upvoted 2 times

Ramye 10 months, 1 week ago
After delving further and considering it's a single resource, the answers should be for the:
1st box: Subscription Contributor
2nd box: Resource Group Owner
upvoted 6 times

estyj 11 months, 3 weeks ago

Security admin and Resource Group Owner since it just says a resource (Not resources) not spanning multiple RG. So Resource Group Owner for Principle of least privilege.
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct, Contribuitor / Owner Resource group level) then Contributor (Subscription level)
upvoted 1 times

IT_Nerd31 1 year, 2 months ago
The answer is
. Sec Admin -
. Resource Group Owner - "Apply Security recommendations to a resource" (Resource is the key word here.)
upvoted 3 times

mali1969 1 year, 4 months ago
To enable and disable Azure Defender, you need the Security Admin role1. This role allows you to update the security policy and enable or disable Azure Defender plans.

To apply security recommendations to a resource, you need the Subscription Contributor role. This role grants full access to manage all resources, including the ability to apply security recommendations for a resource
upvoted 2 times

donathon 1 year, 4 months ago
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
Answer is correct based on past contributors
upvoted 1 times

donathon 1 year, 3 months ago
Sorry I change to Security Admin and Resource Group Owner. A resource can only be within a single resource group so this should be enough.
upvoted 1 times

xping85 1 year, 4 months ago
The solution must use the principle of least privilege
Box1: Subscription Contributor
Box2: Resource Group Owner
reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 3 times

tirajvid 1 year, 6 months ago
What if a subscription has hundreds of resource groups belongs to many departments ? Subscription contributor access will provide access to all those additional RGs. ?
upvoted 1 times

Veracloud 1 year, 6 months ago
answer is correct, https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 1 times

tatendazw 1 year, 6 months ago
Sub Contributor
Resource Group owner
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 3 times

imsidrai 1 year, 9 months ago
Correct ans is Contributor Contributor , because contributor role at subscription level has both the capabilities
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 1 times

Emyr 1 year, 10 months ago
For me I think the correct answer should be :
- sub contributor
- resource owner

https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 5 times

Ahmed_Root 2 years ago

it is clearly mentioned in the following link that for disabling/enabling you can use "Security Admin" at least and for applying security recommendations at least you need "Ressource Group Contributor or Owner". here we have only owner not contributor.
https://docs.microsoft.com/en-us/azure/security-center/security-center-permissions

upvoted 3 times

Question #26 *Topic 2*

HOTSPOT -

You have an Azure subscription that uses Azure Defender.

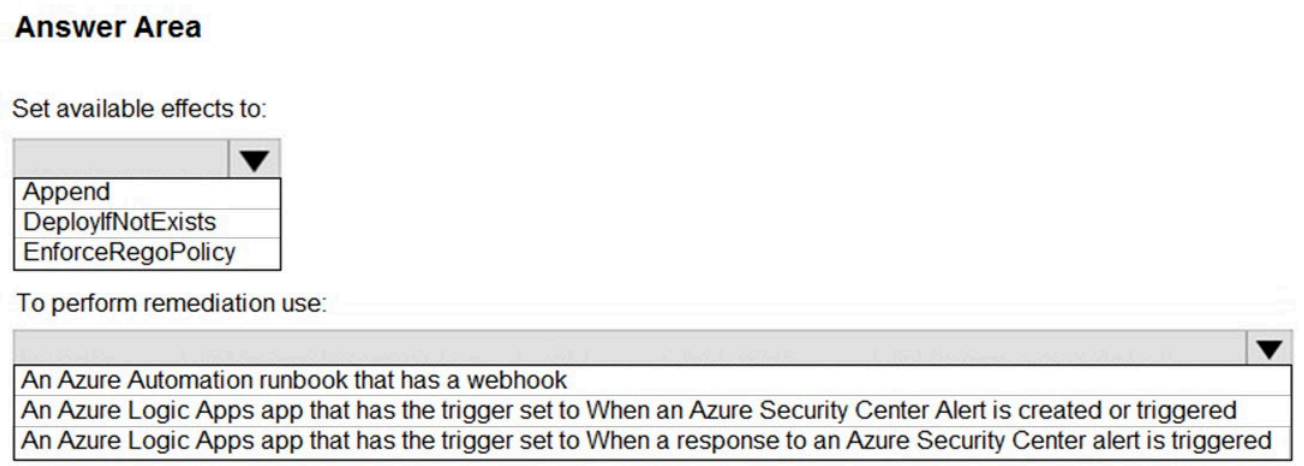
You plan to use Azure Security Center workflow automation to respond to Azure Defender threat alerts.

You need to create an Azure policy that will perform threat remediation automatically.

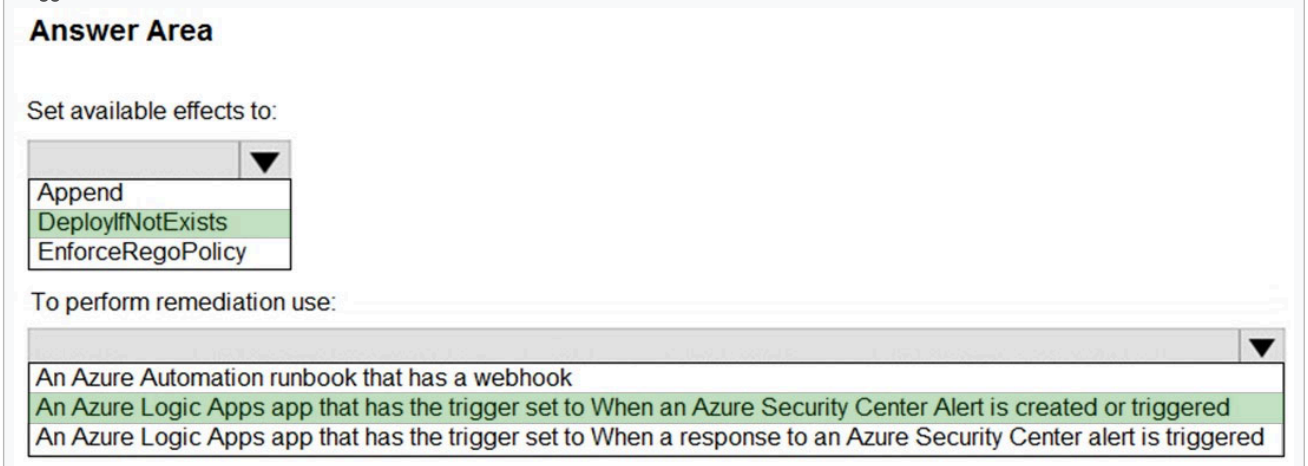
What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects https://docs.microsoft.com/en-us/azure/security-center/workflow-automation

Lion007 Highly Voted 1 year, 6 months ago

Correct answers. DeployIfNotExist explained here https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#deployifnotexists-properties

upvoted 8 times

Mthaher Highly Voted 1 year, 8 months ago

Yes Correct

Append is used to add additional fields to the requested resource during creation or update

The following effects are deprecated:

EnforceOPAConstraint

EnforceRegoPolicy

upvoted 6 times

chepeerick Most Recent 2 months, 1 week ago

Correct

upvoted 1 times

Fez786 8 months, 1 week ago

Given answer is correct

upvoted 2 times

scruzer 10 months, 3 weeks ago

Repeated question.

upvoted 1 times

masterofnetscaler 1 year, 1 month ago

Yes.Correct

upvoted 2 times

AbdulMueez 1 year, 7 months ago

Yes. Correct

upvoted 4 times

Question #27 *Topic 2*

You have an Azure subscription that contains a virtual machine named VM1 and uses Azure Defender. Azure Defender has automatic provisioning enabled.
You need to create a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1.
What should you do first?

A. From Azure Security Center, add a workflow automation.

B. On VM1, run the Get-MPThreatCatalog cmdlet.

C. On VM1 trigger a PowerShell alert.

D. From Azure Security Center, export the alerts to a Log Analytics workspace.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-alerts?view=o365-worldwide

Community vote distribution
C (83%) A (17%)

Lion007 Highly Voted 2 years, 6 months ago
Correct asnswer. Microsoft docs say: "For a rule to suppress an alert on a specific subscription, that alert type has to have been triggered at least once before the rule is created." https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule
upvoted 30 times

Gurulee 1 year, 2 months ago
Agreed, thank you for the confirming.
upvoted 1 times

Mthaher Highly Voted 2 years, 8 months ago
Correct , you need to generate the alert , then create the suppression rule
https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#what-are-suppression-rules
upvoted 6 times

chepeerick Most Recent 1 year, 2 months ago
Correct
upvoted 2 times

mali1969 1 year, 4 months ago
Selected Answer: C
C. On VM1 trigger a PowerShell alert. This will allow you to create a custom alert suppression rule based on the specific alert that you want to suppress.

To trigger a PowerShell alert on VM1, you can follow these steps:

On VM1, open PowerShell and run the following command: Invoke-WebRequest -Uri https://aka.ms/createalert
Wait for a few minutes until the alert is generated in Azure Security Center.
Go to Security Center in the Azure portal and select Security alerts.
Find the alert with the title “Suspicious use of PowerShell” and the resource name “VM1”.
Click on the alert to open its details pane.
upvoted 2 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 3 times

imhere4you 1 year, 6 months ago
On exam - 19 June 2023
upvoted 4 times

exmITQS 1 year, 10 months ago

Selected Answer: C

Before creating a custom alert suppression rule that will supress false positive alerts for suspicious use of PowerShell on VM1, you need to trigger the suspicious use of PowerShell alert on VM1. So the correct answer is C. On VM1 trigger a PowerShell alert.

upvoted 1 times

jrjrjrchlv 1 year, 11 months ago

Selected Answer: C

You should first C. trigger a PowerShell alert on VM1 to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1. After triggering the alert, you can use the information provided in the alert to create a suppression rule that will prevent similar alerts from being generated in the future.

upvoted 2 times

Lone__Wolf 1 year, 10 months ago

Yep yep!

upvoted 1 times

Fukacz 2 years, 3 months ago

Selected Answer: C

First you need an alert

upvoted 3 times

sainfosec 2 years, 4 months ago

Selected Answer: C

C for correct

upvoted 2 times

vnez 2 years, 4 months ago

Selected Answer: C

Correct!

upvoted 2 times

CatoFong 2 years, 5 months ago

Selected Answer: C

C is correct. Documentation provided by Lion007 and Mthaher

upvoted 3 times

sadako 2 years, 8 months ago

Selected Answer: A

Should be A

upvoted 3 times

j888 2 years, 8 months ago

I think C is correct. You will need an alert for this specific trigger and then you will be able to suppress it.

A is for automation response not supression.

upvoted 5 times

Question #27 *Topic 2*

HOTSPOT -

You have an on-premises datacenter that contains a custom web app named App1. App1 uses Active Directory Domain Services (AD DS) authentication and is accessible by using Microsoft Entra application proxy.

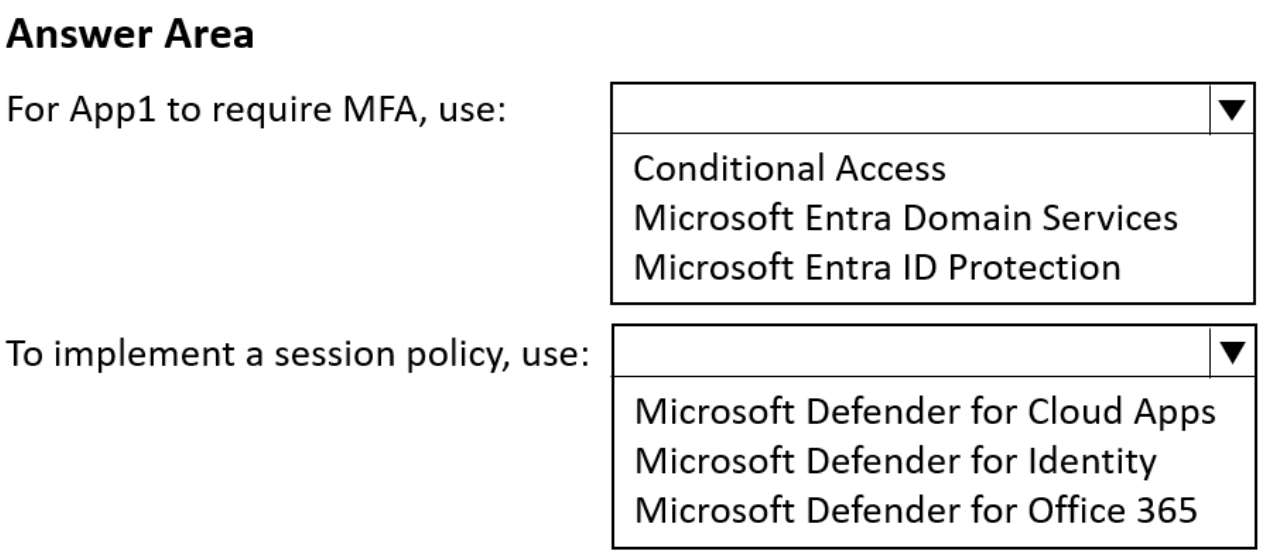
You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR.

You receive an alert that a user downloaded highly confidential documents.

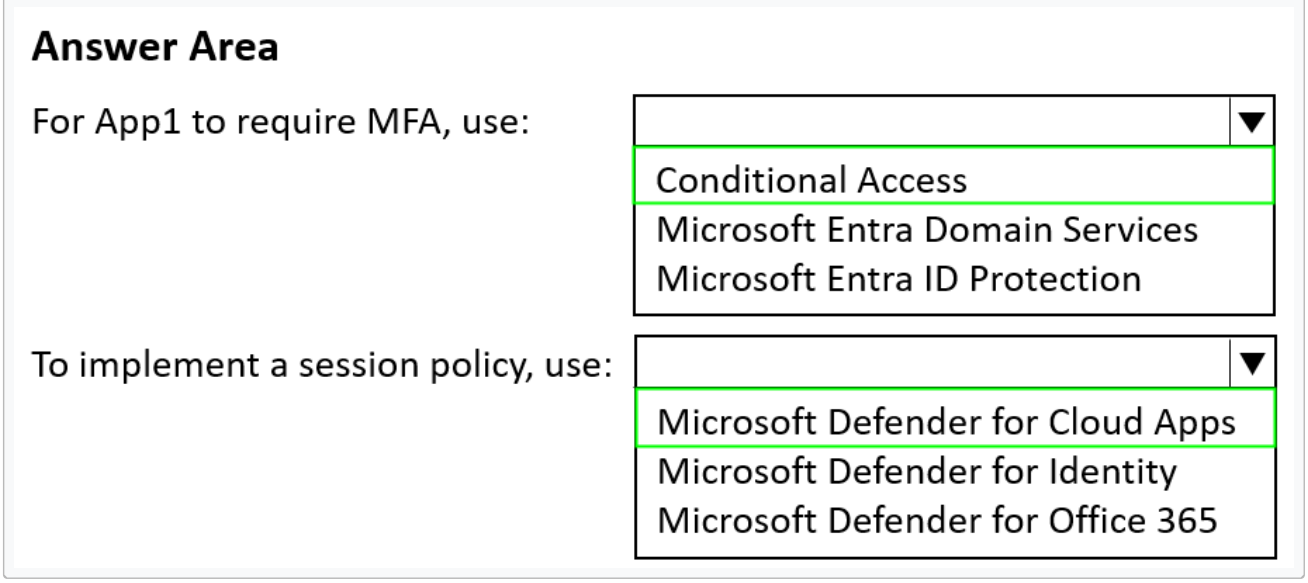
You need to remediate the risk associated with the alert by requiring multi-factor authentication (MFA) when users use App1 to initiate the download of documents that have a Highly Confidential sensitivity label applied.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Correct Answer:



Sparkletoss 1 month, 3 weeks ago

I think the answers are correct
https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

upvoted 1 times

Question #28 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You enable Azure Arc and onboard the virtual machines to Azure Arc.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

Community vote distribution
A (57%) B (43%)

Osamat98 Highly Voted 2 years, 2 months ago
Should Be Yes A

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc
upvoted 21 times

kazaki 11 months ago
You r all wrong azure arc for microsoft non azure machine means physically onprem
upvoted 2 times

Ramye 4 months, 4 weeks ago
No - because this Linux machine is a non-Azure machine as it is on AWS. you do need Azure Arc to get it onboarded to MS Defender for Cloud
upvoted 7 times

Tanasi Highly Voted 1 year, 9 months ago
Selected Answer: A
You need both Azure Arc to see the VM and the LAW agent.

Now, the agent can be automatically deployed after Azure Arc is deployed. Answer should be A) Yes.
upvoted 7 times

DChilds Most Recent 2 months, 1 week ago
Selected Answer: B
Enabling Azure Arc does not meet the objectives. Azure Defender for Cloud relies on Log Analytics agent to protect hybrid machines using Azure Defender for Cloud.

Answer is B.
upvoted 5 times

uday1985 1 month, 4 weeks ago
When automatic provisioning is enabled, Defender for Cloud uses the Log Analytics agent on all supported Azure VMs and any new ones that are created. Automatic provisioning is recommended but manual agent installation is also available.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/faq-data-collection-agents
upvoted 2 times

falkendarkness 4 months, 3 weeks ago

Yes, deploying Azure Defender and enabling auto-provisioning will allow you to monitor virtual machines across various cloud providers, including Amazon Web Services (AWS) and on-premises environments. However, enabling Azure Arc and onboarding the virtual machines to Azure Arc won't directly fulfill the goal of monitoring the virtual machines using Azure Defender.

Azure Arc enables you to extend Azure services and management to any infrastructure, including AWS, on-premises, and other cloud providers. While Azure Defender can be used to protect resources onboarded to Azure Arc, simply enabling Azure Arc and onboarding the virtual machines won't automatically monitor them with Azure Defender.

To monitor the Linux virtual machines on AWS using Azure Defender, you would typically need to deploy the appropriate agents or extensions on those machines to collect security-related data and send it to Azure Security Center for analysis. Then, Azure Defender will provide security insights and recommendations based on the collected data.

Therefore, the solution provided does not meet the goal.

upvoted 2 times

Jay_13 4 months, 3 weeks ago

Selected Answer: B

Enabling Azure Arc and onboarding virtual machines to Azure Arc does not directly meet the goal of monitoring virtual machines using Azure Defender. Azure Arc is a separate service that extends Azure management and services to any infrastructure, including on-premises servers and other cloud providers.

upvoted 1 times

Blachy 5 months, 2 weeks ago

Selected Answer: B

By ChatGPT the given answer is correct, so in B: "Azure Defender is a security service provided by Microsoft for Azure resources, and it is not designed to monitor or protect resources on other cloud platforms like AWS. To monitor virtual machines on AWS, you would typically use AWS-native services or third-party solutions."

upvoted 1 times

Ramye 4 months, 4 weeks ago

Azure Defender and Security are now Microsoft Defender for Cloud which supports multi-cloud platforms, e.g. AWS, GCP etc...

upvoted 1 times

mc250616 7 months, 1 week ago

From this link "https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc"

"If you're connecting machines from other cloud providers, see Connect your AWS account or Connect your GCP project. The multicloud connectors for Amazon Web Services (AWS) and Google Cloud Platform (GCP) in Defender for Cloud transparently handle the Azure Arc deployment for you."

Aso we need Azure RAc but MS Defender for Cloud will handle it for us by using multicloud connectors.

Perfect wording again in one another Micsrosoft Exam !!!

upvoted 1 times

Kurdd 8 months ago

Selected Answer: B

Option B is the correct answer: No.

Enabling Azure Arc and onboarding virtual machines to Azure Arc is not the correct way to monitor Linux virtual machines on Amazon Web Services (AWS) using Azure Defender. Azure Arc is primarily used for managing and monitoring resources in a hybrid environment, including on-premises and multi-cloud resources, but it doesn't specifically enable Azure Defender on virtual machines in AWS.

To monitor virtual machines on AWS with Azure Defender, you would typically use the Azure Security Center for AWS, which provides integration between Azure Defender and AWS resources. Azure Arc would not directly achieve this goal.

upvoted 1 times

chepeerick 8 months, 2 weeks ago

as Linux not Correct

upvoted 1 times

masterdeep 10 months, 2 weeks ago

From Microsoft:

Azure Arc-enabled servers lets you manage Windows and Linux physical servers and virtual machines hosted outside of Azure, on your corporate network, or other cloud provider. For the purposes of Azure Arc, these machines hosted outside of Azure are considered hybrid machines.

upvoted 4 times

aruninsiva 11 months, 2 weeks ago

Selected Answer: A

Since the question mentions 'Auto provisioning is enabled', Azure arc is able to do the task as Azure Arc is capable of 'automatic agent provisioning'.

upvoted 4 times

Marchiano 11 months, 2 weeks ago

Selected Answer: A

Defender for Cloud leverages Azure Arc to simplify the on-boarding and security of virtual machines running in AWS and other clouds. This includes automatic agent provisioning, policy management, vulnerability management, embedded EDR, and much more.

Keyword: automatic agent provisioning

Source https://techcommunity.microsoft.com/t5/itops-talk-blog/step-by-step-how-to-connect-aws-machines-to-microsoft-defender/ba-p/3251096

upvoted 4 times

Marchiano 11 months ago

Sorry guys, I have changed my mind to B, as the provided solution is not complete.

upvoted 1 times

omar_alhajsalem 1 year, 1 month ago

Selected Answer: B

the Question says that you need to monitor not connect if the question says you need to connect the VM on AWS to Azure Defender the answer will be yes but in this case even if I choose yes it will need to install Log Agent to monitor the VM So the Question Says I need to Monitor so enabling Azure Arc won't be the best choice so I go with B

upvoted 3 times

xping85 10 months, 3 weeks ago

auto provisioning is enabled so we don't need to install the agent manually.

Reference: https://learn.microsoft.com/en-us/azure/defender-for-cloud/auto-deploy-azure-monitoring-agent

upvoted 1 times

Rubes 1 year, 4 months ago

ChatGPT says A too lol

upvoted 7 times

Zzziambored 1 year ago

No it does not:

No, enabling Azure Arc and onboarding the Linux virtual machines to Azure Arc does not meet the goal of monitoring the virtual machines using Azure Defender.

Azure Arc is a service that extends Azure management capabilities to resources outside of Azure, including on-premises and multi-cloud environments. It allows you to manage and govern these resources using Azure tools and services. However, Azure Arc itself does not provide the security monitoring and threat detection capabilities offered by Azure Defender.

upvoted 5 times

Marchiano 11 months ago

Check what auto-provisioning is capable of on https://learn.microsoft.com/en-us/azure/defender-for-cloud/auto-deploy-azure-monitoring-agent

Deploy the Azure Monitor Agent with Defender for Cloud

upvoted 2 times

exmITQS 1 year, 4 months ago

Selected Answer: A

A. Yes, this meets the goal. By enabling Azure Arc and onboarding the Linux virtual machines to Azure Arc, you can monitor them using Azure Defender

upvoted 3 times

Lone__Wolf 1 year, 4 months ago

A is the way to go!

upvoted 3 times

Xyz_40 1 year, 9 months ago

answer is A, YES. Brcause auto provisioning is already turned on

upvoted 6 times

Question #29 *Topic 2*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have Linux virtual machines on Amazon Web Services (AWS).
You deploy Azure Defender and enable auto-provisioning.
You need to monitor the virtual machines by using Azure Defender.
Solution: You manually install the Log Analytics agent on the virtual machines.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc

Community vote distribution
B (100%)

ejml Highly Voted 2 years, 7 months ago
Wrong answer. it should be A.
A machine with Azure Arc-enabled servers becomes an Azure resource and - when you've installed the Log Analytics agent on it - appears in Defender for Cloud with recommendations like your other Azure resources.
upvoted 11 times

xRiot007 4 weeks, 1 day ago
You need Azure Arc before the agent can be installed.
upvoted 2 times

Drui 2 years, 7 months ago
It's B because it doesn't mention Azure Arc, it just says Log analytics agent (which by the way is going to be deprecated and replaced by Azure monitor agent) https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-overview?tabs=PowerShellWindows
upvoted 12 times

Anonymousse 2 years, 3 months ago
But the Tip on that link says:
Tip

If you're onboarding machines running on Amazon Web Services (AWS), Defender for Cloud's connector for AWS transparently handles the Azure Arc deployment for you. Learn more in Connect your AWS accounts to Microsoft Defender for Cloud.
upvoted 1 times

Holii 1 year, 8 months ago
SC-200 documentation says otherwise: https://learn.microsoft.com/en-us/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

Complete Azure Arc prerequisites
Make sure the appropriate Azure resources providers are registered:
Microsoft.HybridCompute
Microsoft.GuestConfiguration
upvoted 1 times

Nailik_Ms Highly Voted 1 year, 11 months ago
Selected Answer: B

The question has few traps.
1. You have Linux machines on AWS. (don't specify if already onboarded)
2. You deploy a solution (Azure defender and enable auto provisioning) This doesn't mean any interaction with the previous Linux Machines.

HERE: YOU NEED TO MONITOR THOSE VM WITH AZURE DEFENDER. meaning first we need to do the first step to monitor them, and that first step is not install the Log analytics agent. First we should enable Azure Arc on them. So I think answer is no B
upvoted 9 times

VeiN Most Recent 2 months, 1 week ago
OK so few things:
1. When auto-provisiong worked it worked with MMA agent (Log Analytcis Agent) which is not reliant on Azure Arc. Azure Arc works with AMA & could potentialy be auto-provisioned when ARC was installed (for instance by policy) which is current approach.
Note there is also Multicloud connectors in preview on Azure Arc dashboard.
2. According to this link & checkup there is no auto-provisioning anymore therfore this question is outdated & broken.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/prepare-deprecation-log-analytics-mma-agent?WT.mc_id=Portal-Microsoft_Azure_Security#log-analytics-agent-autoprovisioning-experience---deprecation-plan
upvoted 1 times

uday1985 8 months ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/faq-data-collection-agents
upvoted 1 times

Fedemend 11 months, 2 weeks ago
B. No

Enabling auto-provisioning for Azure Defender means that the required monitoring agents, including the Log Analytics agent, will be automatically installed on the virtual machines. Therefore, there is no need to manually install the Log Analytics agent if auto-provisioning is enabled. The correct answer is "B. No."
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

Marchiano 1 year, 5 months ago
Guys, I am now on MS Defender for Cloud (Getting started) and there is one option here called "Add non-Azure servers" with the following description: "Use the Log Analytics agent to extend Microsoft Defender for Cloud capabilities to servers running outside of Azure, including resources running on-premises and in other clouds."

What are some of the MS Defender for Cloud extended capabilities?
1. Secure cloud application
2. Improve your security posture
3. Protect cloud workloads

Please check also what the Log Analytics agent/extension is capable of, search on the web.

"Azure Monitor Logs provides monitoring, alerting, and alert remediation capabilities across cloud and on-premises assets. [..] The extension installs the Log Analytics agent on Azure virtual machines, and enrolls virtual machines into an existing Log Analytics workspace."

So even if it will be deprecated at some point in 2024, it is still a valid solution in the present.
upvoted 3 times

Marchiano 1 year, 5 months ago
A. Yes
upvoted 2 times

Doinitza 1 year, 4 months ago
Then, what is the purpose of Azure Arc?
upvoted 1 times

XLR8T2 1 year, 5 months ago
No es necesario instalar Log Analytics para monitorear, con Azure Arc es suficiente, respuesta B es la correcta.
upvoted 1 times

Sri534 1 year, 10 months ago

B is correct .. Explanation form ChatGPT
No, manually installing the Log Analytics agent on the virtual machines is not the correct solution for monitoring the virtual machines using Azure Defender after enabling auto-provisioning.

When Azure Defender is enabled with auto-provisioning, it automatically deploys the necessary monitoring agents on the virtual machines. In this case, since you have deployed Linux virtual machines on AWS, you would need to configure the Azure Defender for servers (Linux) solution to monitor these virtual machines. Once enabled, Azure Defender for servers (Linux) will automatically deploy the necessary monitoring agents on the virtual machines without the need for manual installation.

upvoted 3 times

Phantasm 1 year, 11 months ago

Selected Answer: B

B is correct. In order to monitor Linux virtual machines on AWS with Azure Defender, you need to install the Log Analytics agent manually on the virtual machines.

upvoted 2 times

Sango 2 years, 5 months ago

These are non-Azure, AWS PCs. You need to link the AWS environment using Azure Arc first.

upvoted 3 times

Lion007 2 years, 6 months ago

Selected Answer: B

B is Correct. The full correct answer should be "You enable Azure Arc to onboard the virtual machines to Azure Arc, then you enable auto-provisioning to install the Log Analytics agent on the virtual machines automatically."

upvoted 5 times

BlueLightRun 2 years, 7 months ago

Selected Answer: B

https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-portal

There is a manual process for adding VMs

upvoted 1 times

StaxJaxson 2 years, 7 months ago

https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-loganalytic

upvoted 1 times

Question #30 *Topic 2*

You have five on-premises Linux servers.
You have an Azure subscription that uses Microsoft Defender for Cloud.
You need to use Defender for Cloud to protect the Linux servers.
What should you install on the servers first?

A. the Dependency agent

B. the Log Analytics agent

C. the Azure Connected Machine agent

D. the Guest Configuration extension

Suggested Answer: *B*
Defender for Cloud depends on the Log Analytics agent.
Use the Log Analytics agent if you need to:
* Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure
* Etc.
Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/os-coverage https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#log-analytics-agent

Community vote distribution
C (69%) B (31%)

Lone_Wolf Highly Voted 1 year, 10 months ago
Selected Answer: C
The Azure Connected Machine agent is required to connect the on-premises Linux servers to the Azure subscription and integrate them with Microsoft Defender for Cloud. The agent enables communication between the servers and the Defender for Cloud service, allowing security events and data to be collected and analyzed.

Once the Azure Connected Machine agent is installed, you can then install the Log Analytics agent to collect security data from the servers and send it to the Log Analytics workspace in Azure. This will allow you to use Defender for Cloud to monitor the security of your Linux servers, identify threats, and respond to security incidents.
upvoted 23 times

Ramye 10 months, 4 weeks ago
Yes, C appears to be the correct answer
Log Analytics agent and the Azure Monitor agent are the components of the Azure Connected Machine agent.
upvoted 3 times

mfalkjunk Highly Voted 1 year, 8 months ago
Selected Answer: C
I will go with C first, then LA-Agent:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-agents
upvoted 11 times

Yethi_Consulting56 Most Recent 4 months, 1 week ago
Scaling your QA process for large projects requires robust testing automation tools. These tools allow you to handle extensive test cases efficiently by automating repetitive and time-consuming tasks like regression testing. Automation enables parallel test execution, significantly reducing testing time as the project grows. With the ability to integrate into CI/CD pipelines, these tools ensure continuous testing, providing rapid feedback on code changes. Moreover, automated testing improves accuracy, consistency, and coverage, ensuring that even large, complex systems maintain high quality. By leveraging testing automation tools, you can scale your QA processes without compromising speed or reliability.
upvoted 1 times

user636 4 months, 1 week ago
Selected Answer: C

Answer is: C

This is an indeed a tricky question. Focus what is the goal in the question.
Log Analytics Agent can be manually installed on an on-premise machine without first installing azure connected machine (ACM) agent. However, the recommended method is to use ACM, as it provides many other features. Because of this reason, I'll go with C.
Ref: https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent#linux-virtual-machine-on-premises-or-in-another-cloud

The Azure Connected Machine agent package contains several logical components bundled together.
https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview#agent-components
upvoted 1 times

albatros06 8 months, 1 week ago

Selected Answer: B

The Log Analytics agent or Azure Monitor Agent for Windows and Linux is required in order to:

Proactively monitor the OS and workloads running on the machine
Manage it using Automation runbooks or solutions like Update Management
Use other Azure services like Microsoft Defender for Cloud
upvoted 1 times

KRAKE3N 8 months, 2 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview

The Azure Connected Machine agent enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers.

*Note

The Azure Monitor agent (AMA) is a separate agent that collects monitoring data, and it does not replace the Connected Machine agent; the AMA only replaces the Log Analytics agent, Diagnostics extension, and Telegraf agent for both Windows and Linux machines.
upvoted 2 times

Sneekygeek 8 months, 3 weeks ago

Selected Answer: C

This document suggests that Azure Arc must be installed before Log Analytics from non-Azure resources.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines

The connected machine agent looks to be a component of Arc.
https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview
upvoted 2 times

Orel123 10 months, 2 weeks ago

Log Analytics agent should be installed on your Linux-based Azure Arc machines

source:

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines#:~:text=Log%20Analytics%20agent%20should%20be%20installed%20on%20your%20Linux%2Dbased%20Azure%20Arc%20machines
upvoted 2 times

Murtuza 1 year, 1 month ago

The Azure Connected Machine agent enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers
upvoted 1 times

kabooze 1 year, 2 months ago

Selected Answer: C

the azure connected machine agent aka azure arc agent is needed for every machine asset outside of azure
upvoted 1 times

chepeerick 1 year, 2 months ago

Correct

upvoted 1 times

Mercury02m 1 year, 2 months ago

Which is correct ?? so much confusion on B and C ?

upvoted 1 times

Willmc12 1 year, 2 months ago

When you onboard to AMA Azure Machine agent it automatically onboard you to defender. The question is asking for you to protect the machines not ingest logs. You want to protect the servers. The correct answer is C

upvoted 1 times

Gurulee 1 year, 2 months ago

Selected Answer: B

Arc his overkill here, Defender for Cloud is key. https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines#connect-on-premises-machines-by-using-the-azure-portal

upvoted 2 times

TeresaCN 1 year, 3 months ago

Selected Answer: B

I will go for B

upvoted 2 times

cris_exam 1 year, 3 months ago

Selected Answer: B

As this question has nothing mentioned about Azure ARC and there is an option to onbaord Linux VMs onprem without ARC, I go with B - Log Analytics.

As described in the doc below, the Linux machine get's onboarded after wget-ing the required Workspace package (through Log Analytics) and then it becomes available in Defender for Cloud without ARC (which would have required the Azure Connected Machine agent).

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines#onboard-your-linux-server

upvoted 3 times

NICKTON81 1 year, 3 months ago

Selected Answer: B

B - The Log Analytics Agent

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines

upvoted 2 times

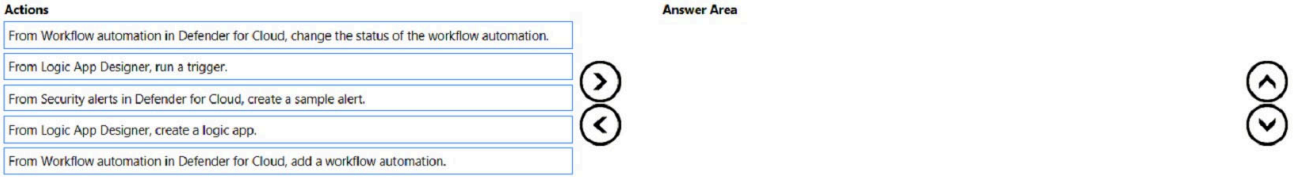
DRAG DROP -

You have an Azure subscription. The subscription contains 10 virtual machines that are onboarded to Microsoft Defender for Cloud.

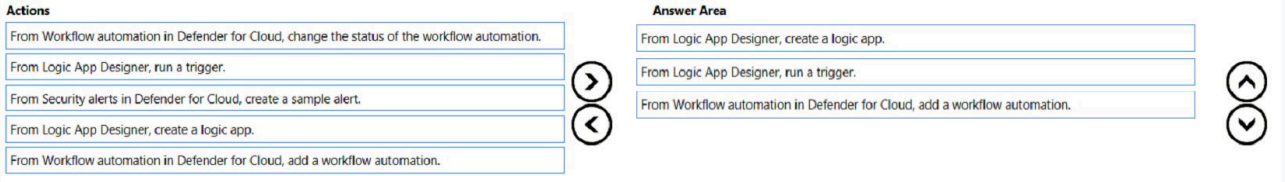
You need to ensure that when Defender for Cloud detects digital currency mining behavior on a virtual machine, you receive an email notification. The solution must generate a test email.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



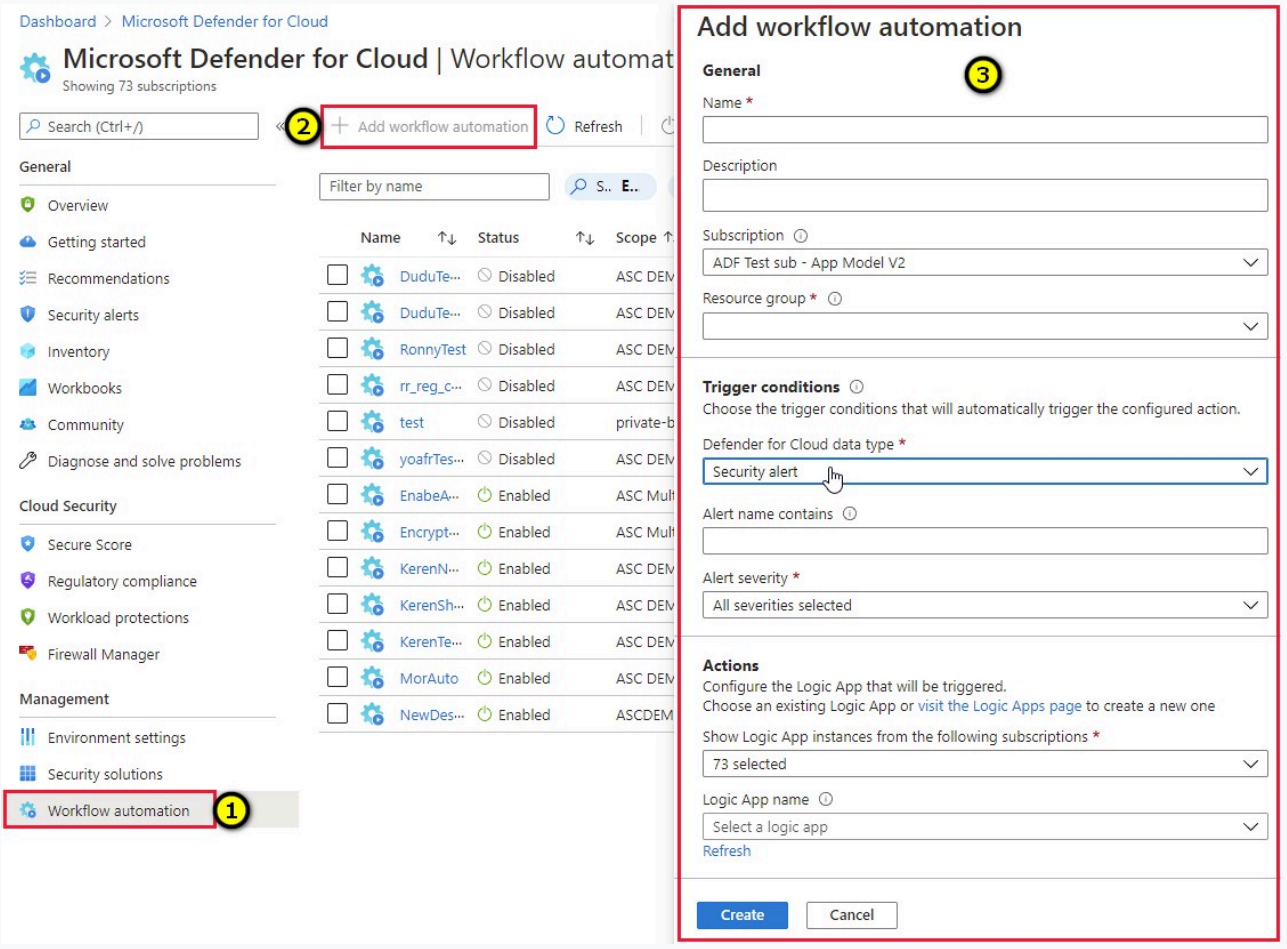
Suggested Answer:



Step 1: From Logic App Designer, create a logic app.

Create a logic app and define when it should automatically run

1. From Defender for Cloud's sidebar, select Workflow automation.
2. To define a new workflow, click Add workflow automation. The options pane for your new automation opens.



Here you can enter:

A name and description for the automation.

The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.

The Logic App that will run when your trigger conditions are met.

3. From the Actions section, select visit the Logic Apps page to begin the Logic App creation process.

4. Etc.
Step 2: From Logic App Designer, run a trigger.

Manually trigger a Logic App -
You can also run Logic Apps manually when viewing any security alert or recommendation.
Step 3: From Workflow automation in Defender for cloud, add a workflow automation.
Configure workflow automation at scale using the supplied policies
Automating your organization's monitoring and incident response processes can greatly improve the time it takes to investigate and mitigate security incidents.

Reference:
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Metasploit Highly Voted 2 years, 2 months ago

This solution does not meet the sequence specified in the question. The solution must generate a test email.

Correct answer is:

1) Create logic app
2) Add workflow automation (specifies action - send email)
3) Trigger logic app (creates alert->workflow automation activates -> sends email)
upvoted 17 times

Tuitor01 4 weeks ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules
1) First automation workflow
2) Crate your logicapp
3) Inside your logicapp designer pager nothing prevents you from testing the trigger
upvoted 1 times

BieLey 2 years, 1 month ago

But don't you need to run a trigger before you should to the workflow automation?
upvoted 7 times

HAjouz 3 weeks, 1 day ago

These steps align with the process described in the Microsoft documentation:

Create a sample alert: This helps you test the workflow automation.
Create a Logic App: This app will define the actions to take when an alert is triggered.
Add a workflow automation: This links the Logic App to the specific alert, ensuring that the defined actions are executed when the alert is triggered.
upvoted 1 times

Marchiano Highly Voted 1 year, 5 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Create a logic app and define when it should automatically run
1. From Defender for Cloud's sidebar, select Workflow automation.
2. To define a new workflow, select Add workflow automation.
3. From the Actions section, select visit the Logic Apps page to begin the logic app creation process.
4. Select (+) Add.
5. Fill out all required fields and select Review + Create.
6. Review the information you entered and select Create.
7. After you've defined your logic app, return to the workflow automation definition pane ("Add workflow automation"). Select Refresh to ensure your new logic app is available for selection.
8. Select your logic app and save the automation. The logic app dropdown only shows those with supporting Defender for Cloud connectors mentioned above.

Given the above, the answer should be:
1. From Workflow automation in Defender for Cloud, add a workflow automation
2. From Logic App Designer, create a logic app
3. From Logic App Designer, run a trigger
upvoted 13 times

davidli 1 year, 2 months ago
This is very valid to me.
upvoted 2 times

kabooze 1 year, 2 months ago
yes, but nothing stops you from creating the logic app before creating the workflow automation. So technically it's
-> create logic app
-> create workflow automation
-> run trigger
upvoted 2 times

user636 Most Recent 4 months, 1 week ago
The correct answer is:
- Step1: Create a Logic app (this will a part of process of creating a workflow automation), the logic app will use "Defender for cloud alert is triggered" as a trigger. The logic app will have a an action item to send email notifications. When the workflow automation in step2 will run, it will automatically run this logic app.
- Step2: Create a workflow automation & use "Security alert" as the cloud data type. This will make sure that this workflow automation will run whenever there is a security alert generated. In the action option "select the logic app" created in Step1. If you do not create the logic app in step1, then it will NOT be shown in the workflow automation page.
- Step3: From the Security alerts in MDC, create a sample alert. There is a sample alert for "digital currency mining".

Once the sample security alert is created, it will trigger the workflow automation & the workflow automation will trigger the logic app. The logic app will send the email.

This is how you do it in real world.
upvoted 1 times

user636 4 months, 1 week ago
The answer is:
Add workflow automation
Create a logic app
Create a sample alert.
as explained in my other comment.
The process in both comments will get the results in the real world. However as per Microsoft docs, start with workflow automation and then logic creation...
upvoted 1 times

user636 4 months, 1 week ago
Keep it simple & don't overthink:
You will first start with creating a workflow automation, during the process you will create a logic app as one of the step. In workflow automation you will define the Trigger conditions. You can use "alert name contains" to define digital currency mining as a trigger. During the logic app creation you will use send email as an action. Once the logic app is created, you will generate a sample alert, this will ensure/test that the workflow automation & logic app in use are both working fine.

The answer is:
Add workflow automation
Create a logic app
Create a sample alert.

There is a sample alert for digital currency mining (ref: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation)
upvoted 1 times

Ramye 10 months, 2 weeks ago
See, you must have a Logic app available to be used for creating workflow automation steps, and you need to have an alert by a trigger for setting up the automation, therefore, the ans should be:
- create the logic app
- trigger the logic app to test
- and finally, add the workflow automation
upvoted 4 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

NICKTON81 1 year, 3 months ago
The answer is correct!
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 2 times

vdabhi123 1 year, 5 months ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
Create a logic app and define when it should automatically run
Manually trigger a logic app
Configure workflow automation at scale using the supplied policies
upvoted 4 times

XLR8T2 1 year, 5 months ago
Estas son las respuestas correctas:

1. From Logic App Designer, create a logic App. -> Correcto: Primero necesitas que exista un LogicApp.
2. From Workflow automation in Defender for Cloud, add workflow automation. -> Correcto: agregar el Logic App antes creado.
3. From Security alerts in Defender for Cloud, create a sample alerta -> Correcto: Para realizar y probar que tu Logic App funciona.
upvoted 3 times

imhere4you 1 year, 6 months ago
On exam - 19 June 2023
upvoted 8 times

teouba 1 year, 8 months ago
If you trigger the app, before you create the workflow, then what's the point?
The provided answer doesnt make any sense, first you need to create the workflow and then trigger the alert
upvoted 5 times

JoeP1 1 year, 5 months ago
Running the trigger tests that the logic app sends the email properly, but does not test the workflow that runs the logic app.
upvoted 2 times

ACSC 2 years, 1 month ago
Answer is correct.
You should:
create the logic app
trigger the logic app to test
and finally add the workflow automation,
upvoted 7 times

Fukacz 2 years, 3 months ago
Correct.

1. Create Logic App
2. trigger (test)
3. apply

upvoted 3 times

amsioso 2 years, 3 months ago

And what happend with "create a sample alert"??

upvoted 3 times

Frankie21 1 year, 2 months ago

indeed that is the one you need to test it

upvoted 1 times

Question #32 *Topic 2*

DRAG DROP
-

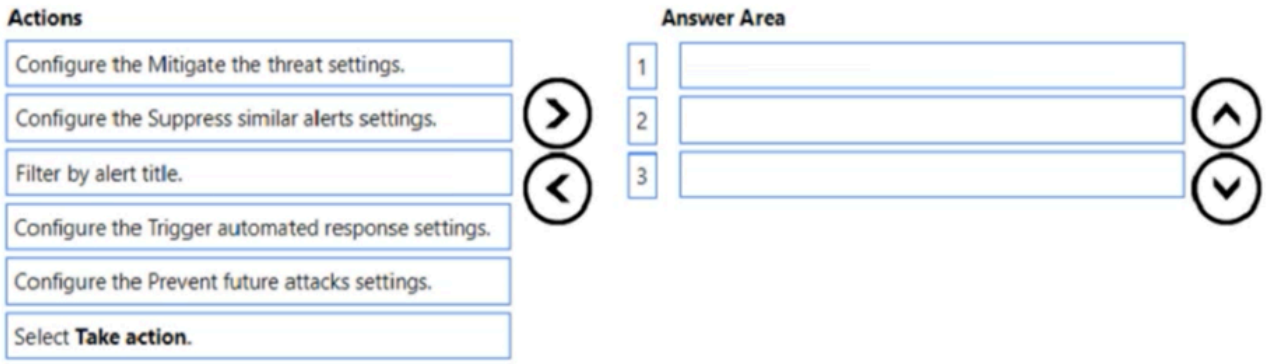
You have a Microsoft subscription that has Microsoft Defender for Cloud enabled.

You configure the Azure logic apps shown in the following table.

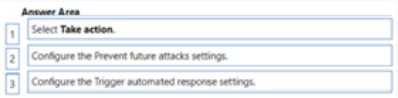
Name	Trigger	Action
LogicApp1	When a Defender for Cloud recommendation is created or triggered	Send an email
LogicApp2	When a Defender for Cloud alert is created or triggered	Send an email

You need to configure an automatic action that will run if a Suspicious process executed alert is triggered. The solution must minimize administrative effort.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Suggested Answer:



saurabh123sml Highly Voted 1 year, 5 months ago
Filter by Alert Title
Take Action
Trigger Automated Response
upvoted 46 times

HAjouz 3 weeks, 1 day ago
Select Take action.
Configure the Trigger automated response settings.
Configure the Prevent future attacks settings.
upvoted 1 times

ACSC Highly Voted 1 year, 5 months ago
Filter by alert title
Select Take action
Configure the Trigger automated response settings

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts
upvoted 22 times

RodrigoLima 1 year, 5 months ago

Actually correct! Just pay attention to the link content.

"Trigger automated response - provides the option to trigger a logic app as a response to this security alert"

while

"Prevent future attacks - provides security recommendations to help reduce the attack surface, increase security posture, and thus prevent future attacks"

upvoted 4 times

Jay_13 Most Recent 4 months, 3 weeks ago

Filter by Alert Title

Select Take Action

Trigger Automated Response

upvoted 2 times

chepeerick 8 months, 2 weeks ago

Filter by Alert Title

Take Action

Trigger Automated Respons

upvoted 1 times

donathon 10 months, 1 week ago

Filter by Alert Title

Take Actions

Configure the Trigger Automated Response settings

upvoted 1 times

XLR8T2 11 months, 3 weeks ago

La respuesta correcta es:

1. Filter by alert title
2. Select take action
3. Configure Trigger automard response settings

Con esto utilizas el LogicApp_2 previamente informado en la pregunta.

upvoted 1 times

ct1984 1 year ago

It's INCREDIBLY frustrating that the answers are NEVER updated.

upvoted 17 times

Ramye 4 months, 3 weeks ago

@ExamTopics, paying attention?

upvoted 2 times

QM21 1 year, 5 months ago

Shouldn't it mitigate first?

upvoted 1 times

ACSC 1 year, 5 months ago

No, you need to configure an automatic action. Mitigate the threat provides manual remediation steps.

upvoted 4 times

Question #33 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine named Server1 that runs Windows Server 2022 and is hosted in Amazon Web Services (AWS).

You need to collect logs and resolve vulnerabilities for Server1 by using Defender for Cloud.

What should you install first on Server1?

A. the Microsoft Monitoring Agent

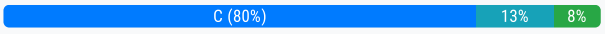
B. the Azure Monitor agent

C. the Azure Arc agent

D. the Azure Pipelines agent

Suggested Answer: *B*

Community vote distribution



teouba Highly Voted 1 year, 8 months ago

Typical Microsoft Question..
In order to collect logs and connect to Defender for Cloud you need Azure monitor Agent, but first you also need to connect the machine to Azure so you have to install Azure Arc Agent which is actually called Azure Connected Machine Agent.
So answering this question is impossible because the answers provided are as stupid as the question

upvoted 31 times

appieh4ck Highly Voted 1 year, 11 months ago

Selected Answer: C

Azure Arc for servers installed on your EC2 instances
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings

upvoted 18 times

nhmh90 1 year, 11 months ago

Other extensions should be enabled on the Arc-connected machines:
-Microsoft Defender for Endpoint
-VA solution (TVM/Qualys)
-Log Analytics (LA) agent on Arc machines or Azure Monitor agent (AMA)

Make sure the selected LA workspace has security solution installed. The LA agent and AMA are currently configured in the subscription level.
All of your AWS accounts and GCP projects under the same subscription will inherit the subscription settings for the LA agent and AMA.

upvoted 1 times

uday1985 1 year, 6 months ago

Where the agent is required to be installed?? on the windows ? or on the EC2 instance?

upvoted 1 times

Sekpluz Most Recent 6 months, 3 weeks ago

Selected Answer: C

First C and then B

upvoted 1 times

ecasjo 8 months ago

I can't find anything called as "Azure Arc Agent" in the documentation.
If this is the Azure Connected Machine agent why don't just call it like that?

upvoted 2 times

DChilds 8 months, 1 week ago

As of April 2024, the answer to this question is always the Microsoft Monitoring Agent, previously known as the Log Analytics Agent.

The Microsoft Practice exams also highlight the agent even when Azure Arc is part of the choices.
upvoted 2 times

Murtuza 1 year ago
To answer these type of ambiguous question its important to pay attention to " what must be installed first " typically in all cases it will be the ARC AGENT as your answer dont over think this
upvoted 4 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

donathon 1 year, 4 months ago
ARC is a pre-requisite and enable auto-provisioning.
upvoted 1 times

xping85 1 year, 4 months ago
The question says by using Defender for Cloud -> so Azure Monitor Agent is not the correct Answer.
C is the correct answer
upvoted 1 times

XLR8T2 1 year, 5 months ago
La respuesta correc es la C: C. the Azure Arc agent Most Voted
Ya que la pregunta hace mención que tambien se requiere resolver vulnerabilidades, al desplegar conectarte con la instancia de EC2 solo se instala AMA, pero para las vulnerabilidades necesitas Microsoft Defender for Server que contiene Microsoft Defender for Endpoint (VM) y esa extensión se instala con Azure Arc.
upvoted 1 times

billo79152718 1 year, 7 months ago
Selected Answer: C
C. The Azure Arc Agent
upvoted 1 times

exmITQS 1 year, 10 months ago
Selected Answer: A
Option B (the Azure Monitor agent) is incorrect, as it is used for monitoring and collecting performance data, not security-related logs or vulnerability assessments.

Option C (the Azure Arc agent) is also incorrect, as it is used for managing servers and other resources across different environments, but not specifically for collecting security-related logs or vulnerability assessments.

Option D (the Azure Pipelines agent) is also incorrect, as it is used for building and deploying applications, not for security-related tasks.

To collect logs and resolve vulnerabilities for Server1 using Defender for Cloud, you should install the Microsoft Monitoring Agent (MMA) on Server1 first
upvoted 3 times

Holii 1 year, 8 months ago
AMA agent is the replacement for the Legacy MMA agent...and can also be used for security-related logs (Syslog/CEF).
This is simply a syntax issue between whether Azure Arc is preconfigured or not.
Since MMA and AMA are options here, I assume it's C.
upvoted 3 times

Rockf0rd 1 year, 10 months ago
Selected Answer: C
In the following article, it is clearly indicated that installing Azure Arc is a prerequisite which is the first thing to do
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings
upvoted 4 times

Lone__Wolf 1 year, 10 months ago
Selected Answer: C

I will go with C as B doesn't state the correct agent name 'Azure Connected Machine agent'. So 'Azure Arc Agent' makes more sense. Further 'Azure Connected Machine agent' and 'Microsoft Monitoring Agent' is not same.

upvoted 6 times

Raminjan 1 year, 10 months ago

This is from MS documentation - Non-Azure: To install the agent on physical servers and virtual machines hosted outside of Azure (that is, on-premises) or in other clouds, you must install the Azure Arc Connected Machine agent first, at no added cost.

upvoted 1 times

Subhakaran 1 year, 10 months ago

Selected Answer: B

To connect hybrid machines to Azure, you install the Azure Connected Machine agent on each machine. This agent does not replace the Azure Log Analytics agent / Azure Monitor Agent. The Log Analytics agent or Azure Monitor Agent for Windows and Linux is required in order to:

Proactively monitor the OS and workloads running on the machine
Manage it using Automation runbooks or solutions like Update Management
Use other Azure services like Microsoft Defender for Cloud

upvoted 2 times

Subhakaran 1 year, 10 months ago

To connect hybrid machines to Azure, you install the Azure Connected Machine agent on each machine. This agent does not replace the Azure Log Analytics agent / Azure Monitor Agent. The Log Analytics agent or Azure Monitor Agent for Windows and Linux is required in order to:

Proactively monitor the OS and workloads running on the machine
Manage it using Automation runbooks or solutions like Update Management
Use other Azure services like Microsoft Defender for Cloud

upvoted 1 times

Question #34 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a storage account named storage1.

You receive an alert that there was an unusually high volume of delete operations on the blobs in storage1.

You need to identify which blobs were deleted.

What should you review?

A. the activity logs of storage1

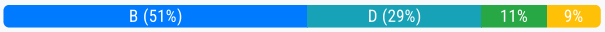
B. the Azure Storage Analytics logs

C. the alert details

D. the related entities of the alert

Suggested Answer: *B*

Community vote distribution



RodrigoLima Highly Voted 1 year, 11 months ago

Selected Answer: B

Seems like the answer is actually correct.
"Azure Storage Analytics performs logging and provides metrics data for a storage account. You can use this data to trace requests, analyze usage trends, and diagnose issues with your storage account."

upvoted 12 times

imhere4you Highly Voted 1 year, 6 months ago

On exam - 19 June 2023

upvoted 7 times

HAjouz Most Recent 3 weeks, 1 day ago

Selected Answer: A

Activity logs offer a more precise and reliable way to identify the deleted blobs because they capture detailed information about each operation performed on the storage account. By analyzing these logs, you can pinpoint the exact blobs that were deleted, the time of deletion, and potentially the user or process responsible.

upvoted 2 times

talosDevbot 3 months ago

Selected Answer: D

D) "Related entities" of the alert

Question is saying you need to identify the blob involved in the alert you just received.
Each alert in Defender for Cloud has a "Related entities" section. 'Entities' can be users, IP addresses, Resource ID, Hostname, File, Process.

In this case, the Related entities section will have the resource ID of the blob related to the alert

upvoted 2 times

user636 4 months, 1 week ago

Selected Answer: D

The answer is D.

upvoted 1 times

user636 4 months, 1 week ago

The answer is D.

Related entities will have the details of the blobs that were deleted.
The alert details does not give the name of the blobs, but will only list the "Operations" that was performed. In this scenario, the operation name is "Storage.Blob_DeletionAnomaly".

(Ref: https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-azure-storage#unusual-deletion-in-a-storage-account)

The question expects you to use the tool "Microsoft Defender for Cloud", so try to stick with the options/features provided by the tool & not the complete Azure platform.

upvoted 1 times

Sekpluz 6 months, 3 weeks ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts

upvoted 2 times

Sneekygeek 8 months, 3 weeks ago

Selected Answer: D

Under the alert details there is a related entities field which will tell you to which resources are related to the alert. I would definitely start here before I dove blindly into the logs.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts

upvoted 1 times

ostralo 9 months, 3 weeks ago

The answer is D.

When you open an Alert(Delete operations on the blobs in storage 1)

When you open the alert by clicking "View full details", it shows you the Alert details tab.

If you scroll down, you will find the "Related entities" section.

It shows Azure Resource (Resource ID, Subscription ID), Blob container (Name, Storage resource) etc..

It doesn't make sense the alert doesn't provide blob container name.

upvoted 2 times

Gurulee 12 months ago

To identify deleted blobs in Azure Blob Storage, you can enable Storage Analytical logs. These logs contain details of each and every operation, including the ones that delete blobs.

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct

upvoted 1 times

NICKTON81 1 year, 3 months ago

Selected Answer: D

D - Related Entities

https://learn.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts#respond-to-security-alerts

upvoted 3 times

mali1969 1 year, 3 months ago

Selected Answer: D

The activity logs of storage1 and the Azure Storage Analytics logs are not sufficient to identify the deleted blobs, as they only provide general information about the operations performed on the storage account. The alert details provide more specific and contextual information about the activity and the related entities

upvoted 3 times

mali1969 1 year, 3 months ago

The related entities are the objects that are involved in or affected by the activity, such as blobs, containers, files, shares, directories, etc. You can use the related entities to identify which blobs were deleted in your storage account

upvoted 2 times

donathon 1 year, 4 months ago

Selected Answer: B

https://learn.microsoft.com/en-us/rest/api/storageservices/storage-analytics-logged-operations-and-status-messages#logged-operations

upvoted 1 times

[Removed] 1 year, 4 months ago

Selected Answer: B

Azure Storage Analytics logs provide detailed insights into the activities performed on your storage account, including information about blob operations like delete operations. These logs capture information about operations, including their types, targets, timestamps, and

authentication details. By analyzing the Storage Analytics logs, you can determine which blobs were deleted and gather other relevant details about the delete operations.

The other options are not as directly related to identifying which specific blobs were deleted:

A. the activity logs of storage1: While the activity logs provide information about management activities and data plane operations on Azure resources, they might not contain the detailed information needed to identify individual deleted blobs.

upvoted 1 times

therealletsgo 1 year, 8 months ago

Tough one, but B seems to be for "Storage Analytics logs detailed information about successful and failed requests to a storage service."
I suppose I will go with A and be the black sheep based on these:
https://learn.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/storage/blobs/monitor-blob-storage-reference

upvoted 1 times

therealletsgo 1 year, 8 months ago

nvm on this....

upvoted 2 times

haskelatchi 1 year, 8 months ago

Selected Answer: C

You are all incorrect. Answer is C

When Microsoft Defender for Cloud generates an alert, it includes detailed information about the event that triggered the alert, including information about the specific resources that were affected. In this case, since the alert was triggered by an unusually high volume of delete operations on the blobs in storage1, the alert details would provide information about which specific blobs were deleted.

Azure Storage Analytics logs provide detailed information about successful and failed requests to a storage service, including delete operations. However, in this specific scenario where you have received an alert from Microsoft Defender for Cloud about an unusually high volume of delete operations on the blobs in storage1, the alert details would be the best place to look for information about which blobs were deleted.

upvoted 3 times

Holii 1 year, 8 months ago

Security alert -> View Full Details -> Alert details does NOT contain a list of affected blob resources.
In order to see affected blob containers affected by a deletion event, the answer would be D
Expand the Related Entities -> Blob container -> Provides a list of all blob entities affected by the alert.

Since this is specifically talking about an alert, and the entities affected by the deletion of the alert, I think it would honestly be best to do it from inside the 'Related Entities -> blob containers' page rather than generating a view of deleted blob incidents.

You don't know whether a blob container was deleted that was not part of that alert if you're searching the analytics logs or storage account logs.

For the fact that it is specifically targeting blobs touching this alert, im choosing D.

upvoted 5 times

Question #35 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to filter the security alerts view to show the following alerts:

• Unusual user accessed a key vault
• Log on from an unusual location
• Impossible travel activity

Which severity should you use?

A. Informational

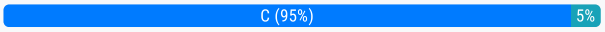
B. Low

C. Medium

D. High

Suggested Answer: *C*

Community vote distribution



ACSC Highly Voted 1 year, 11 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview#how-are-alerts-classified

upvoted 11 times

arturro007 Most Recent 3 weeks, 4 days ago

Selected Answer: C

Access from a suspicious IP address to a key vault
Severity: Medium

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-azure-key-vault

upvoted 1 times

talosDevbot 3 months ago

Selected Answer: C

High - high probability that your resource is compromised
Medium - probably a suspicious activity might indicate that a resource is compromised
Low - might be a benign positive or blocked attack
Informational

All of these alerts are for suspicious activity

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview#how-are-alerts-classified

upvoted 1 times

g_man_rap 4 months, 1 week ago

Selected Answer: D

Clear is D. Why do you put links which are not related with the options?

upvoted 1 times

aks_exam 8 months, 3 weeks ago

outdated.
The relationship between activity and security alerts is not publicly available at this time.

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct

upvoted 1 times

mfalkjunk 1 year, 5 months ago

Selected Answer: C

Better site:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference

Gives details for all alerts and their threat levels.

upvoted 3 times

Zak366 1 year, 10 months ago

Selected Answer: C

Medium is correct
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference#alerts-fusion

upvoted 4 times

jayek 1 year, 11 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference#alerts-fusion

upvoted 4 times

Question #36 *Topic 2*

You plan to review Microsoft Defender for Cloud alerts by using a third-party security information and event management (SIEM) solution.

You need to locate alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic.

Which JSON key should you search?

A. Description

B. Intent

C. ExtendedProperies

D. Entities

Suggested Answer: *A*

Community vote distribution

B (97%)

VictorLiu Highly Voted 1 year, 11 months ago

Selected Answer: B

B. Intent

https://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?tabs=HTTP#intent

upvoted 19 times

Fcnet 1 year, 11 months ago

Intent

PrivilegeEscalation string

Privilege escalation is the result of actions that allow an adversary to obtain a higher level of permissions on a system or network.

upvoted 4 times

g_man_rap Most Recent 4 months, 3 weeks ago

Correct Answer: C. ExtendedProperties

Explanation:

The ExtendedProperties JSON key is designed to hold additional and structured information about the alert. In the context of Microsoft Defender for Cloud and other security platforms, this often includes detailed metadata such as MITRE ATT&CK tactic mappings. Therefore, searching the ExtendedProperties key will likely yield results that specifically indicate the Privilege Escalation tactic.

upvoted 1 times

falkendarkness 10 months, 3 weeks ago

Option B ("Intent") is not typically used to directly represent the MITRE ATT&CK tactics or techniques associated with an alert in Microsoft Defender for Cloud.

The "Intent" field, if present in the alert data, might provide information about the suspected purpose or objective of the observed activity. However, it does not specifically indicate the MITRE ATT&CK tactic or technique being employed.

On the other hand, the "ExtendedProperties" field often contains additional contextual information about the alert, including any associated MITRE ATT&CK tactics and techniques. This field is more likely to contain the specific details needed to identify alerts related to the Privilege Escalation tactic.

Therefore, in the context of locating alerts related to the Privilege Escalation MITRE ATT&CK tactic, the "ExtendedProperties" field (Option C) is more relevant to search within the JSON data.

upvoted 1 times

Durden871 8 months, 4 weeks ago

I used ChatGPT as well and got the same answer. Every other dump seems to indicate intent is the answer. No one who says ExtendedProperties has given a link as to why this is the case. I normally trust ChatGPT, but this case I don't. Properties.Intent: The kill chain

related intent behind the alert. For list of supported values, and explanations of Azure Security Center's supported kill chain intents.
https://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?view=rest-defenderforcloud-2022-01-01&tabs=HTTP#intent
upvoted 1 times

neo73 11 months ago
To locate Privilege Escalation MITRE ATT&CK tactic alerts in Microsoft Defender for Cloud, search the Description JSON key.

To locate alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic in Microsoft Defender for Cloud, you should search the Description JSON key. The Description key provides a detailed explanation or summary of the alert, and it may include information about the observed behavior or activity related to privilege escalation.

By searching the Description key, you can filter and identify alerts that specifically mention or describe privilege escalation techniques. This can help in effectively reviewing and addressing such alerts using the third-party security information and event management (SIEM) solution.
upvoted 1 times

chepeerick 1 year, 2 months ago
B intent
upvoted 1 times

NICKTON81 1 year, 3 months ago
Selected Answer: B
B. Intent
https://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?tabs=HTTP#intent:~:text=%22High%22%2C-,%22intent%22%3A%20%22Execution%22%2C,-%22startTimeUtc%22%3A
upvoted 1 times

mali1969 1 year, 4 months ago
Selected Answer: D
The JSON key that you should search for alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic is Entities.

This key contains information about the entities involved in the alert, such as users, devices, files, etc. The value of this key can include a MITRETechniques property that lists the MITRE ATT&CK techniques associated with the alert.
upvoted 1 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 4 times

srajal 1 year, 5 months ago
Which is correct answer
upvoted 2 times

exmITQS 1 year, 10 months ago
Selected Answer: B
The "Intent" key is part of the JSON format used by Microsoft Defender for Cloud to transmit security alert data to third-party security information and event management (SIEM) solutions. The "Intent" key provides information on the type of attack or tactic that the alert is related to, and can be used to identify alerts that are specifically related to the Privilege Escalation tactic.
upvoted 3 times

PhoenixSlasher 1 year, 10 months ago
Selected Answer: B
B. Intent
Personally find the extendedProperties to contain the data as well but Intent clearly defines Privilege Escalation without digging around in extended properties.
upvoted 3 times

[Removed] 1 year, 11 months ago
Selected Answer: B
B - https://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?tabs=HTTP#intent:~:text=%22High%22%2C-,%22intent%22%3A%20%22Execution%22%2C,-%22startTimeUtc%22%3A
upvoted 4 times

jayek 1 year, 11 months ago

https://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?tabs=HTTP#intent:~:text=%22High%22%2C-,%22intent%22%3A%20%22Execution%22%2C,-%22startTimeUtc%22%3A

upvoted 2 times

WRITER00347 1 year, 11 months ago

The JSON key you should search for to locate alerts that indicate the use of the Privilege Escalation MITRE ATT&CK tactic is extendedProperties.

The extendedProperties key in the JSON structure of an alert contains the MITRE ATT&CK information for the alert, such as the tactics and techniques used by the attacker. The key contains the tactic name in the MITRE ATT&CK framework, such as "Privilege Escalation", "Initial Access", "Execution" and so on.

You can use the extendedProperties key to filter and search for alerts that are related to the Privilege Escalation tactic in your third-party SIEM solution.

It's also important to note that, the other options A,B,C are not related to the MITRE ATT&CK information and are used for different purposes.

upvoted 1 times

WRITER00347 1 year, 11 months ago

so C. ExtendedProperties

upvoted 2 times

Fcnet 1 year, 11 months ago

https://learn.microsoft.com/en-us/rest/api/defenderforcloud/alerts/list?tabs=HTTP#intent

upvoted 3 times

Fcnet 1 year, 11 months ago

this is for the intent answer wich is the right answer

upvoted 3 times

JoshJosh 1 year, 11 months ago

Entities

upvoted 1 times

Question #37 *Topic 2*

DRAG DROP
-

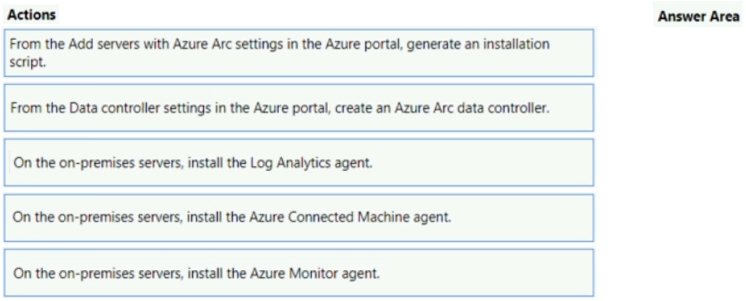
You have 50 on-premises servers.

You have an Azure subscription that uses Microsoft Defender for Cloud. The Defender for Cloud deployment has Microsoft Defender for Servers and automatic provisioning enabled.

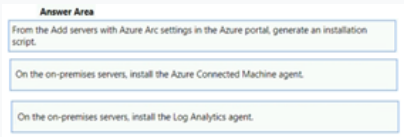
You need to configure Defender for Cloud to support the on-premises servers. The solution must meet the following requirements:

• Provide threat and vulnerability management.
• Support data collection rules.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Suggested Answer:



herta Highly Voted 1 year, 11 months ago
for me it is 1-4-5

from the portal generate the script
install the agent on the on premise server with the script
install the azure monitor agent (for the data collection)

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection
https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm
upvoted 24 times

Tuitor01 3 weeks, 6 days ago
Log Analytics Agent is Deprecated now, use AMA agent when possible. 1 extra vote for me.
upvoted 1 times

AJ2021 Highly Voted 1 year, 10 months ago
Question in Exam today
upvoted 17 times

e072f83 Most Recent 7 months, 1 week ago
first create the script for installation, (1)
then install the azure arc client, for basic threat and vulnerability mgmt. (5)
third install the monitoring agent to collect the data (3)

https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent

upvoted 2 times

Gurulee 12 months ago

If you are currently using the Log Analytics agent, it is recommended that you migrate to the Azure Monitor agent before the Log Analytics agent is retired on August 31, 2024

upvoted 3 times

chepeerick 1 year, 2 months ago

1 4 and 5

upvoted 1 times

itsadel 1 year, 5 months ago

If the solution must meet the support data collection rules, then you should use the Azure Monitor Agent. So that I choose 1-4-5

upvoted 2 times

cyber_rip 1 year, 7 months ago

it should be in this order 1-4-5

upvoted 2 times

pewpewvx 1 year, 8 months ago

For Data Collection Rules (DCR) you need to use the AMA Agent, and not the MMA Agent.
For this reason. 1,4,5 are correct.

upvoted 2 times

GeorgeEC 1 year, 8 months ago

The answer is correct
https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines?pivots=azure-arc
You need Log analytics to analyze the server

upvoted 2 times

AJ2021 1 year, 11 months ago

Agree, the updated answer should be 1, 4, 5

upvoted 5 times

RodrigoLima 1 year, 11 months ago

I guess this is outdated stuff. But Log Analytics option is out, since we need to support DCRs.
I would say, 1, 4, 5. By this exact order

upvoted 9 times

JoshJosh 1 year, 11 months ago

4,1,2 the steps

upvoted 2 times

HOTSPOT
-

You have an Azure subscription that uses Microsoft Defender for Cloud and contains an Azure logic app named app1.

You need to ensure that app1 launches when a specific Defender for Cloud security alert is generated.
How should you complete the Azure Resource Manager (ARM) template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
"resources": [
    {
      "type": [                                          ▼
                Microsoft.Automation/automationAccounts",
                "Microsoft.Logic/workflows"',
                "Microsoft.Security/automations",
      "apiVersion": "2019-01-01-preview",
      "name": "[parameters('name')]",
      "location": "[resourceGroup().location]",
      "properties": {
        "description": "[format(variables('description'),'{0}', parameters('subscriptionId'))]",
        "isEnabled": true,
        "actions": [
          { "actionType": "LogicApp",
            "logicAppResourceId": "[resourceId('Microsoft.Logic/workflows', parameters('app1'))]",
            "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),parameters('resourceGroupName'),
                    'Microsoft.Logic/workflows/ [          ▼
                                                  actions
                                                  contents
                                                  triggers
                    parameters('app1'),'manual'), '2019-05-01').value]"
          }
        ],
```

Suggested Answer:

AJ2021 Highly Voted 11 months ago

Question in Exam today

upvoted 12 times

herta Highly Voted 11 months, 1 week ago

answer is correct

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-automation-alert?tabs=CLI

upvoted 10 times

chepeerick Most Recent 2 months, 1 week ago

Correct

upvoted 1 times

JoeP1 5 months, 1 week ago

This appears to be the same script as Topic 2 Question 14. The dropdowns are for different parts of the same lines in the code.

upvoted 4 times

Houssemonline 11 months ago

CORRECT ANSWER

upvoted 4 times

jayek 11 months, 1 week ago

https://github.com/MicrosoftDocs/azure-docs/blob/main/articles/defender-for-cloud/quickstart-automation-alert.md#:~:text=If%20your%20environment%20meets%20the%20prerequisites%20and%20you%27re%20familiar%20with%20using%20ARM%20templates

upvoted 2 times

Question #39 *Topic 2*

HOTSPOT
-

You have an Azure subscription that has Microsoft Defender for Cloud enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Defender for Cloud.

You need to test LA1 in Defender for Cloud.

What should you do? To answer, select the appropriate options in the answer area.

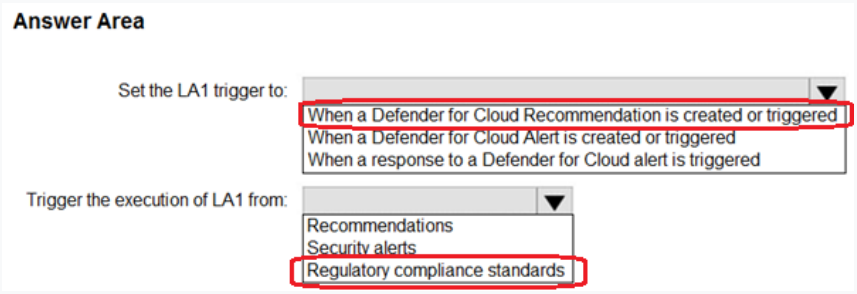
NOTE: Each correct selection is worth one point.

Answer Area

Set the LA1 trigger to:
- When a Defender for Cloud Recommendation is created or triggered
- When a Defender for Cloud Alert is created or triggered
- When a response to a Defender for Cloud alert is triggered

Trigger the execution of LA1 from:
- Recommendations
- Security alerts
- Regulatory compliance standards

Suggested Answer:



Holii Highly Voted 1 year, 8 months ago

When a Defender for Cloud Recommendation is created or triggered
and
Security alerts

Regulatory Compliance Standards is based on pre-defined compliance standards and, while they can provide remediation to security risks, I think Security alerts better answers the question and offers the ability to customize.
upvoted 20 times

xRiot007 4 weeks, 1 day ago

You should trigger the execution of the LA from Recommendations.
upvoted 1 times

tirajvid Highly Voted 1 year, 6 months ago

Question says " You plan to use LA1 to automatically remediate security risks detected in Defender for Cloud"
Security risks are not security alerts nor policy non compliance issues.

Based on that, the correct second answer should be "Recommendations"
https://azurecloudai.blog/2021/08/10/regulatory-compliance-in-azure-security-center-workflow-automation-reaches-ga/
upvoted 18 times

user636 Most Recent 4 months, 1 week ago

The answers are:
Set Trigger to when a defender for Cloud recommendation is created or triggered

Trigger the execution of LA1 from Recommendations.

If you set the trigger of a logic app of a particular type, then you can only trigger it from that type.
For e.g. if the trigger is alert , then you can tigger the logic app from a alert & if the trigger is recommendation, then you can trigger it from a recommendation.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/review-security-recommendations#explore-a-recommendation
upvoted 4 times

HAjouz 3 weeks, 1 day ago

100%Set the LA1 trigger to:

When a Defender for Cloud Recommendation is created or triggered
By triggering LA1 based on recommendations, you can proactively address potential security issues before they escalate into actual alerts.

Trigger the execution of LA1 from:

Recommendations
You can manually trigger LA1 from the Recommendations section in Defender for Cloud to test its remediation capabilities.

Remember to configure LA1 to take appropriate actions based on the specific recommendations, such as applying security patches, hardening configurations, or disabling vulnerable services.
upvoted 1 times

user636 4 months, 1 week ago

The answer is:
Set trigger to Cloud recommendation is created or triggered & Trigger the execution from Recommendations.

You can trigger a logic app from recommendations in MDC. Click a recommendation & then navigate to "Take action" option.
Also, why would you use "security alert" as a trigger execution if the logic app is configured with a trigger "when a recommendation is created/triggered".
The logic app will be executed via a same trigger that it is configured as.
upvoted 1 times

Sneekygeek 8 months, 3 weeks ago

Seems to be another example of poorly worded question making this about test taking ability and not competence with Microsoft products.

I think the phrasing 'security risks' as opposed to 'security incident' means we would be talking about recommendations and not alerts. The recommendations exist for configurations deemed risky (similar to secure score), whereas an alert would be doing something in response to activity which triggered the alert, which I would consider an incident, not a risk.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference
upvoted 1 times

Ramye 10 months, 1 week ago

Based on the specific ask on the question: "You plan to use LA1 to automatically remediate security risks detected in Defender for Cloud"
It clearly says automatically remediate the risk -that means don't have to rely on recommendations, so the 2nd box is clearly Security alerts.
upvoted 1 times

Gurulee 1 year ago

Recommendations trigger.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation#supported-triggers
upvoted 1 times

danlo 1 year, 1 month ago

Remediate security risks = recommendations
Alerts would be alerts as is not mentioned
https://learn.microsoft.com/en-us/azure/well-architected/security/monitor-remediate

upvoted 1 times

chepeerick 1 year, 2 months ago

check this

upvoted 1 times

Anil0512 1 year, 3 months ago

Seems nobody is 100% sure?

upvoted 2 times

Fez786 1 year, 3 months ago

its

Cloud Recommendation is created or triggered

and

Security alerts

upvoted 4 times

donathon 1 year, 4 months ago

My thoughts are this related to risks not actual inccidents. Hence it should be Recommendations for both instead of alerts.

upvoted 2 times

Ramye 10 months, 3 weeks ago

But, does not recommendations are generated based on alerts/incidents sometimes?

upvoted 1 times

AK4U_111 1 year, 6 months ago

be careful not to mistake with Topic 2 - Question Set 2 Question#3

You have an Azure subscription that has Azure Defender enabled for all supported resource types.
You create an Azure logic app named LA1.
You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.
You need to test LA1 in Security Center.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

upvoted 2 times

Ramye 10 months, 4 weeks ago

Azure Defender and Azure Security center together now is Defender for Cloud, so this question is now updated with the updated name.

upvoted 1 times

MrAce 1 year, 7 months ago

The question can be interpreted in multiple ways, but I think that the answer should be:

When a Defender for Cloud Alert is created or triggered
Security Alerts

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

upvoted 4 times

JoeP1 1 year, 5 months ago

According to that link: "To manually run a logic app, open an alert, or a recommendation and select Trigger logic app"
So the Logic App can be manually triggered in this case from the Recommendation.

The answers should be:
When a Defender for Cloud Recommendation is created or triggered
Recommendations

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

upvoted 7 times

Question #40 *Topic 2*

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?

A. Run the Log Analytics Troubleshooting Tool.

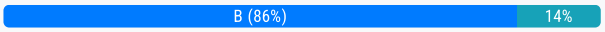
B. Copy and executable and rename the file as ASC_AlertTest_662jfi039N.exe.

C. Modify the settings of the Microsoft Monitoring Agent.

D. Run the MMASetup executable and specify the –foo argument.

Suggested Answer: *B*

Community vote distribution



exmITQS Highly Voted 10 months, 2 weeks ago

Selected Answer: B

you can use the built-in ASC AlertTest tool.

Here's what you should do first:

Connect to the virtual machine.

Open a web browser and navigate to the Microsoft Defender Security Center portal.

Click on the "Settings" tab in the left-hand menu.

Click on the "Advanced features" link to expand the advanced features section.

In the "Advanced features" section, click on the "Download" link next to the "ASC AlertTest" tool.

Download and save the ASC AlertTest tool to the virtual machine.

Double-click the downloaded ASC AlertTest executable to run it.

Follow the on-screen prompts to generate an alert in Microsoft Defender for Cloud. You may need to specify the IP address or hostname of the virtual machine, as well as a description and category for the simulated attack.

upvoted 5 times

chepeerick Most Recent 2 months, 1 week ago

Correct

upvoted 2 times

kazaki 5 months ago

All answers are wrong

Correct is
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden $ErrorActionPreference = 'silentlycontinue';(New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-MDATP-test\\invoice.exe');Start-Process 'C:\\test-MDATP-test\\invoice.exe'

upvoted 3 times

kabooze 2 months ago

they're all wrong or the question is wrong. I see people refer to "ASC_AlertTest_662jfi039N" but this is only for K8s. Not for windows VM's...
upvoted 2 times

marv__ 9 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation
upvoted 2 times

Comicbookman 10 months, 2 weeks ago

Selected Answer: B

Simulate alerts on your Azure VMs (Windows)
After the Log Analytics agent is installed on your machine, follow these steps from the computer where you want to be the attacked resource of the alert:

Copy an executable (for example calc.exe) to the computer's desktop, or another directory of your convenience, and ----------> rename it as ASC_AlertTest_662jfi039N.exe. <----------
Open the command prompt and execute this file with an argument (just a fake argument name), such as ASC_AlertTest_662jfi039N.exe -foo
Wait for 5 to 10 minutes and open Defender for Cloud Alerts. An alert should appear.
upvoted 3 times

watoz1851 10 months, 2 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alert-validation#simulate-alerts-on-your-azure-vms-windows-
upvoted 2 times

m_saeed 10 months, 2 weeks ago

Selected Answer: D

chat GPT explanation,
To simulate an attack on the virtual machine that will generate an alert, you should first run the MMASetup executable and specify the –foo argument. This will simulate an attack and generate an alert in Defender for Cloud. You can then view the alert in the Azure portal to verify that the attack was successful.
upvoted 2 times

Holii 8 months, 2 weeks ago

You already have Log Analytics installed...why do you need to run MMASetup executable again? This is B.
upvoted 3 times

Question #41 *Topic 2*

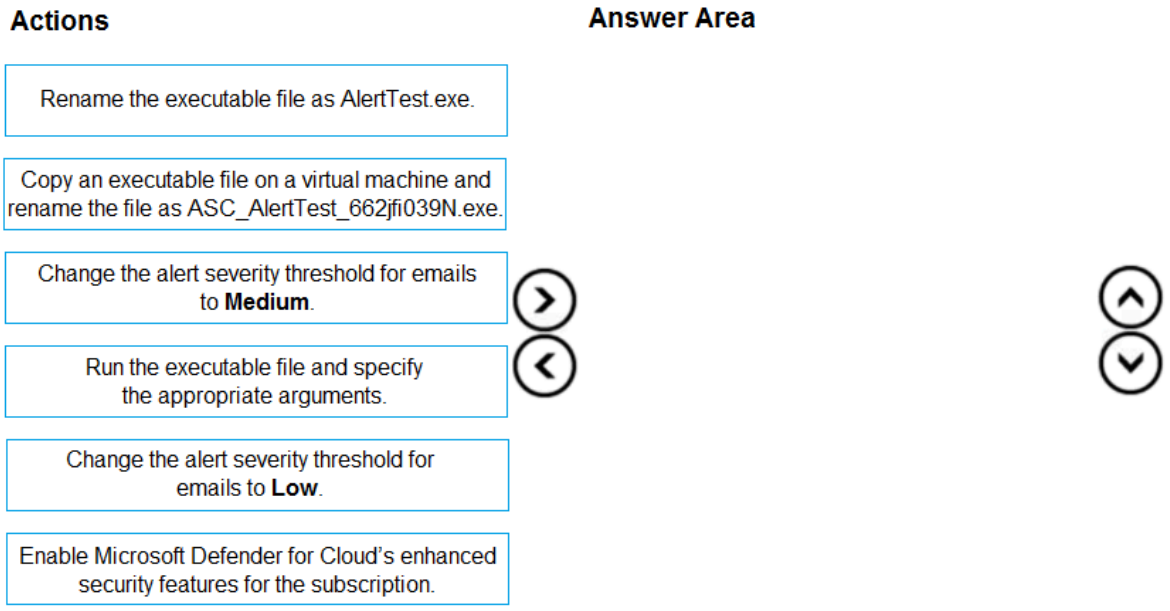
DRAG DROP
-

You create a new Azure subscription and start collecting logs for Azure Monitor.

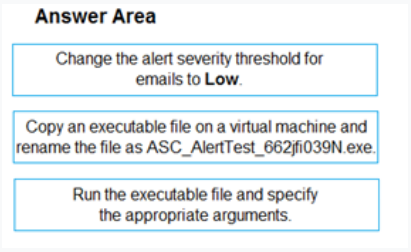
You need to validate that Microsoft Defender for Cloud will trigger an alert when a malicious file is present on an Azure virtual machine running Windows Server.

Which three actions should you perform in a sequence? To answer, move the appropriate actions from the list of action to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.



Suggested Answer:



antoniokt Highly Voted 10 months, 1 week ago
Correct is 6-2-4
upvoted 31 times

wsrudmen Highly Voted 10 months, 1 week ago
1. Enable Microsoft Defender

Logs is already collected for Azure Monitor, then events will be managed by Defender.
We can then proceed with our test.

2. Copy an executable file...
3. Run the executable
upvoted 12 times

chepeerick Most Recent 2 months, 1 week ago
check this
upvoted 1 times

jamclash 3 months, 2 weeks ago

in exam 9/20/23

upvoted 3 times

donathon 4 months, 4 weeks ago

624 for me

upvoted 2 times

Nivos23 6 months, 1 week ago

6 2 4

This is the answer in my opinion

upvoted 4 times

cyber_rip 7 months, 3 weeks ago

We can then proceed with our test.

1-Enable Microsoft Defender

2. Copy an executable file...

3. Run the executable

upvoted 4 times

Question #42 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common.

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

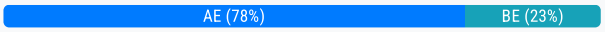
C. From the Azure portal, create an Azure Event Grid subscription.

D. From the workspace created by Defender for Cloud, set the data collection level to All Events.

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Suggested Answer: *AE*

Community vote distribution



teouba Highly Voted 1 year, 8 months ago

Selected Answer: AE

Answer is correct.
Microsoft Endpoint Manager (Intune) has nothing to do with configuring Defender for Cloud to collect data from VMs
Plus it would need a lot of administrative effort also to make relevant Intune configurations.

All you need to do is enable auto-provisioning from Defender for Cloud. There you ll be asked if you want to store security events and in what level (none, minimal, common, all).
Since there are only 2 options provided here (common & all) we go with the least effort so A -> common

You can check the below video at 04:14
https://www.youtube.com/watch?v=Ufk65R7UJCc
upvoted 20 times

kabooze 1 year, 2 months ago

You go for "common" for the least costs, not the effort :) (being pedantic here, i know)
upvoted 3 times

Ramye 10 months, 4 weeks ago

Note: Auto-Provisioning page has been renamed to Settings & monitoring in Microsoft Defender for Cloud
Microsoft Defender for Cloud --> Environment settings --> Azure Subscription --> Defender plans --> Settings & monitoring
upvoted 2 times

exmITQS Highly Voted 1 year, 10 months ago

Selected Answer: BE

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment: This will automatically enroll all Windows devices, including the virtual machines in your subscription, in Microsoft Endpoint Manager, which will then allow Defender for Cloud to collect event data from these devices. To enable automatic enrollment, you can follow the steps in the Microsoft documentation.

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines: This will automatically configure the virtual machines to send event data to Defender for Cloud without the need for manual configuration or agent installation. To enable automatic provisioning, you can follow the steps in the Azure Defender documentation.
upvoted 7 times

Holii 1 year, 8 months ago

Intune is for Device Management for onboarding company/BYOD devices and not relevant here.
Goal is the least administrative effort possible with least cost. We would at least need a Data Connector to fulfill lower costs.

This would be AE.
upvoted 7 times

aks_exam Most Recent 8 months, 2 weeks ago
on exam 2024/April
upvoted 1 times

kazaki 10 months, 3 weeks ago
Selected Answer: AE
Simple A and E
Don't even think
upvoted 1 times

a95f6f1 1 year, 1 month ago
AE for me too!
upvoted 1 times

im20batman 1 year, 1 month ago
Selected Answer: BE
not correct
BE
upvoted 1 times

Hawklx 6 months, 2 weeks ago
Microsoft Endpoint Manager is not Defender for Cloud
upvoted 1 times

chepeerick 1 year, 2 months ago
check this
upvoted 1 times

donathon 1 year, 4 months ago
Selected Answer: AE
AE for me
upvoted 1 times

EricShon 1 year, 4 months ago
Selected Answer: AE
E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Automatic provisioning allows Microsoft Defender for Cloud to automatically deploy the Log Analytics agent to Azure VMs, which will then forward the event data to a Log Analytics workspace. This reduces the administrative effort as you won't have to manually install and configure the agent on each VM.

A. From the workspace created by Defender for Cloud, set the data collection level to Common.

Setting the data collection level to "Common" minimizes costs because it means only essential security-related events will be collected. The "All Events" setting (Option D) would result in higher costs because more data would be stored in the workspace, but it might not be necessary for security monitoring.
upvoted 2 times

tatendazw 1 year, 6 months ago
In MS Defnder for Cloud environment settings Defender plans there you enabled auto provision with LAA/MMA turned on and configure Security events storage to Common
https://learn.microsoft.com/en-us/azure/defender-for-cloud/auto-deploy-azure-monitoring-agent#deploy-the-azure-monitor-agent-with-defender-for-cloud
upvoted 1 times

tatendazw 1 year, 6 months ago
LAA/MMA = Log Analytics agent/Azure Monitor agent
upvoted 1 times

D_PaW 1 year, 7 months ago

Selected Answer: AE

Endpoint Manager is for "Endpoints" only ie. Windows 10/11, Android, iOS and Mac. NOT Server or Defender for Cloud related.

So must be AE

https://learn.microsoft.com/en-us/azure/defender-for-cloud/working-with-log-analytics-agent#what-event-types-are-stored-for-common-and-minimal

upvoted 2 times

Elpintintun 1 year, 7 months ago

AE

B is not possible because Microsot Endpoint Manager doesnt enroll servers and it says:

contains 100 virtual machines that run windows server.

upvoted 3 times

ccurio 1 year, 6 months ago

https://techcommunity.microsoft.com/t5/intune-customer-success/windows-server-devices-now-recognized-as-a-new-os-in-intune/ba-p/3767773

upvoted 1 times

default_wizard 1 year, 8 months ago

Selected Answer: AE

Agree, A/E are correct

upvoted 4 times

haskelatchi 1 year, 8 months ago

Selected Answer: AE

The answer is not B, enrolling windows devices has no direct impact on configuring defender for cloud to collect event data from virtual machines

upvoted 3 times

evilprime 1 year, 9 months ago

seems correct to me, A and E.

upvoted 1 times

antoniokt 1 year, 10 months ago

Selected Answer: BE

Correct is BE

upvoted 1 times

Question #43 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a user named User1.

You need to ensure that User1 can modify Microsoft Defender for Cloud security policies. The solution must use the principle of least privilege.

Which role should you assign to User1?

A. Security operator

B. Security Admin

C. Owner

D. Contributor

Suggested Answer: *B*

Community vote distribution

B (100%)

TheHuman_ Highly Voted 6 months, 4 weeks ago

Selected Answer: B

Security Admin has less privileges than the Contributor or Owner roles, but is still able to modify security policies.

See: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-admin

upvoted 6 times

smosmo Most Recent 3 weeks, 2 days ago

Selected Answer: B

Only Security Admin and Owner of the Subsc. can modify policies. SecAdmin has least priv.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
Security Admin: A user that belongs to this role has the same access as the Security Reader and can also update the security policy, and dismiss alerts and recommendations.

upvoted 1 times

chepeerick 8 months, 2 weeks ago

Correct B

upvoted 1 times

Doinitza 11 months, 1 week ago

Question from ESI:
You have an Azure subscription that uses Microsoft Defender for Cloud.
You create a user named Admin1.
You need to ensure that Admin1 can create and assign security policies in Defender for Cloud. The solution must follow the principle of least privilege.
Which role should you assign to Admin1?

Right Answer: Contributor in the Azure subscription
Wrong Answer: Security Admin in the Azure subscription

Comment from MS: Defender for Cloud uses Azure role-based access control (RBAC), which provides built-in roles that can be assigned to users, groups, and services in Azure. Azure AD roles do not have permissions in Defender for Cloud.
Only Contributor and Owner roles at the Azure subscription level have sufficient permissions to create and assign security policies in Defender for Cloud. Contributor has less permissions than Owner, and because of that you should assign Admin1 the Contributor role.

***Maybe the Contributor is the right answer.

upvoted 3 times

Ramye 4 months, 3 weeks ago

Wrong ..

Contributor Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.

Security Admin View and update permissions for Microsoft Defender for Cloud. Same permissions as the Security Reader role and can also update the security policy and dismiss alerts and recommendations.

Source: https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#security-admin
upvoted 1 times

cyber_rip 1 year, 1 month ago
B-Security Admin
upvoted 1 times

antoniokt 1 year, 4 months ago
Selected Answer: B
Security reader: Has rights to view Defender for Cloud items such as recommendations, alerts, policy, and health. Can't make changes.
Security admin: Has the same view rights as security reader. Can also update the security policy and dismiss alerts.
upvoted 4 times

watoz1851 1 year, 4 months ago
Selected Answer: B
https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy#who-can-edit-security-policies
upvoted 3 times

Question #44 *Topic 2*

You have an Azure subscription that contains a user named User1.

User1 is assigned an Azure Active Directory Premium Plan 2 license.

You need to identify whether the identity of User1 was compromised during the last 90 days.

What should you use?

A. the risk detections report

B. the risky users report

C. Identity Secure Score recommendations

D. the risky sign-ins report

Suggested Answer: *B*

Community vote distribution

Marchiano Highly Voted 1 year, 5 months ago

Selected Answer: B

On the Risky Users page you will have to select an account and then select the Risk History tab. This will show you if the entity was compromised or not for the past 90 days.

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk#risky-users

This question very confusing...Risky Users and Risk Detections are the only ones that provide data for the past 90 days, but both provide info about the Risk State....like Confirmed Compromised...

upvoted 18 times

mandragon Highly Voted 1 year, 10 months ago

Selected Answer: A

Just tested it and correct answer is A - the risk detections report. D only shows one month of risky sign ins. From risk detections you select from risk state the checkbox on confirm compromised and detection time last 90 days.

upvoted 8 times

choukou Most Recent 1 month, 1 week ago

A - the risk detections report -90 days

upvoted 1 times

Studytime2023 4 months, 3 weeks ago

Selected Answer: B

Just tested this with the tenant of the MSP I work for. It shows risky user accounts right back to a couple of years ago.
I went to portal.azure.com
Then "Entra ID"
Then "Security"
Then "Identity protection"
Then I see "Report" and under that I see "Risky users".

upvoted 3 times

Studytime2023 4 months, 3 weeks ago

I also just went to entra.microsoft.com and under "Protection" then "Risky activities" I also found the same "Risky users" report also showing back a couple of years.

upvoted 1 times

Vokuhila 7 months ago

B

This report lists all users whose accounts are currently or were considered at risk of compromise. It includes a Risk history tab that shows all the events that have led to a user risk change in the last 90 days

https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk
upvoted 3 times

Sneekygeek 8 months, 3 weeks ago

Selected Answer: B

The Risky users report doesn't have any time limit; I have detections in my lab from as far back as 2018. From this page you can click on a user and then get to risk detections associated with them. Risk detections report is applicable here but I would start with the Risky Users report.
upvoted 3 times

Durden871 6 months, 3 weeks ago

This is an underrated comment. I tricked myself into thinking risky users showed history of users at risk over the past 90 days, but now that you mention it I distinctively remember seeing risky users going back to 2021. Risky users are entirely static and will stay there until you remove them. You also can not filter risky users in any way, shape or form.
upvoted 1 times

d16cba9 2 months, 2 weeks ago

Not true. You can apply filters on Risky users as well. Look at the link: https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-protection-investigate-risk?pivots=b2c-user-flow
There's an option says you can 'Apply filters'
upvoted 1 times

cdgdhj 2 months, 2 weeks ago

What's the correct answer?
upvoted 1 times

luisM14 9 months ago

Selected Answer: A

Risk Detection is correct.
Tested. it's the only that gives information from past 90 days
upvoted 2 times

Durden871 9 months, 2 weeks ago

ChatGPT is of no help:
Review Risky Users:

Check the list of risky users to see if User1 is listed. Risky users are flagged based on suspicious activities or behaviors that indicate a potential compromise.
Look for indicators such as multiple failed sign-in attempts, unusual sign-in locations, or other anomalous activities associated with User1.
Check Risk Detection Reports:

Review risk detection reports to see if any security events or activities related to User1 have been flagged as risky in the last 90 days.
Look for risk detections such as unusual sign-ins, impossible travel, or suspicious activity patterns that may indicate a compromised identity.
upvoted 1 times

Durden871 9 months, 2 weeks ago

Check Risk Detection Reports:

Review risk detection reports to see if any security events or activities related to User1 have been flagged as risky in the last 90 days.
Look for risk detections such as unusual sign-ins, impossible travel, or suspicious activity patterns that may indicate a compromised identity.
upvoted 1 times

Durden871 9 months, 2 weeks ago

Investigate Sign-In Logs:

Review sign-in logs to identify any suspicious sign-in activities associated with User1 in the last 90 days.
Look for unusual sign-in locations, multiple failed sign-in attempts, or sign-in activities outside of User1's normal behavior patterns.
upvoted 1 times

Durden871 9 months, 2 weeks ago

Oh, nvm. ChatGPT seems to agree it's A, not B.
upvoted 1 times

4rk4n4 10 months, 1 week ago

Selected Answer: A

A can filter to 90 days.

upvoted 1 times

shimon893 10 months, 1 week ago

Selected Answer: A

https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-investigate-risk#risky-users

upvoted 1 times

DChilds 8 months, 3 weeks ago

This document says "The risky users report lists all users whose accounts are currently or were considered at risk of compromise." and "The Risk history tab also shows all the events that have led to a user risk change in the last 90 days."

This makes the choice to be B.

upvoted 1 times

mmmyo 10 months, 3 weeks ago

Selected Answer: B

With the information provided by the risky users report, administrators can find:

Which users are at risk, have had risk remediated, or have had risk dismissed?
Details about detections
History of all risky sign-ins
Risk history
Administrators can then choose to take action on these events. Administrators can choose to:
Reset the user password
Confirm user compromise
Dismiss user risk
Block user from signing in
Investigate further using Microsoft Defender for Identity

upvoted 2 times

Ramye 10 months, 4 weeks ago

Selected Answer: A

A. the risk detections report ---- > can filter to 90 days
B. the risky users report Most Voted ---- > there is no filter for days / period
C. Identity Secure Score recommendations ---- > Does not apply
D. the risky sign-ins report ------> Can filter only for 1 Month max

upvoted 6 times

MentalG 11 months, 1 week ago

D. the risky sign-ins report. This report shows the sign-ins that have been flagged as risky by the identity protection system, and it stores the data for 90 days for Microsoft Entra ID P2 licenses1. You can use this report to investigate the risk level, risk type, and risk detail of each sign-in, and take actions to remediate the risk.

upvoted 1 times

Pradeep064 11 months, 2 weeks ago

It's a risky detection report has 90 days of detection period

Answer: A

upvoted 1 times

CollabGuy 11 months, 2 weeks ago

Selected Answer: A

I've tested in my lab
The only option that shows 90days and risk (At Risk, Confirmed Compromised, etc) is the Risk detections page.
Risky sign-ins only allows until 30 days
Risky users you can't filter date

upvoted 1 times

estyj 11 months, 3 weeks ago

Would have to go with A: risk detection report shows last 90 days, while Risky users report only shows last 30 days.

upvoted 1 times

Gurulee 12 months ago

The Risky users report in Microsoft Entra ID Protection provides a detailed history of all the events that have led to a user risk change in the last 90 days

upvoted 1 times

Question #45 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account that contains an Amazon Elastic Compute Cloud (EC2) instance named EC2-1.

You need to onboard EC2-1 to Defender for Cloud.

What should you install on EC2-1?

A. the Log Analytics agent

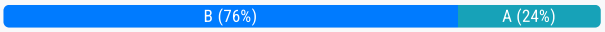
B. the Azure Connected Machine agent

C. the unified Microsoft Defender for Endpoint solution package

D. Microsoft Monitoring Agent

Suggested Answer: *A*

Community vote distribution



exmITQS Highly Voted 1 year, 10 months ago

Selected Answer: B

To onboard an Amazon Elastic Compute Cloud (EC2) instance to Microsoft Defender for Cloud, you should install the Azure Connected Machine agent on the instance. Therefore, the correct answer is B.

upvoted 11 times

user636 Most Recent 4 months, 1 week ago

Selected Answer: B

Azure Connected Machine agent is the first step to onboard any non-azure device to azure. The ACM agent can be used to deploy LA agent & other extensions.

Ref: https://learn.microsoft.com/en-us/training/modules/connect-non-azure-machines-to-azure-defender/3-connect-non-azure-machines
Ref: https://learn.microsoft.com/en-us/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

upvoted 2 times

wheeldj 8 months, 2 weeks ago

Just to throw more confusion into this question you can also connect non-Azure machines to Defender for Cloud directly using the Defender for Endpoint Agent which offers a single unified solution. Sounds like answer C to anyone else?

https://learn.microsoft.com/en-us/azure/defender-for-cloud/onboard-machines-with-defender-for-endpoint

D is definitely not correct, but I think there is an argument for A, B and C. I agree B is probably the most obvious answer, but who knows what's in the head of the Microsoft Examiners!!

upvoted 2 times

user636 4 months, 1 week ago

The question does not mention that you have the M365 Defender subscription/license. Don't assume stuff, this is an exam. C cannot be the answer to this question.

upvoted 2 times

KRAKE3N 8 months, 2 weeks ago

Selected Answer: A

(after installing Arc to onboard the vm from another cloud or on-premise) you should install the
Log Analytics agent(to be replaced with Azure Monitoring Agent this year, id recommend install AMA for obvious reason but to answer this question, the answer should be A)

upvoted 1 times

kazaki 10 months, 3 weeks ago

Outdated but B
upvoted 3 times

estyj 11 months, 3 weeks ago
To onboard AWS EC2 you would need the B. the Azure connected Machine agent.
upvoted 1 times

chepeerick 1 year, 2 months ago
Incorrect, option B, he Azure Connected Machine agent is used to connect and manage non-Azure machines (in this case, the EC2 instance) with Microsoft Defender for Cloud. It allows you to monitor and protect non-Azure resources in your environment.
upvoted 3 times

cris_exam 1 year, 3 months ago
Selected Answer: A
Well... if the question would have mentioned ARC anywhere, I would have totally agreed with B: Connected Machine agent
https://learn.microsoft.com/en-us/azure/azure-arc/servers/learn/quick-enable-hybrid-vm#install-the-agent-using-the-script

BUT... there is an option without ARC and as the question is neutral about the onboarding flavor, it makes the answer to be A: Log Analytics in my opinion.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-machines#connect-on-premises-machines-by-using-the-azure-portal
upvoted 4 times

kabooze 1 year, 2 months ago
they're deprecating LA agent though... It all depends on when these questions were made and with which solution in mind, but i'd say "B"
upvoted 3 times

Ramye 10 months, 4 weeks ago
LA Agent is still valid as Defender for Cloud and has the same name as of now - 9 Feb 2024), however, the Log Analytics agent (also known as MMA) is on a deprecation path and will be retired in Aug 2024.
upvoted 1 times

Gurulee 12 months ago
what he/she said ;-)
Azure Monitor agent to replace LA agent
upvoted 1 times

glauciasdiniz 1 year, 3 months ago
The answer corret is letter ---> C

Microsoft Defender for Endpoint integrates seamlessly with Microsoft Defender for Servers. You can onboard servers automatically, have servers monitored by Microsoft Defender for Cloud appear in Defender for Endpoint, and conduct detailed investigations as a Microsoft Defender for Cloud customer. For more information please go to Protect your endpoints with Defender for Cloud's integrated EDR solution: Microsoft Defender for Endpoint

https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-server-endpoints?view=o365-worldwide
upvoted 1 times

Stfnl 1 year, 4 months ago
Selected Answer: B
https://learn.microsoft.com/en-us/azure/azure-arc/servers/agent-overview

The Azure Connected Machine agent enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers.
upvoted 2 times

Marchiano 1 year, 5 months ago
Selected Answer: B
A & D are the same thing, C is out of context, while Azure Connected Machine agent = Azure Arc

"We recommend that you use the auto-provisioning process to install Azure Arc on all of your existing and future EC2 instances. To enable the Azure Arc auto-provisioning, you need Owner permission on the relevant Azure subscription."

Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws

upvoted 3 times

theplaceholder 1 year, 5 months ago

Selected Answer: B

ARC it up

upvoted 3 times

EM1234 1 year, 5 months ago

Selected Answer: B

You're going to need defender for servers which needs ARC. So choice B makes the most sense.

Also A and D are the same thing, and yes they are "legacy". The log analytics agent has been called OMS (the code came from it) and also the Microsoft Monitoring agent.

This is different than the Azure monitor agent, which has a whole new code base and features.

Link for choosing B: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws#defender-for-servers

Hope this helps.

upvoted 3 times

teouba 1 year, 8 months ago

Selected Answer: B

Answer is B

Please check the video below at 04:15

As you can see, server is already onboarded using Azure Arc agent and there is a recommendation to also install Log Analytics agent.

So FIRST you need to install Arc agent

https://www.youtube.com/watch?v=uogTZe6p7nc

upvoted 4 times

danb67 1 year, 2 months ago

Agree with B

upvoted 1 times

torvy 1 year, 8 months ago

Answer is D, you should install MMA on EC2

upvoted 1 times

haskelatchi 1 year, 8 months ago

The answer is D. Log analytics agent is legacy.

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-migration

upvoted 2 times

cosmin_mm 1 year, 9 months ago

Selected Answer: A

Forgot to vote :)

upvoted 2 times

Question #46 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains a resource group named RG1. RG1 contains 20 virtual machines that run Windows Server 2019.

You need to configure just-in-time (JIT) access for the virtual machines in RG1. The solution must meet the following requirements:

• Limit the maximum request time to two hours.
• Limit protocols access to Remote Desktop Protocol (RDP) only.
• Minimize administrative effort.

What should you use?

A. Azure AD Privileged Identity Management (PIM)

B. Azure Policy

C. Azure Bastion

D. Azure Front Door

Suggested Answer: *C*

Community vote distribution

Walaakb Highly Voted 1 year, 9 months ago

Selected Answer: B

correct me if Im wrong but Bastion dose not seems to allow time limit , Im going with B

upvoted 17 times

Ramye 10 months, 3 weeks ago

Also the requirement is to use RDP only, so Bastion can't be an answer because with Bastion you do not connect with RDP protocol.

upvoted 1 times

Sekpluz 6 months, 3 weeks ago

With Bastion Standard, you can connect with RDP on windows and SSH on linux, the basic Bastion is only SSL from the web browser.

upvoted 1 times

uday1985 7 months, 3 weeks ago

you can configure the rules to allow only RDP, but JIT is not possible

upvoted 2 times

exmITQS Highly Voted 1 year, 10 months ago

Selected Answer: C

To meet the given requirements, you should use Azure Bastion to configure just-in-time (JIT) access for the virtual machines in RG1.

Azure Bastion provides secure and seamless RDP and SSH access to virtual machines over a web browser and eliminates the need for a public IP address. It simplifies the process of connecting to virtual machines by allowing users to connect directly to virtual machines through the Azure portal.

To enable JIT access with Azure Bastion, you can create a JIT policy that defines the rules for access, including limiting access to specific protocols like RDP and setting the maximum request time to two hours. This can be done using the Azure portal or Azure CLI, and once the policy is created, Azure Bastion will automatically enforce the access rules when users try to connect to the virtual machines.

upvoted 7 times

jwkin 1 year, 10 months ago

I agree. https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage

upvoted 3 times

sebas12345 6 months ago

The link you shared doesn't mention anything about Bastion !

upvoted 1 times

talosDevbot Most Recent 3 months ago

You use Azure Bastion to limit the protocol to RDP only.
Bastion does not have JIT access capabilities but Defender for Cloud does.

The question states that you already have a Defender for Cloud subscription.

upvoted 1 times

Btwldonno 3 months, 2 weeks ago

I don't even know if there is a clear definition of Azure Policy. I'd choose A because user needs to require for access to the VMs, and that should be via PIM.

upvoted 1 times

g_man_rap 4 months, 3 weeks ago

Selected Answer: C

A. Azure AD Privileged Identity Management (PIM):

Incorrect: PIM is a service that helps manage, control, and monitor access to important resources in Azure. It is primarily focused on managing privileged roles within Azure AD, like who has access to a specific role and for how long. It doesn't provide direct JIT access to virtual machines.

B. Azure Policy:

Incorrect: Azure Policy helps to enforce organizational standards and assess compliance at scale by applying policies to resources. While you can use policies to control things like allowed VM sizes or locations, Azure Policy does not handle JIT access configurations.

C. Azure Bastion:

Correct: Azure Bastion is a fully managed service that provides secure and seamless RDP and SSH connectivity to your VMs directly in the Azure portal over SSL. It supports JIT access by limiting the exposure of VMs to the internet and only allowing connections via the Azure portal. It can be configured to limit access to specific protocols (like RDP) and to enforce time restrictions, such as the 2-hour maximum access time requested.

upvoted 1 times

g_man_rap 4 months, 1 week ago

Among the provided options, Azure Bastion (Option C) is the closest to the correct response, although it doesn't provide Just-in-Time (JIT) access management.

upvoted 2 times

Durden871 6 months, 2 weeks ago

From another exam site who says, "Bastion".
To meet the given requirements, you should use Azure Bastion to configure just-in-time (JIT) access for the virtual machines in RG1.Azure Bastion provides secure and seamless RDP and SSH access to virtual machines over a web browser and eliminates the need for a public IP address. It simplifies the process of connecting to virtual machines by allowing users to connect directly to virtual machines through the Azure portal.To enable JIT access with Azure Bastion, you can create a JIT policy that defines the rules for access, including limiting access to specific protocols like RDP and setting the maximum request time to two hours. This can be done using the Azure portal or Azure CLI, and once the policy is created, Azure Bastion will automatically enforce the access rules when users try to connect to the virtual machines.

upvoted 2 times

Durden871 7 months, 3 weeks ago

This is a stupid question. Bastion is the best fit for security purposes to allow RDP access to a machine without exposing it to the internet. There is no option for JIT in Bastion. In order to set this up, you need a policy. Now, does that mean Azure Policy?

Navigate to Microsoft Defender for Cloud in the Azure portal.
Go to the Just-in-time VM access section under Configuration & management.
Select the virtual machines in RG1 you want to configure JIT for.
Configure the JIT policy:
Set the maximum request time to 2 hours.
Specify RDP (port 3389) as the allowed protocol.
Save the configuration.

upvoted 2 times

Ramye 10 months, 4 weeks ago

Selected Answer: B

Answer is B since one of the requirements is to use RDP only.

With Bastion you don't connect using RDP and Microsoft specifically mentions not to use RDP as the requirement.

upvoted 3 times

Jay_13 10 months, 3 weeks ago

Azure Bastion is a fully managed PaaS service that you provision to securely connect to virtual machines via private IP address. It provides secure and seamless RDP/SS…

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network for which it's provisioned.

upvoted 2 times

xoe123 11 months, 1 week ago

Know that Azure Bastion and JIT access cannot be used together. If you enable Azure Bastion with an existing JIT access policy enabled on a VM, the bastion host will not connect to the target machine and you will get a connection error!. https://dev.to/adbertram/how-to-enable-and-configure-azure-jit-for-vms-4a26

upvoted 1 times

Gurulee 12 months ago

I'd go with Azure Policy since Bastion alone does not support all the requirements listed in question.

Azure Bastion and Just in time (JIT) access are two different technologies

upvoted 1 times

estyj 1 year ago

You can setup JIT network access policy for the Resource Group. https://learn.microsoft.com/en-us/rest/api/defenderforcloud/jit-network-access-policies?view=rest-defenderforcloud-2020-01-01

upvoted 1 times

chepeerick 1 year, 2 months ago

Azure Policy

upvoted 1 times

Vika_1_111 1 year, 3 months ago

Selected Answer: B

If i read this article correctly, then it can be accomplished by configuring the policy https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage

upvoted 1 times

donathon 1 year, 4 months ago

Selected Answer: B

Azure Policy make more sense

upvoted 1 times

donathon 1 year, 4 months ago

Selected Answer: B

A. Azure AD Privileged Identity Management (PIM) >> You cannot restrict to protocol.

B. Azure Policy >> Looks like the answer.

C. Azure Bastion >> You cannot limit the time using this.

D. Azure Front Door >> Not for this purpose

upvoted 4 times

itsadel 1 year, 5 months ago

Selected Answer: C

Azure Bastion provides secure and seamless RDP and SSH access to Azure virtual machines directly through the Azure portal. It acts as a jump server or a bastion host, eliminating the need to expose public IP addresses or configure virtual private networks (VPNs) for remote access.

upvoted 2 times

Marchiano 1 year, 5 months ago

Selected Answer: B

There are no references for Azure Bastion on the SC-200 MS Learn course

upvoted 2 times

Marchiano 1 year, 5 months ago

I have changed my mind to A. Azure AD Privileged Identity Management (PIM)

With PIM you can set the "Activation maximum duration" and since you are looking to configure JIT, which can restrict the ports, then it will make more sense to me to go through this path.

Why to configure an Azure Policy since the scenario specifies that you are looking to configure JIT? So PIM and JIT can provide what is requested.

https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings
"Use the Activation maximum duration slider to set the maximum time, in hours, that an activation request for a role assignment remains active before it expires. This value can be from one to 24 hours."

https://learn.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage
"JIT lets you allow access to your VMs only when the access is needed, on the ports needed, and for the period of time needed."
upvoted 2 times

Question #47 *Topic 2*

HOTSPOT
-

You have an Azure subscription that uses Microsoft Defender for Cloud.

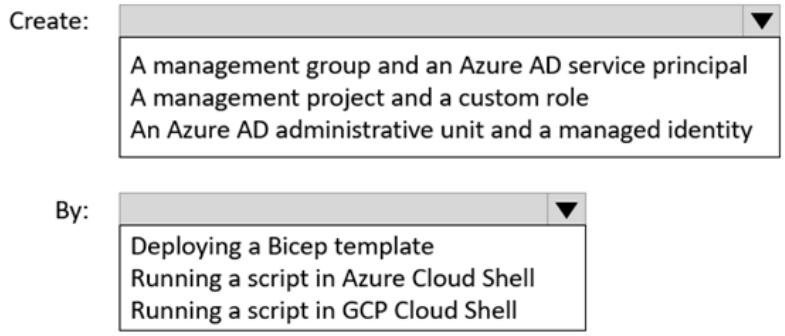
You create a Google Cloud Platform (GCP) organization named GCP1.

You need to onboard GCP1 to Defender for Cloud by using the native cloud connector. The solution must ensure that all future GCP projects are onboarded automatically.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area

Create:
A management group and an Azure AD service principal
A management project and a custom role
An Azure AD administrative unit and a managed identity

By:
Deploying a Bicep template
Running a script in Azure Cloud Shell
Running a script in GCP Cloud Shell

splearner Highly Voted 1 year, 8 months ago

Answer seems correct: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp

5. Enter all relevant information.
(Optional) If you select Organization, a management project and an organization custom role will be created on your GCP project for the onboarding process. Auto-provisioning will be enabled for the onboarding of new projects.
(...)
10. Select the GCP Cloud Shell >.
upvoted 14 times

cris_exam 1 year, 3 months ago

I agree here, as per the above doc shared by splearner, provided answer is correct.
upvoted 2 times

g_man_rap Most Recent 4 months, 1 week ago

In GCP: You are responsible for creating a management project and a custom role. The management project centralizes all integration-related tasks, and the custom role ensures that the service principal from Azure has the correct permissions.
In Azure: You run a script in Azure Cloud Shell, which sets up the connection between GCP and Azure Defender for Cloud. This script automates much of the integration work, configuring the necessary permissions and API interactions.
upvoted 1 times

xRiot007 4 weeks ago
The script is run the GCP Cloud Shell, not Azure shell. https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp#configure-access-for-your-organization
upvoted 1 times

estyj 1 year ago
Create a management project and a custom role, by running a script in GCP Cloud Shell. https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-gcp#connect-your-gcp-project
upvoted 2 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

mali1969 1 year, 3 months ago
Create : A management project and custom role
By : Running a script in Azure Cloud Shell
upvoted 1 times

jinxie 10 months, 2 weeks ago
GCP cloud shell as the script is ran against the google platform and not the Azure platform. Google does not support Azcli
upvoted 1 times

Question #48 *Topic 2*

You have an Azure subscription that contains a virtual machine named VM1 and uses Microsoft Defender for Cloud.

Microsoft Defender for Cloud has automatic provisioning configured to use Azure Monitor Agent.

You need to create a custom alert suppression rule that will suppress false positive alerts for suspicious use of PowerShell on VM1.

What should you do first?

A. From Microsoft Defender for Cloud, export the alerts to a Log Analytics workspace.

B. From Microsoft Defender for Cloud, add a workflow automation.

C. On VM1, trigger a PowerShell alert.

D. On VM1, run the Get-MPThreatCatalog cmdlet.

Suggested Answer: *C*

Community vote distribution

C (100%)

peponokefalos Highly Voted 8 months ago

Correct answer is C.

In order to deploy a suppression rule, you must first trigger an alert.

upvoted 7 times

Gurulee Most Recent 6 months ago

C

Alert types that were never triggered on a subscription or management group before the rule was created won't be suppressed.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-suppression-rules#create-a-suppression-rule

upvoted 1 times

chepeerick 8 months, 1 week ago

Correct C

upvoted 1 times

[Removed] 11 months, 3 weeks ago

Selected Answer: C

Answer is C. You must trigger the alert before deploying a suppression rule.

upvoted 4 times

GeoPoi 1 year, 1 month ago

The answer its C , repeated question.

upvoted 3 times

HOTSPOT
-

Case study
-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might conta`in exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
-
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
-

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment
-

Identity Environment
-

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

Microsoft 365 Environment
-

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

-

Fabrikam has an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

-

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

-

Planned changes

-

Fabrikam plans to implement the following services:

• Microsoft Defender for Cloud
• Microsoft Sentinel

Business Requirements

-

Fabrikam identifies the following business requirements:

• Use the principle of least privilege, whenever possible.
• Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

• Ensure that impossible travel alert policies are based on the previous activities of each user.
• Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

• Ensure that the members of Group2 can modify security policies.
• Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
• Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
• Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

• Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
• From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
• Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
• Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
• Ensure that App1 is available for use in Microsoft Sentinel automation rules.
• Identify the mean time to triage for incidents generated during the last 30 days.
• Identify the mean time to close incidents generated during the last 30 days.
• Ensure that the members of Group1 can create and run playbooks.
• Ensure that the members of Group1 can manage analytics rules.
• Run hunting queries on Pool1 by using Jupyter notebooks.
• Ensure that the members of Group2 can manage incidents.
• Maximize the performance of data queries.
• Minimize the amount of collected data.

You need to meet the Microsoft Defender for Cloud Apps requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

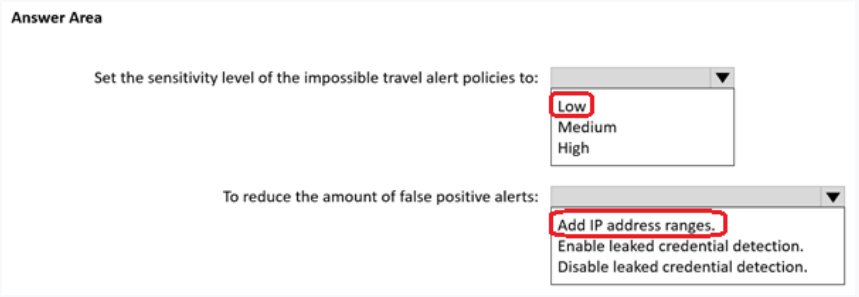
Set the sensitivity level of the impossible travel alert policies to:

- Low
- Medium
- High

To reduce the amount of false positive alerts:

- Add IP address ranges.
- Enable leaked credential detection.
- Disable leaked credential detection.

Suggested Answer:



ant0b1 Highly Voted 1 year, 3 months ago
based on this source the answer is medium and add ip address ranges
https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy#tune-anomaly-detection-policies
upvoted 16 times

7d801bf Most Recent 6 months ago
should be medium
upvoted 3 times

Ramye 10 months ago
Yes, the first should be Medium as you wan to limit the alerts per the requirements.
upvoted 2 times

Jay_13 10 months, 3 weeks ago
Low
Add IP address range.
upvoted 1 times

mb0812 10 months ago
Not Low. It is Medium.
upvoted 4 times

Gurulee 12 months ago
The default severity of an alert triggered by Microsoft Defender's impossible travel detection is medium.
Admins can also use the sensitivity slider feature to tune the detection to be more or less sensitive, depending on the organization's needs. For example, low sensitivity levels will use system suppressions (built-in detections that are always suppressed); tenant suppressions (common activities based on previous activity in the tenant); and user suppressions (common activities based on a user's previous behavior). High sensitivity levels will suppress only system-level detections.
upvoted 2 times

chepeerick 1 year, 2 months ago
medium and add IP address
upvoted 4 times

trashbox 1 year, 3 months ago
The first one should be Medium.

Severity Medium: "for example a sign-in attempt from an unusual location."
https://learn.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
upvoted 3 times

billo79152718 1 year, 5 months ago
Correct
upvoted 1 times

HOTSPOT
-

Case study
-

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might conta`in exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study
-
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview
-

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment
-

Identity Environment
-

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

Microsoft 365 Environment
-

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment

-

Fabrikam has an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues

-

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements

-

Planned changes

-

Fabrikam plans to implement the following services:

• Microsoft Defender for Cloud
• Microsoft Sentinel

Business Requirements

-

Fabrikam identifies the following business requirements:

• Use the principle of least privilege, whenever possible.
• Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

• Ensure that impossible travel alert policies are based on the previous activities of each user.
• Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

• Ensure that the members of Group2 can modify security policies.
• Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
• Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
• Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements

Fabrikam identifies the following Microsoft Sentinel requirements:

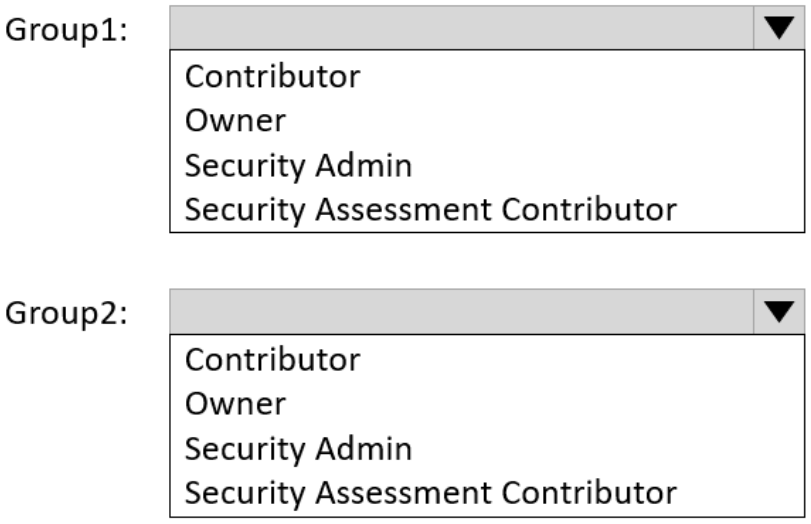
• Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
• From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
• Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
• Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
• Ensure that App1 is available for use in Microsoft Sentinel automation rules.
• Identify the mean time to triage for incidents generated during the last 30 days.
• Identify the mean time to close incidents generated during the last 30 days.
• Ensure that the members of Group1 can create and run playbooks.
• Ensure that the members of Group1 can manage analytics rules.
• Run hunting queries on Pool1 by using Jupyter notebooks.
• Ensure that the members of Group2 can manage incidents.
• Maximize the performance of data queries.
• Minimize the amount of collected data.

You need to assign role-based access control (RBAC) roles to Group1 and Group2 to meet the Microsoft Defender for Cloud requirements and the business requirements.

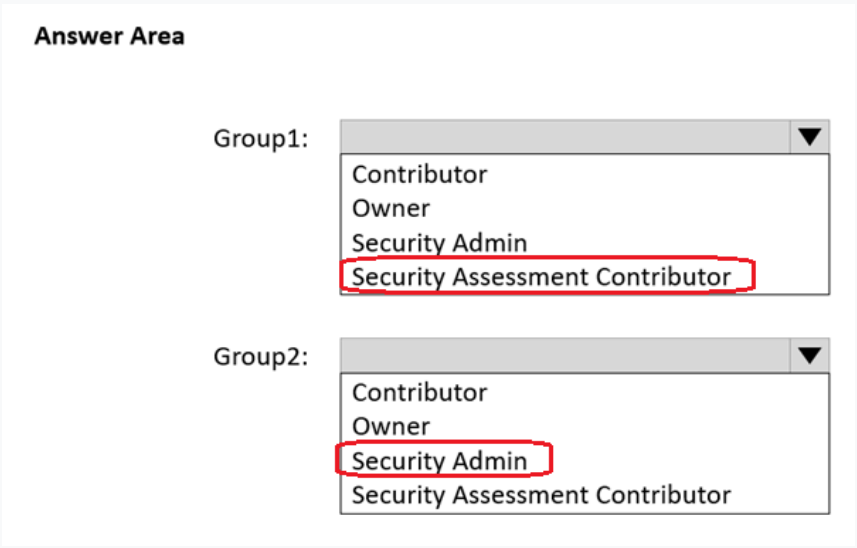
Which role should you assign to each group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



Marchiano Highly Voted 11 months ago

Group 1: Owner, as only the Owner can "Add/assign initiatives (including) regulatory compliance standards)" at subscription level, as requested.

Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions

Group 2: Security Admin

upvoted 43 times

billo79152718 Highly Voted 11 months, 1 week ago

Group1: Contributor

Group2: Security Admin

There is nothing called Secuirty Assesment Contributor.

upvoted 7 times

Ramye 4 months, 3 weeks ago

Wrong answer for Group 1. Checkout this link https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions

upvoted 1 times

jsTec 11 months ago

Well, actually there is a Role called Security Assessment Contributor in Azure:
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles
upvoted 1 times

Gurulee 6 months ago
In Microsoft Defender for Cloud, the Security Assessment Contributor role allows you to push assessments to Microsoft Defender for Cloud. To assign this role to a user, you must have the Owner or Security Manager role.
upvoted 1 times

billo79152718 11 months ago
That is correct. But still does not change the answer in the question.

Security Assessment Contributor "Lets you push assessments to Microsoft Defender for Cloud"

An assessment is conducted before an incident. The Microsoft Sentinel Requirements states: Ensure that the members of Group2 can manage incidents.
upvoted 1 times

Sneekygeek Most Recent 2 months, 2 weeks ago
According to the matrix in this security admin can perform both actions and is less privileged than sub owner.
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 2 times

DChilds 2 months, 3 weeks ago
I hope this question is outdated because according to current Microsoft Learn documentation, Security Admin can do both tasks.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 3 times

Ramye 4 months, 2 weeks ago
Based on the business (least privilege permission) and MS Defender for Cloud requirements given below - note for group1 it specifically says permission will go at the Subscription level
• Ensure that the members of Group2 can modify security policies.
• Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.

Answers are:
Group1 ---> Owner (because it is at the subscription level and only Owner at this level)
Group2 ---> Security Admin (because of least privilege and the question does not say specifically if it is at the subscription level)

Source: https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 3 times

Gurulee 6 months ago
Group1: The Security Admin role is required to add and assign initiatives, including regulatory compliance standards, at the subscription level 1.
Group2: The Security Admin role is required to modify security policies.
upvoted 3 times

estyj 6 months ago
looking at chart https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions Looks like Security Admin can also add/assign initiatives, but security admin cannot at the the subscription level
Group1: Owner
Group 2: Security Admin- can modify security policies - least privileged.
upvoted 2 times

blacksheep_29 7 months, 3 weeks ago
Group1 - Owner
Group 2 - Security Admin

Source - https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 1 times

chepeerick 8 months, 1 week ago
Did not find the role

upvoted 1 times

mali1969 9 months, 4 weeks ago

According to the article User roles and permissions - Microsoft Defender for Cloud, you need to assign the following roles to Group1 and Group2:

Group 1: Security Admin. This role allows the user to update the security policy, dismiss alerts and recommendations, and apply recommendations. It also allows the user to assign regulatory compliance policy initiatives at the Azure subscription level.

Group 2: Contributor. This role allows the user to apply security recommendations for a resource and use Fix. It also allows the user to modify security policies.

upvoted 3 times

EricShon 10 months, 2 weeks ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions

For Group1:
Role: "Owner"
According to the chart, the "Owner" role at the Subscription level allows for adding/assigning initiatives, including regulatory compliance standards. This meets the requirement that members of Group1 should be able to assign regulatory compliance policy initiatives at the Azure subscription level.

For Group2:
Role: "Security Admin"
This role allows for the editing of security policies, which aligns with the requirement that members of Group2 should be able to modify security policies.

upvoted 1 times

JandedFelloh 11 months ago

Answer from @Marchiano is correct. Clearly straightforward from the link he provided.

upvoted 2 times

donathon 11 months ago

Security Admin for both. Owner is at the subscription level which has more permissions. https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions

upvoted 1 times

Doinitza 10 months, 3 weeks ago

Hi, check the question Question #26 Topic 1, @Marchiano is right.

upvoted 3 times

danb67 8 months, 3 weeks ago

Nope Security admin will do for group 2

upvoted 2 times

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Fabrikam, Inc. is a financial services company.

The company has branch offices in New York, London, and Singapore. Fabrikam has remote users located across the globe. The remote users access company resources, including cloud resources, by using a VPN connection to a branch office.

Existing Environment -

Identity Environment -

The network contains an Active Directory Domain Services (AD DS) forest named fabrikam.com that syncs with an Azure AD tenant named fabrikam.com. To sync the forest, Fabrikam uses Azure AD Connect with pass-through authentication enabled and password hash synchronization disabled.

The fabrikam.com forest contains two global groups named Group1 and Group2.

Microsoft 365 Environment -

All the users at Fabrikam are assigned a Microsoft 365 E5 license and an Azure Active Directory Premium Plan 2 license.

Fabrikam implements Microsoft Defender for Identity and Microsoft Defender for Cloud Apps and enables log collectors.

Azure Environment -

Fabrikam has an Azure subscription that contains the resources shown in the following table.

Name	Type	Description
App1	Azure logic app	To automate incident generation in an internal ticketing system, the security operations (SecOps) team invokes App1 by using an HTTP endpoint.
SAWkspc1	Azure Synapse Analytics workspace	SAWkspc1 hosts an Apache Spark pool named Pool1.
LAWkspc1	Log Analytics workspace	LAWkspc1 will be used in a planned Microsoft Sentinel implementation.

Amazon Web Services (AWS) Environment

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and does NOT have any agents installed.

Current Issues -

When the users use the VPN connections, Microsoft 365 Defender raises a high volume of impossible travel alerts that are false positives.

Defender for Identity raises a high volume of Suspected DCSync attack alerts that are false positives.

Requirements -

Planned changes -

Fabrikam plans to implement the following services:

• Microsoft Defender for Cloud
• Microsoft Sentinel

Business Requirements -

Fabrikam identifies the following business requirements:

• Use the principle of least privilege, whenever possible.
• Minimize administrative effort.

Microsoft Defender for Cloud Apps Requirements

Fabrikam identifies the following Microsoft Defender for Cloud Apps requirements:

• Ensure that impossible travel alert policies are based on the previous activities of each user.
• Reduce the amount of impossible travel alerts that are false positives.

Microsoft Defender for Identity Requirements

Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Defender for Cloud Requirements

Fabrikam identifies the following Microsoft Defender for Cloud requirements:

• Ensure that the members of Group2 can modify security policies.
• Ensure that the members of Group1 can assign regulatory compliance policy initiatives at the Azure subscription level.
• Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.
• Minimize the administrative effort required to investigate the false positive alerts.

Microsoft Sentinel Requirements -

Fabrikam identifies the following Microsoft Sentinel requirements:

• Query for NXDOMAIN DNS requests from the last seven days by using built-in Advanced Security Information Model (ASIM) unifying parsers.
• From AWS EC2 instances, collect Windows Security event log entries that include local group membership changes.
• Identify anomalous activities of Azure AD users by using User and Entity Behavior Analytics (UEBA).
• Evaluate the potential impact of compromised Azure AD user credentials by using UEBA.
• Ensure that App1 is available for use in Microsoft Sentinel automation rules.
• Identify the mean time to triage for incidents generated during the last 30 days.
• Identify the mean time to close incidents generated during the last 30 days.
• Ensure that the members of Group1 can create and run playbooks.
• Ensure that the members of Group1 can manage analytics rules.
• Run hunting queries on Pool1 by using Jupyter notebooks.
• Ensure that the members of Group2 can manage incidents.
• Maximize the performance of data queries.
• Minimize the amount of collected data.

You need to deploy the native cloud connector to Account 1 to meet the Microsoft Defender for Cloud requirements.

What should you do in Account1 first?

A. Create an AWS user for Defender for Cloud.

B. Configure AWS Security Hub.

C. Deploy the AWS Systems Manager (SSM) agent.

D. Create an Access control (IAM) role for Defender for Cloud.

Suggested Answer: *A*

Community vote distribution

CDR 2 weeks, 2 days ago

Selected Answer: D

To meet the Microsoft Defender for Cloud requirements and deploy the native cloud connector to Account1, the first step you should take is to create an AWS user for Defender for Cloud. This user will need the necessary permissions to allow Defender for Cloud to access and manage your AWS resources.

After creating the AWS user, you can proceed with deploying the AWS Systems Manager (SSM) agent and configuring other necessary settings.
upvoted 2 times

g_man_rap 4 months, 1 week ago

Selected Answer: C

C. Deploy the AWS Systems Manager (SSM) agent

Explanation: AWS Systems Manager (SSM) provides the ability to manage and automate the administration of EC2 instances. By deploying the SSM agent, you enable the management of your instances from AWS Systems Manager, which can be used to run scripts, install software, and manage your EC2 instances remotely. This includes deploying the Azure Connected Machine agent across existing and future EC2 instances.

Conclusion: Deploying the SSM agent is crucial for automating the deployment of any additional software, including the Azure Connected Machine agent.

upvoted 2 times

user636 4 months, 1 week ago

Selected Answer: B

Answer is B.

The question did not say if AWS security hub is enabled. As per the docs, the first thing we need to configure is the AWS Security Hub.
https://learn.microsoft.com/en-us/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

The rest of the options (A,C,D) will be done during the later steps of the integration.

upvoted 1 times

Sneekygeek 8 months, 3 weeks ago

Selected Answer: B

https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

upvoted 4 times

oricgoldfinger 9 months, 1 week ago

Selected Answer: B

https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

upvoted 3 times

ostralo 9 months, 3 weeks ago

Selected Answer: C

AWS Systems Manager manages autoprovisioning by using the SSM Agent. Some Amazon Machine Images already have the SSM Agent preinstalled. If your EC2 instances don't have the SSM Agent, install it by using either of the following instructions from Amazon:

ref) https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws#defender-for-servers

upvoted 4 times

mmmyo 10 months, 3 weeks ago

Selected Answer: B

First step is Set up AWS Security Hub

upvoted 4 times

Ramye 10 months, 4 weeks ago

Selected Answer: B

Based on the learning given below you need to Set up AWS Security Hub: first https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

upvoted 4 times

Discuss4certi 10 months, 3 weeks ago

in the description it indeed says to set up the security hub first. However if you read properly it say you need a master account

upvoted 1 times

CollabGuy 11 months, 2 weeks ago

Selected Answer: C

You need SSM

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws#native-connector-plan-requirements:~:text=If%20your%20EC2%20instances%20don%27t%20have%20the%20SSM%20Agent%2C%20install%20it%20by%20using%20either%20of%

upvoted 2 times

CollabGuy 11 months, 2 weeks ago

but I guess A is also valid
https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts#:~:text=AWS%20user%20for%20Defender%20for%20Cloud%20%2D%20A%20less%20secure%20option%20if%20you%20don%27t%20have%20I

toss a coin

upvoted 1 times

Rubes 1 year, 1 month ago

I think the correct answer was A but this is now an outdated question based on the link below?
https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-aws-connector

"The retired Classic cloud connector - Requires you to configure your AWS account to create a user that Defender for Cloud can use to connect to your AWS environment. The classic connector is only available to customers who have previously connected AWS accounts with it."
upvoted 2 times

blacksheep_29 1 year, 1 month ago
The Keyword is Native Connector - According to the article it says Creation of AWS account
Link -https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws

AWS account can refer to AWS User - So i'll go with A. Correct me if I'm wrong.
upvoted 1 times

kabooze 1 year, 2 months ago
Selected Answer: B
guide as described by shadowdark shows it's option B
upvoted 1 times

shadowdark83 1 year, 2 months ago
Selected Answer: B
Based on the documentation below, the first step is set up the AWS Security Hub, so I go with B.

https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts
upvoted 2 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

User25673 1 year, 2 months ago
This is how the SC-200 course on Learn describes the process:

https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts
upvoted 1 times

cris_exam 1 year, 3 months ago
Selected Answer: C
The question specifically asks what you need to do IN the AWS account (Account1), so not an action that needs to be done in Azure.

Based on the provided options, the only one that makes sense is C: Deploy AWS Systems Manager (SSM) agent.

https://learn.microsoft.com/en-us/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts

"Configure the SSM Agent
AWS Systems Manager is required for automating tasks across your AWS resources. If your EC2 instances don't have the SSM Agent, follow the relevant instructions from Amazon:"
upvoted 2 times

- **cris_exam** 1 year, 3 months ago
  Just to add some more clarification, since the focus is on ARC config and deployment, this implies we need the Microsoft Defender for Cloud integration and NOT the AWS Security Hub, hence that's why B is not correct here.
  upvoted 2 times

  - **kabooze** 1 year, 2 months ago
    but for automation it's the "AWS Systems Manager" and it asks us to config account1 which is in AWS
    upvoted 1 times

- **cris_exam** 1 year, 3 months ago
  OK, so after some second thoughts - I re-read the whole AWS connector integration process and I actually agree with A, the given answer.

  A - AWS User needed for Defender for Cloud

You need a AWS user before proceeding with any further step.

Sorry for confusing you guys here.
upvoted 5 times

kabooze 1 year, 2 months ago
It would be B according to this guide: https://learn.microsoft.com/en-za/training/modules/connect-non-azure-machines-to-azure-defender/4-connect-aws-accounts
upvoted 1 times

Anil0512 1 year, 3 months ago
Correct Answer is C
upvoted 1 times

Question #52 *Topic 2*

You have the resources shown in the following table.

Name	Type	Description	Location
Server1	Server	File server that runs Windows Server	On-premises
Server2	Virtual machine	Application server that runs Linux	Amazon Web Services (AWS)
Server3	Virtual machine	Domain controller that runs Windows Server	Azure
Server4	Server	Domain controller that runs Windows Server	On-premises

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to enable Microsoft Defender for Servers on each resource.

Which resources will require the installation of the Azure Arc agent?

A. Server3 only

B. Server1 and Server4 only

C. Server1, Server2, and Server4 only

D. Server1, Server2, Server3, and Server4

Suggested Answer: *C*

Community vote distribution

C (100%)

mali1969 Highly Voted 3 months, 3 weeks ago

Selected Answer: C

Azure Arc agent is a software that enables you to manage your Windows and Linux machines hosted outside of Azure on your corporate network or other cloud providers. It allows you to project your existing non-Azure and/or on-premises resources into Azure Resource Manager

upvoted 12 times

Murtuza Most Recent 1 month ago

Choices should be only AWS and On-Premises

upvoted 1 times

chepeerick 2 months, 1 week ago

Correct as it Azure

upvoted 1 times

Question #53 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have a GitHub account named Account1 that contains 10 repositories.

You need to ensure that Defender for Cloud can access the repositories in Account1.

What should you do first in the Microsoft Defender for Cloud portal?

A. Enable integrations.

B. Enable a plan.

C. Add an environment.

D. Enable security policies.

Suggested Answer: *C*

Community vote distribution

C (100%)

mali1969 Highly Voted 9 months, 4 weeks ago

Selected Answer: C

To add an environment, you need to sign in to the Azure portal, go to Microsoft Defender for Cloud > Environment settings, select Add environment, and then select GitHub. You also need to enter a name, select your subscription, resource group, and region.

upvoted 8 times

63f5d81 Most Recent 1 month, 4 weeks ago

Selected Answer: C

An environment represents an external service or platform that you want to integrate with Defender for Cloud. It acts as a bridge between Defender for Cloud and the external resource.

upvoted 1 times

chepeerick 8 months, 1 week ago

Correct

upvoted 1 times

RafaelAlvexx 9 months, 1 week ago

On exam 27-September-23

upvoted 2 times

trashbox 9 months, 3 weeks ago

Selected Answer: C

The answer is correct, "Environment settings."

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-github#connect-your-github-account

upvoted 1 times

Question #54 *Topic 2*

HOTSPOT
-

You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud.

You have an Azure DevOps organization named AzDO1.

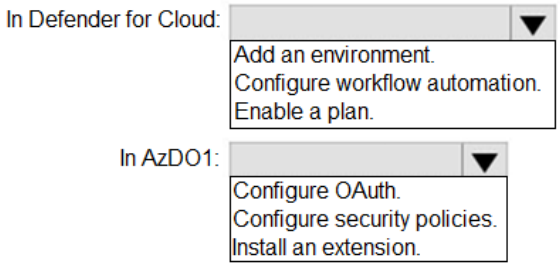
You need to integrate Sub1 and AzDO1. The solution must meet the following requirements:

• Detect secrets exposed in pipelines by using Defender for Cloud.
• Minimize administrative effort.

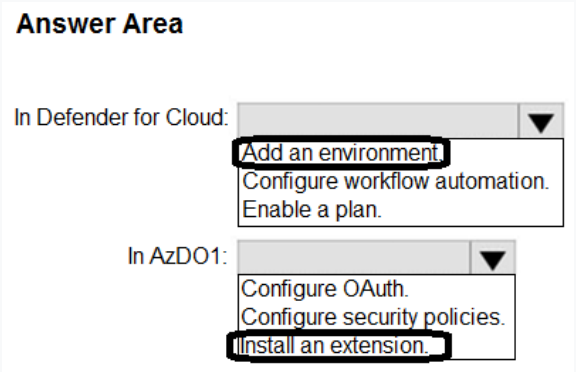
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:



VeiN 2 months, 1 week ago

1. Environment
2. ?

I`m not sure here since after adding devops via Def For Cloud I can see on devops organization> extensions that extensions were automatcally added:
Microsoft Security DevOps
Microsoft Defender for DevOps Container Mapping

IDK did this change ? Was it previously not automatic ?

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct

upvoted 2 times

NICKTON81 1 year, 3 months ago

The answer is correct!

https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-devops?branch=main

https://learn.microsoft.com/en-us/azure/defender-for-cloud/azure-devops-extension
upvoted 4 times

Ramye 10 months, 3 weeks ago
But it appears the Azure DevOps environment is already exist as it the question says the below: so does it have to be created?
You have an Azure DevOps organization named AzDO1.
upvoted 1 times

xRiot007 4 weeks ago
Organization is not Environment. Two different things :P
upvoted 1 times

Ramye 10 months, 3 weeks ago
By created I meant to say added.
upvoted 1 times

Ramye 10 months, 1 week ago
The answers given are correct. I was under the impression this AzDO1 was within Azure but the fact is it is outside of Azure just like AWS or GCP environment. Those environments first need to be onboarded to be protected.
upvoted 1 times

mali1969 1 year, 3 months ago
To integrate Sub1 and AzDO1, you should do the following:

In Defender for Cloud:
- Enable a plan for your subscription. This will allow you to use Defender for Cloud features such as secret detection, vulnerability assessment, and threat protection.
- Configure workflow automation to send alerts and notifications to AzDO1 when secrets are exposed in pipelines2. You can use webhooks or Azure Logic Apps to create custom workflows.

In AzDO1:
- Install an extension called Azure DevOps Secrets Scanner from the marketplace3. This will enable you to scan your code and pipelines for secrets and report them to Defender for Cloud.

- Configure OAuth to authorize the extension to access your Azure subscription and Defender for Cloud. You can use the Azure Active Directory OAuth provider to grant permissions.
upvoted 3 times

mali1969 1 year, 3 months ago
Correct answer :
In Defender for Cloud, add an environment
In AzDO1, install an extension
upvoted 5 times

pigl3t 1 year, 3 months ago
right answer based on this: https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-devops?branch=main
upvoted 1 times

Fez786 1 year, 3 months ago
This new question arrived today 9th september 2023.
Can someone please verify the correct answer?
upvoted 1 times

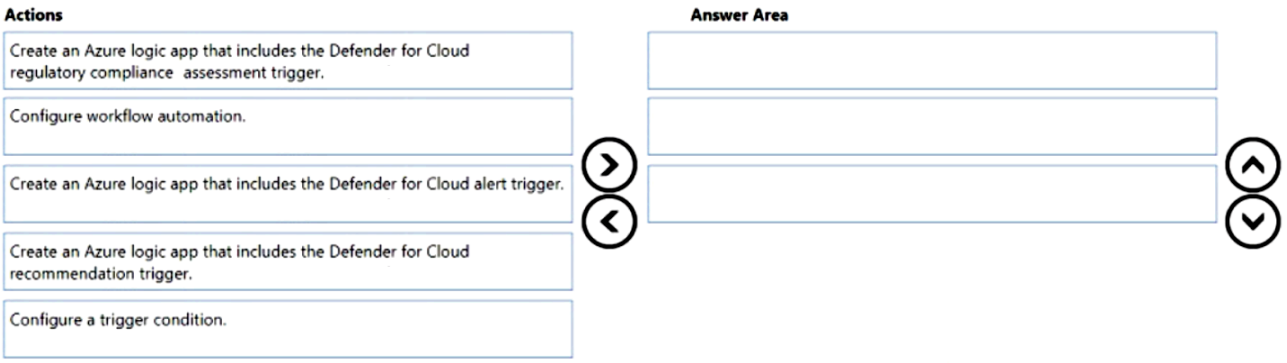
Question #55 *Topic 2*

DRAG DROP
-

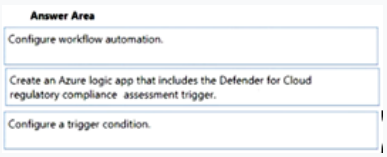
You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to create a workflow that will send a Microsoft Teams message to the IT department of your company when a new Microsoft Secure Score action is generated.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Suggested Answer:



ceejay12 Highly Voted 1 year, 3 months ago

1. Configure workflow automation
2. Configure a trigger condition
3. Create a logic app that has the Defender for Cloud recommendation trigger

https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 27 times

davidli 1 year, 2 months ago

Agree with this answer and confirm that the secure score is a recommendation.
https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide
upvoted 2 times

hovlund 1 year, 2 months ago

It is in reverse...
upvoted 4 times

danb67 1 year, 2 months ago

No it's not. The link he provides shows the order.
upvoted 1 times

Tuitor01 3 weeks, 6 days ago

you're right, the think I I get that people get confused by M$ chosen nomenclature. It's all about the context, trigger inside the logic app and the trigger inside the workflow automation template that triggers the action. So the order is indeed correct in ceeja12 answer.
upvoted 1 times

Tuitor01 3 weeks, 6 days ago

btw, in the automation template triggers are called in the ' trigger conditions' section.
upvoted 1 times

Vokuhila 7 months ago

The links show:
Create a logic app and define when it should automatically run
Manually trigger a logic app
Configure workflow automation at scale
upvoted 2 times

Durden871 6 months, 1 week ago

I'm literally looking at the link right now:
1. From Defender for Cloud's sidebar, select Workflow automation.
4. The triggers that will initiate this automatic workflow. For example, you might want your logic app to run when a security alert that contains "SQL" is generated.
6. From the Actions section, select visit the Logic Apps page to begin the logic app creation process.
upvoted 4 times

xRiot007 4 weeks ago

The logic app can be created before configuring the workflow automation or while configuring it. At step 6 you can use an existing logic app, you are not forced to create a new one.
upvoted 1 times

Gurulee 12 months ago

Agree with your answer.
You can also use Power Automate.
1. Create a new flow.
2. Select the Microsoft Secure Score connector.
3. Choose the trigger When a secure score improvement action is generated.
4. Select the Microsoft Teams connector.
upvoted 1 times

shadowdark83 Highly Voted 1 year, 2 months ago

It is not possible to create a Workflow Automation without first creating a logic app to place in the action field.

So, after creating the Logic App, you create the Workflow Automation, and during the creation of the Workflow Automation, you select the trigger as "Recommendation".

So the answer is 4-2-5.
upvoted 12 times

Ramye 10 months, 2 weeks ago

I thought too not possible but apparently, it's possible. Step # 6 under the section: "Create a logic app and define when it should automatically run" in this link tells you you can use the existing Logic app or create a new one while creating Workflow Automation:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 1 times

Hawklx 5 months, 4 weeks ago

you are correct. but most of the preparation questions from Microsoft stress that you need to create a Logic App first, and Logic App, Trigger, Workflow automation is a working solution.
upvoted 1 times

xRiot007 4 weeks ago

Both are working solutions. The logic app can be created before starting workflow automation configuration or when arriving at the respective step during configuration
upvoted 1 times

user636 Most Recent 4 months, 1 week ago

Another Vague question, you need total of 4 steps. I see multiple correct answers here. I guess Microsoft just wanna test your knowledge & is not looking for the complete solution.

You can either start with the workflow automation, define a trigger condition, pause the workflow automation configuration, then manually create a logic & then you have to manually return to the workflow automation configuration page & then must select the logic app in the actions part of the workflow automation. This is a complete setup.
OR
Create a logic app with a with the appropriate trigger (MDC recommendation trigger in this case), then create a workflow automation and define a

trigger condition and select the logic app in the action part. This is a complete setup.

You cannot select a logic app in the workflow automation if the logic app with the appropriate trigger doesn't exists.
As for the exam, I'll go with the:
- create a workflow automation
- define a trigger condition
- create a logic app

However the next step is to select the logic app in the workflow automation, else the workflow automation will never trigger the logic app.
Good luck!
upvoted 1 times

g_man_rap 4 months, 1 week ago
Verified:
1. Create an Azure logic app that includes the Defender for Cloud recommendation trigger.
2. Configure a trigger condition.
3. Configure workflow automation.
upvoted 2 times

Studytime2023 4 months, 3 weeks ago
I've got to say, I'm starting to really despise Microshit and all their mixed messages.
This is directly from their practice test:

"Question 30 of 50
Your company uses Microsoft Defender for Cloud.

You need to create a Defender for Cloud workflow automation.

What should you create first?

Your Answer
a logic app
This answer is correct.
Correct Answer
a logic app
This answer is correct.
Workflow automation in Defender for Cloud can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. For example, you might want Defender for Cloud to email a specific user when an alert occurs. If you want to create workflow automation, you must configure it with an already existing logic app, which will be triggered by the workflow automation. As such, you must first create a logic app, and only after that, you can create a workflow automation in Defender for Cloud."
upvoted 1 times

Studytime2023 4 months, 3 weeks ago
In their comments bit with their feedback on the answer they included these two links:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
https://learn.microsoft.com/en-us/training/modules/remediate-azure-defender-security-alerts/

Obviously the first link then contradicts their statement.
For the sake of my test in two days time. If I'm presented with this question. I'll choose logic apps. workflow. trigger.
I'm pretty sure this is the last M$ cert I'm doing. I'm fed up with their nonsense.
upvoted 1 times

SC200XMEN 4 months, 4 weeks ago
CoPilot states;

Create an Azure logic app that includes the Defender for Cloud recommendation trigger.
Configure workflow automation.
Configure a trigger condition.
upvoted 1 times

Vokuhila 7 months ago

The correct order is:
1 Create logic app with compliance assessment trigger
2 Configure trigger
3 Configure workflow
upvoted 3 times

Vokuhila 7 months ago
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 1 times

aks_exam 8 months, 2 weeks ago
on exam 2024/April
upvoted 1 times

KRAKE3N 8 months, 2 weeks ago
1. Logic App
5. Trigger
2. Workflow automation
https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 3 times

Murtuza 1 year ago
This is the correct sequence

1. Create a logic app that has the Defender for Cloud recommendation trigger

2) Configure workflow automation

3) Configure a trigger condition
upvoted 11 times

Ramye 10 months, 1 week ago
These steps will work but you may want to follow the Microsoft given steps here https://learn.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

Mercury02m 1 year, 2 months ago
the answer should be 2,1,5

You can trigger logic app only after you create .

First you create workflow automation -> create logic app (regulatory compliance) and then trigger it.
upvoted 2 times

Anil0512 1 year, 2 months ago
To me it's 1 5 2
upvoted 2 times

Question #56 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Configure auto-provisioning by setting the security event storage to Common.

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

C. From the Azure portal, create an Azure Event Grid subscription.

D. Configure auto-provisioning by setting the security event storage to All Events.

E. From Defender for Cloud in the Azure portal, enable Microsoft Defender for Servers.

Suggested Answer: *AE*

Community vote distribution

AE (100%)

Faceless443 Highly Voted 8 months, 2 weeks ago

Selected Answer: AE

Answer seems correct to me. A and E.

Enable Auto-Provisioning from Defender for Cloud. And there you will be ask which Secrity Events should be stored. It is Nonne - Common - All.

and yeah, without enabling Defender for servers in the Defender for Cloud Portal this won't work.

upvoted 5 times

Murtuza Most Recent 6 months, 3 weeks ago

The question says to save costs so you need to choose COMMON and not ALL EVENTS

upvoted 1 times

TheHuman_ 6 months, 4 weeks ago

Selected Answer: AE

Indeed, you need to activate Defender for Servers in order to configure it. In addition, we want to minimize administrative effort, so we want 'common' instead of 'all events'.

upvoted 4 times

chepeerick 8 months, 1 week ago

Correct

upvoted 2 times

Question #57 *Topic 2*

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) subscription. The subscription contains multiple virtual machines that run Windows Server.

You need to enable Microsoft Defender for Servers on the virtual machines.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct answer is worth one point.

A. From Defender for Cloud, enable agentless scanning.

B. Onboard the virtual machines to Microsoft Defender for Endpoint.

C. From Defender for Cloud, configure the AWS connector.

D. Install the Azure Virtual Machine Agent (VM Agent) on each virtual machine.

E. From Defender for Cloud, configure auto-provisioning.

Suggested Answer: *BC*

Community vote distribution

CE (100%)

danb67 Highly Voted 1 year, 2 months ago

Selected Answer: CE

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers?source=recommendations

• For a Defender for Servers deployment, you set up a connector, turn off plans you don't need, configure auto-provisioning settings, authenticate to AWS/GCP, and deploy the settings.

• Auto-provisioning includes the agents used by Defender for Cloud and the Azure Connected Machine agent for onboarding to Azure with Azure Arc.

upvoted 11 times

DigitalV Highly Voted 1 year, 2 months ago

Selected Answer: CE

A. is incorrect because agentless scanning is an optional feature.
B. is incorrect because "when you enable Defender for Servers, Defender for Cloud automatically deploys a Defender for Endpoint extension." there is no need to onboard the machines with Defender for endpoint.
D. is incorrect because virtual machine agent has nothing to do

For me the correct answers are:
C. From Defender for Cloud, configure the AWS connector.
E. From Defender for Cloud, configure auto-provisioning.

https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers?source=recommendations

upvoted 7 times

g_man_rap Most Recent 4 months, 3 weeks ago

Selected Answer: CE

C. From Defender for Cloud, configure the AWS connector.

E. From Defender for Cloud, configure auto-provisioning.

upvoted 1 times

Avaris 7 months, 3 weeks ago

yes its CE checked with copilot

upvoted 1 times

kazaki 11 months ago

outdated question Arc is used now

upvoted 4 times

chepeerick 1 year, 2 months ago

Correct connector and onboard

upvoted 2 times

Question #58 *Topic 2*

HOTSPOT
-

You have an Azure subscription named Sub1 and an Azure DevOps organization named AzDO1. AzDO1 uses Defender for Cloud and contains a project that has a YAML pipeline named Pipeline1.

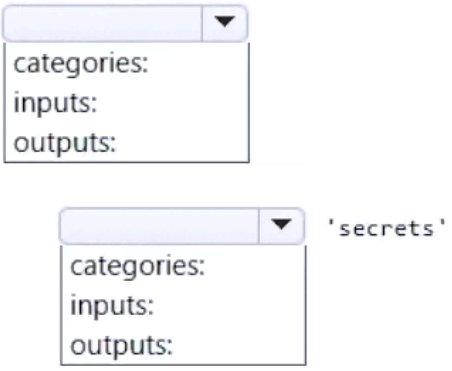
Pipeline1 outputs the details of discovered open source software vulnerabilities to Defender for Cloud.

You need to configure Pipeline to output the results of secret scanning to Defender for Cloud.

What should you add to Pipeline1? To answer, select the appropriate options in the answer area.

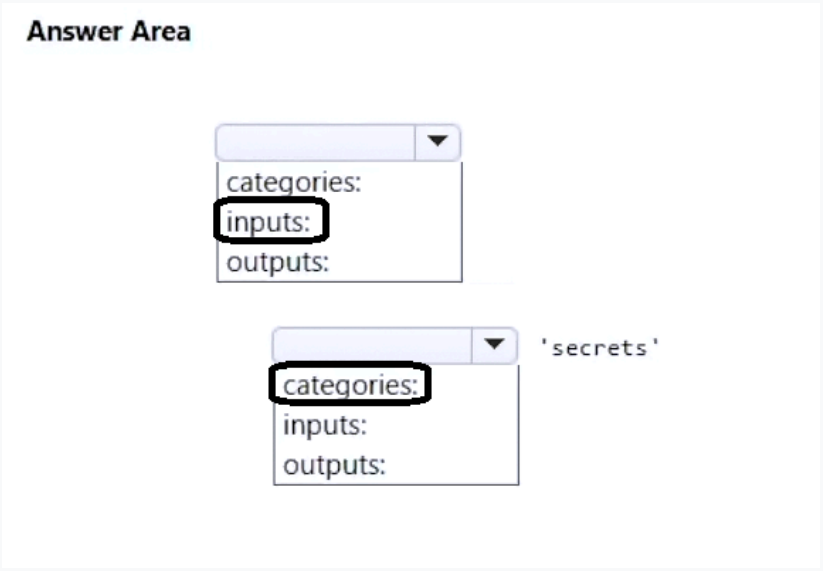
NOTE: Each correct selection is worth one point.

Answer Area



Suggested Answer:

Answer Area



ceejay12 Highly Voted 1 year, 3 months ago

1. inputs
2. categories

https://learn.microsoft.com/en-us/azure/defender-for-cloud/detect-exposed-secrets
upvoted 9 times

g_man_rap Most Recent 4 months, 1 week ago

- task: MicrosoftSecurityDevOps@1
inputs:
categories: 'secrets'
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct To add secret scanning to Azure DevOps build process:

Sign in to Azure DevOps

Navigate to Pipeline.

Locate the pipeline with MSDO Azure DevOps Extension is configured.

Select Edit.

Add the following lines to the YAML file

yml

Copy
inputs:
categories: 'secrets'
upvoted 2 times

Anil0512 1 year, 2 months ago
Yes correct. Inputs and Categories.
upvoted 1 times

Question #59 *Topic 2*

You create an Azure subscription named sub1.

In sub1, you create a Log Analytics workspace named workspace1.

You enable Microsoft Defender for Cloud and configure Defender for Cloud to use workspace1.

You need to collect security event logs from the Azure virtual machines that report to workspace1.

What should you do?

A. From Defender for Cloud, modify Microsoft Defender for Servers plan settings.

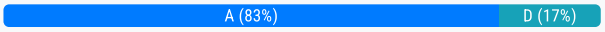
B. In sub1, register a provider.

C. From Defender for Cloud, create a workflow automation.

D. In workspace1, create a workbook.

Suggested Answer: *A*

Community vote distribution



user636 4 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 2 times

Murtuza 1 year ago

Answer is A

https://learn.microsoft.com/en-us/azure/defender-for-cloud/tutorial-enable-servers-plan

upvoted 1 times

im20batman 1 year, 1 month ago

Selected Answer: D

Answer is D

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/tutorial-monitor-vm-guest

upvoted 1 times

Fez786 1 year, 2 months ago

Selected Answer: A

THIS QUESTION IS SAME AS QUESTION 6 TOPIC 2.

CORRECT ANSWER IS A. thats a guarantee!!!

upvoted 3 times

danb67 1 year, 2 months ago

Selected Answer: A

I am not too sure about this one

https://learn.microsoft.com/en-us/azure/defender-for-cloud/working-with-log-analytics-agent#configure-the-log-analytics-agent-and-workspaces

I go with A - the below is from the above url

When the Log Analytics agent is on, Defender for Cloud deploys the agent on all supported Azure VMs and any new ones created. For the list of supported platforms, see Supported platforms in Microsoft Defender for Cloud.

To configure integration with the Log Analytics agent:

From Defender for Cloud's menu, open Environment settings.

Select the relevant subscription.

In the Monitoring Coverage column of the Defender plans, select Settings.

From the configuration options pane, define the workspace to use.

upvoted 2 times

jinxie 10 months, 2 weeks ago

looking at the question though, it already specifies that you have configured Defender for Cloud to use the workspace so in my mind that means step A has already been performed so why would you do that again? D would seem the obvious next step after

upvoted 1 times

Yaya 1 year, 2 months ago

The correct answer I think should be D (In workspace1, create a workbook).

To collect security event logs from the Azure virtual machines that report to workspace1, you can create a workbook in workspace1. A workbook is a collection of visualizations that allow you to analyse your data. You can create a workbook that visualizes the security event logs from your virtual machines.

upvoted 3 times

kabooze 1 year, 2 months ago

workbooks visualize, they don't collect logs

upvoted 5 times

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Adatum Corporation is a United States-based financial services company that has regional offices in New York, Chicago, and San Francisco.

Existing Environment -

Identity Environment -

The on-premises network contains an Active Directory Domain Services (AD DS) forest named corp.adatum.com that syncs with an Azure AD tenant named adatum.com. All user and group management tasks are performed in corp.adatum.com. The corp.adatum.com domain contains a group named Group1 that syncs with adatum.com.

Licensing Status -

All the users at Adatum are assigned a Microsoft 365 ES license and an Azure Active Directory Premium P2 license.

Cloud Environment -

The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.com tenant, and the resources shown in the following table.

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

On-premises Environment -

The on-premises network contains the resources shown in the following table.

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

Requirements -

Planned changes -

Adatum plans to perform the following changes:

• Implement a query named rulequery1 that will include the following KQL query.

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

• Implement a Microsoft Sentinel scheduled rule that generates incidents based on rulequery1.

Microsoft Defender for Cloud Requirements

Adatum identifies the following Microsoft Defender for Cloud requirements:

• The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
• Microsoft Defender for Servers Plan 2 must be enabled on all the Azure virtual machines.
• Server2 must be excluded from agentless scanning.

Microsoft Sentinel Requirements -

Adatum identifies the following Microsoft Sentinel requirements:

• Implement an Advanced Security Information Model (ASIM) query that will return a count of DNS requests that results in an NXDOMAIN response from Infoblox1.
• Ensure that multiple alerts generated by rulequery1 in response to a single user launching Azure Cloud Shell multiple times are consolidated as a single incident.
• Implement the Windows Security Events via AMA connector for Microsoft Sentinel and configure it to monitor the Security event log of Server1.
• Ensure that incidents generated by rulequery1 are closed automatically if Azure Cloud Shell is launched by the company's SecOps team.
• Implement a custom Microsoft Sentinel workbook named Workbook1 that will include a query to dynamically retrieve data from Webapp1.
• Implement a Microsoft Sentinel near-real-time (NRT) analytics rule that detects sign-ins to a designated break glass account.
• Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.
• Ensure that higher than normal volumes of password resets for corp.adatum.com user accounts are detected.
• Minimize the overhead associated with queries that use ASIM parsers.
• Ensure that the Group1 members can create and edit playbooks.
• Use built-in ASIM parsers whenever possible.

Business Requirements -

Adatum identifies the following business requirements:

• Follow the principle of least privilege whenever possible.
• Minimize administrative effort whenever possible.

You need to implement the Defender for Cloud requirements.

What should you configure for Server2?

A. the Microsoft Antimalware extension

B. the Azure Automanage machine configuration extension for Windows

C. an Azure resource lock

D. an Azure resource tag

Suggested Answer: *D*

Community vote distribution

D (100%)

Gurulee 6 months ago

Resource tag;
To configure agentless scanning for machines, select Edit configuration. Enter the tag name and tag value that applies to the machines that you want to exempt. You can enter multiple tag:value pairs.

upvoted 2 times

Pfui 6 months, 3 weeks ago

Selected Answer: D

correct

upvoted 3 times

ethhacker 7 months, 2 weeks ago

Correct - Server2 should be excluded from agentless scanning - therefore a tag is needed.

upvoted 3 times

[Removed] 7 months, 3 weeks ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms#exclude-machines-from-scanning

upvoted 1 times

Case study -

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study -
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview -

Adatum Corporation is a United States-based financial services company that has regional offices in New York, Chicago, and San Francisco.

Existing Environment -

Identity Environment -

The on-premises network contains an Active Directory Domain Services (AD DS) forest named corp.adatum.com that syncs with an Azure AD tenant named adatum.com. All user and group management tasks are performed in corp.adatum.com. The corp.adatum.com domain contains a group named Group1 that syncs with adatum.com.

Licensing Status -

All the users at Adatum are assigned a Microsoft 365 ES license and an Azure Active Directory Premium P2 license.

Cloud Environment -

The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.com tenant, and the resources shown in the following table.

Name	Type	Description
Sentinel1	Microsoft Sentinel workspace	Includes a custom hunting query named HuntingQuery1
Server2	Azure virtual machine	Runs Windows Server 2022

On-premises Environment -

The on-premises network contains the resources shown in the following table.

Name	Type	Description
Server1	Server	Runs Windows Server 2019 Has Azure Arc-enabled and the Azure Monitor agent installed
Webapp1	Web service	An on-premises, public-facing HTTP/HTTPS web service that generates JSON output in response to GET HTTP requests
Infoblox1	Infoblox DNS service	A third-party DNS service appliance linked to Sentinel1 by using a data connector

Requirements -

Planned changes -

Adatum plans to perform the following changes:

• Implement a query named rulequery1 that will include the following KQL query.

```
AzureActivity
| where ResourceProviderValue == "MICROSOFT.CLOUDSHELL"
| where ActivityStatusValue == "Start"
| extend
    Account_0_Name = tostring(split(Caller, '@', 0)[0]),
    Account_0_UPNSuffix = tostring(split(Caller, '@', 1)[0])
| project Account_0_Name, Account_0_UPNSuffix, CallerIpAddress, TimeGenerated
```

• Implement a Microsoft Sentinel scheduled rule that generates incidents based on rulequery1.

Microsoft Defender for Cloud Requirements

Adatum identifies the following Microsoft Defender for Cloud requirements:

• The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
• Microsoft Defender for Servers Plan 2 must be enabled on all the Azure virtual machines.
• Server2 must be excluded from agentless scanning.

Microsoft Sentinel Requirements -

Adatum identifies the following Microsoft Sentinel requirements:

• Implement an Advanced Security Information Model (ASIM) query that will return a count of DNS requests that results in an NXDOMAIN response from Infoblox1.
• Ensure that multiple alerts generated by rulequery1 in response to a single user launching Azure Cloud Shell multiple times are consolidated as a single incident.
• Implement the Windows Security Events via AMA connector for Microsoft Sentinel and configure it to monitor the Security event log of Server1.
• Ensure that incidents generated by rulequery1 are closed automatically if Azure Cloud Shell is launched by the company's SecOps team.
• Implement a custom Microsoft Sentinel workbook named Workbook1 that will include a query to dynamically retrieve data from Webapp1.
• Implement a Microsoft Sentinel near-real-time (NRT) analytics rule that detects sign-ins to a designated break glass account.
• Ensure that HuntingQuery1 runs automatically when the Hunting page of Microsoft Sentinel in the Azure portal is accessed.
• Ensure that higher than normal volumes of password resets for corp.adatum.com user accounts are detected.
• Minimize the overhead associated with queries that use ASIM parsers.
• Ensure that the Group1 members can create and edit playbooks.
• Use built-in ASIM parsers whenever possible.

Business Requirements -

Adatum identifies the following business requirements:

• Follow the principle of least privilege whenever possible.
• Minimize administrative effort whenever possible.

You need to implement the Defender for Cloud requirements.

Which subscription-level role should you assign to Group1?

A. Security Assessment Contributor

B. Contributor

C. Security Admin

D. Owner

Suggested Answer: *C*

Community vote distribution

D (66%) C (34%)

NeoTactics Highly Voted 6 months, 3 weeks ago

Selected Answer: D

It is 100% owner, because right should be assigned at subscription level. Not possible to use "Security Admin" on subscription level. Check: https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 7 times

Gurulee 6 months ago

Agreed; Security Admin cannot 'Add/assign initiatives (including) regulatory compliance standards)' at sub level: https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 1 times

LLLLL5 4 months, 1 week ago

according to your link security admin can.

upvoted 1 times

uday1985 1 month, 3 weeks ago

Security Admin has less privileges compared to the owner.

upvoted 1 times

DCT Highly Voted 6 months ago

Selected Answer: D

Questions had been mentioned Which "subscription-level role" should you assign to Group1?
So confirmed answer is D. Owner

upvoted 6 times

HAjouz Most Recent 3 weeks, 1 day ago

Selected Answer: C

Here's a breakdown of why this role is the most appropriate for Group1 based on the Adatum case study requirements:

Required Permissions: Group1 needs to be able to:

Enable Defender for Cloud plans (such as the Defender for Servers Plan 2).
Apply regulatory compliance initiatives.
Security Admin Role: The Security Admin role in Azure has the specific permissions required for these tasks. It allows users to manage security policies, enable and disable Defender for Cloud plans, and apply regulatory compliance initiatives.

Principle of Least Privilege: Assigning the Security Admin role adheres to the principle of least privilege. It grants the necessary permissions without providing excessive access like the Owner role would.

upvoted 1 times

KRISTINMERIEANN 2 months, 4 weeks ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 3 times

ostralo 3 months, 2 weeks ago

Selected Answer: D

Read the question carefully,
it is asking about Subscription-level role.
Security Admin and Owner both can do the tasks but it is asking a Sub-level role.
So Owner is correct.

upvoted 3 times

estyj 5 months ago

D: Only Owner can enable defender for cloud plans and apply regulatory compliance initiatives at subscription level.

upvoted 2 times

kazaki 5 months, 1 week ago

Selected Answer: C

Security admin
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 2 times

kazaki 5 months ago

i was wrong only owner can do on subscription level so it is D

upvoted 4 times

kazaki 5 months, 1 week ago

Security admin can do anything owner can do except exemption of policy
So security admin
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 3 times

CollabGuy 5 months, 2 weeks ago

Selected Answer: C

There are only 2 roles that can Add/assign initiatives: Security Admin and Owner.
As the exercise asks to follow the least priviledge principle, I'd go for Security Admin.
For people who look at https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions and say that Security Admin cannot be given at a Subscription level, please test it.
You can give a user any role at any level - https://learn.microsoft.com/en-us/azure/role-based-access-control/overview
The table in the first link just tries to show the difference between giving a Owner/Contributor at Resource Group level and Subscription level

If you give a user Security Admin Role, he will be able to do what the exercise requests and not more - contrary if we choose owner he can do anything.

upvoted 2 times

Gurulee 6 months ago

I chose Owner b/c:
The scenario states: "The cloud environment contains a Microsoft 365 subscription, an Azure subscription linked to the adatum.com tenant".
Therefore single subscription.
===
It is a best practice to assign Azure roles at the subscription level. This helps you to manage access control more efficiently and effectively. You can use Azure Role-Based Access Control (RBAC) to segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices#limit-privileged-administrator-role-assignments
===
Security Admin cannot 'Add/assign initiatives (including) regulatory compliance standards)' at sub level:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions

upvoted 1 times

Murtuza 6 months, 1 week ago

After reviewing it further and noticing that this question doesnt mention anything about •The members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives AT subscription level so OWNER doesnt apply. Secondly the business

requirement is least privilege access so in this case SECURITY admin is the correct answer
upvoted 1 times

Gurulee 6 months ago
Security Admin cannot 'Add/assign initiatives (including) regulatory compliance standards)' at sub level:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions#roles-and-allowed-actions
upvoted 1 times

Pfui 6 months, 3 weeks ago
Selected Answer: C
Secuirty Admin is correct
upvoted 1 times

Murtuza 6 months, 3 weeks ago
Review Question #50 the answer there is OWNER
Owner can "Add/assign initiatives (including) regulatory compliance standards" at subscription level
upvoted 2 times

DChilds 7 months ago
Selected Answer: C
According to this learning link, a Security Admin can perform the stated functions:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 2 times

ethhacker 7 months, 2 weeks ago
Selected Answer: D
Only user that can assign initiatives.

Owner is correct.
upvoted 3 times

ethhacker 7 months, 2 weeks ago
Sorry guys, due to this updated doc, Security ADMIN is right! https://learn.microsoft.com/en-us/azure/defender-for-cloud/permissions
upvoted 3 times

clary_meta 7 months, 3 weeks ago
Selected Answer: D
ANSWER: Owner
upvoted 2 times

clary_meta 7 months, 3 weeks ago
At subsciption level it will be: Owner
as the members of Group1 must be able to enable Defender for Cloud plans and apply regulatory compliance initiatives.
upvoted 2 times

Question #1 *Topic 3*

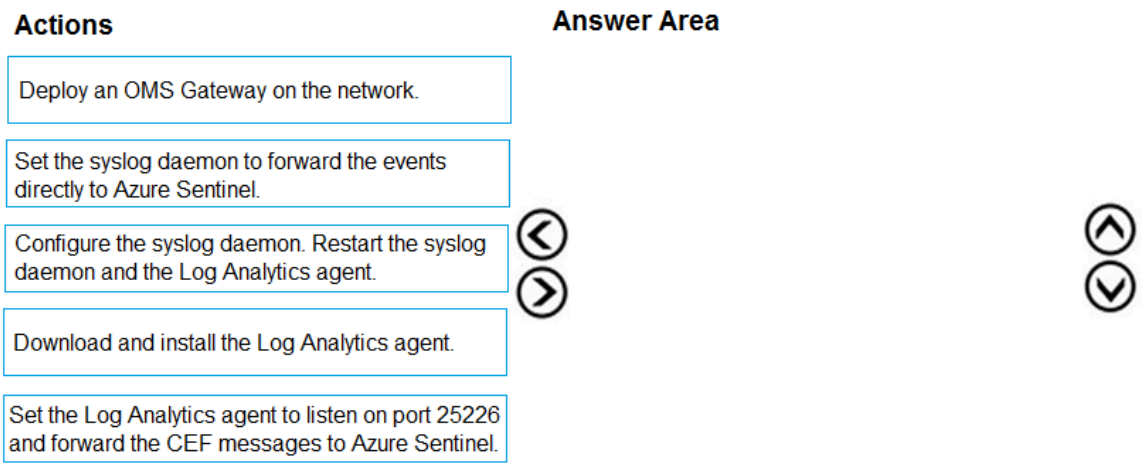
DRAG DROP -

You plan to connect an external solution that will send Common Event Format (CEF) messages to Azure Sentinel.

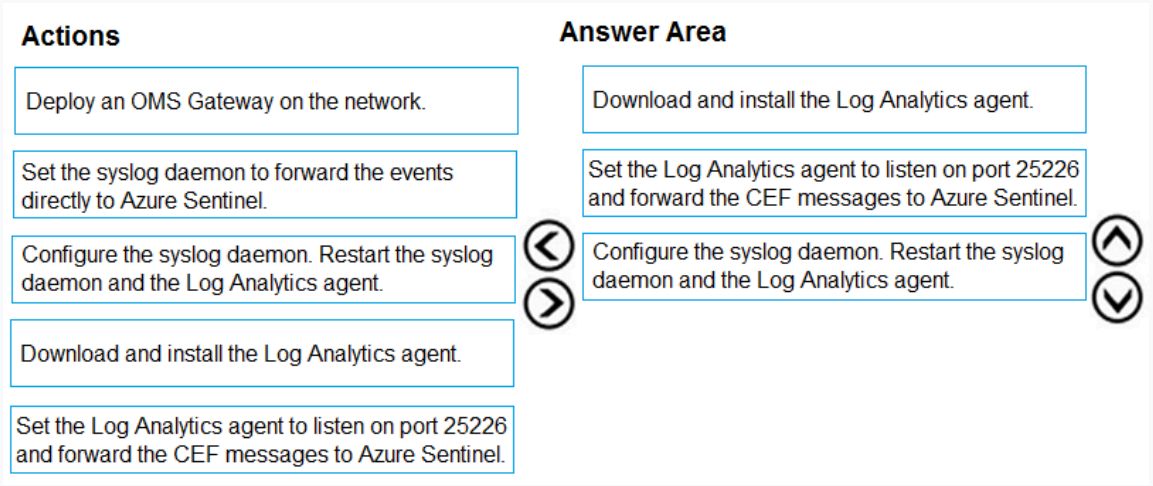
You need to deploy the log forwarder.

Which three actions should you perform in sequence? To answer, move the appropriate actions form the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/connect-cef-agent?tabs=rsyslog

somsom Highly Voted 3 years, 9 months ago

correct

upvoted 29 times

Ken88 Highly Voted 2 years, 9 months ago

Answer is correct

https://docs.microsoft.com/en-us/azure/sentinel/connect-common-event-format#designate-a-log-forwarder-and-install-the-log-analytics-agent

upvoted 13 times

Lion007 2 years, 6 months ago

Correct answer. From the link Ken88 provided:

1- Installs the Log Analytics agent for Linux (also known as the OMS agent) and configures it for the following purposes:
--- listening for CEF messages from the built-in Linux Syslog daemon on TCP port 25226
--- sending the messages securely over TLS to your Microsoft Sentinel workspace, where they are parsed and enriched

2- Configures the built-in Linux Syslog daemon (rsyslog.d/syslog-ng) for the following purposes:
--- listening for Syslog messages from your security solutions on TCP port 514

--- forwarding only the messages it identifies as CEF to the Log Analytics agent on localhost using TCP port 25226

The need for restarting the daemon and the agent is to ensure the changes take effect (on Linux this is required)
upvoted 12 times

VeiN Most Recent 2 months, 1 week ago
This is obsolite (maybe worth to learn ?).
Currently when using AMA with non azure machine (I assume since in description "external device")

The steps I`ve done on my lab:
1. Install Azure ARC on linux Forwarder (& connect to azure subscription)
2. Install connector: Common Event Format (CEF) via AMA
3. via connector : Create Data Collection Rule, add linux forwarder ARC object + configure log types to collected)
4. execute script on forwarder: sudo wget -O Forwarder_AMA_installer.py
upvoted 4 times

Sneekygeek 8 months, 3 weeks ago
Correct but log analytics will soon be deprecated. The new guides saw to the Azure Monitoring Agent
https://learn.microsoft.com/en-us/azure/sentinel/connect-cef-syslog-ama?tabs=single%2Csyslog%2Cportal
upvoted 2 times

Ramye 10 months, 1 week ago
Is this still valid now - now that a lot of changes happened in the last 2 yrs...
upvoted 1 times

stevenr868 5 months, 1 week ago
No, you now use an AMA agent
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

rupeshngp 1 year, 10 months ago
was in the exam today! The answer is correct!
upvoted 5 times

Anko6116 1 year, 10 months ago
Answer is correct according to below article:
https://learn.microsoft.com/en-us/azure/sentinel/connect-log-forwarder?tabs=rsyslog
upvoted 3 times

AJ2021 1 year, 10 months ago
Question in Exam today
upvoted 6 times

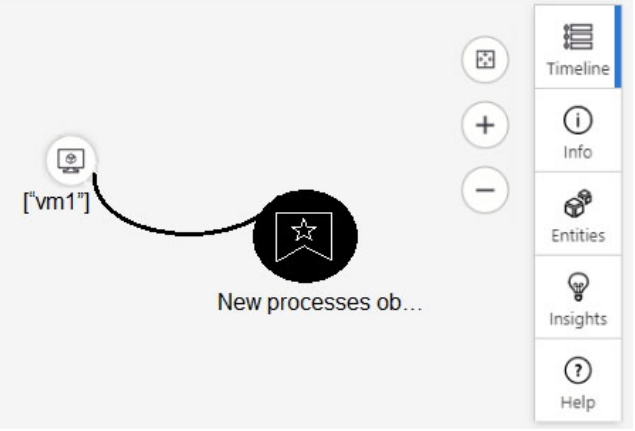
Eltooth 3 years, 3 months ago
Correct.
upvoted 6 times

invaderfr 3 years, 3 months ago
agree with answers
upvoted 5 times

Question #2 *Topic 3*

HOTSPOT -

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice],** you can navigate to the items related to the incident.

- Entities
- Info
- Insights
- Timeline

Suggested Answer:

Answer Area

If you hover over the virtual machine named vm1, you can view **[answer choice].**

- the inbound network security group (NSG) rules
- the last five Windows security log events
- the open ports on the host
- the running processes

If you select **[answer choice],** you can navigate to the items related to the incident.

- Entities
- Info
- Insights
- Timeline

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

Haz56 Highly Voted 2 years, 3 months ago

Definitely "Entities", as this button shows items in 3 sections: 1) Entities involved in the incident (user, device, IP etc.), 2) Alerts and 3) Bookmarks. These are the items associated with the incident.
upvoted 21 times

zaqwsx Highly Voted 2 years, 9 months ago
what is item? xD

IMO here can be also entities answer
upvoted 14 times

Jos8 2 years, 6 months ago
I think this is not correct because in this case, this is a Bookmark... and is like Remilia said: "In the Entities tab, you can see all the entities that you mapped as part of the alert rule definition."
upvoted 2 times

Harryd82 Most Recent 2 months ago
Running Processes

Entities
upvoted 2 times

MentalG 3 months, 3 weeks ago
Running Processes

Entities
upvoted 2 times

ApexPredator84 7 months ago
Second one has to be entities...I use sentinel everyday
upvoted 6 times

mc250616 7 months, 1 week ago
For second one I'll go with Entities for second.
upvoted 2 times

chepeerick 8 months, 1 week ago
Running and enteties
upvoted 3 times

danb67 8 months, 2 weeks ago
Processes
Entities

I use Sentinel in a production environment and just tested. If you click Entities then you see all the related entities. Simples.
upvoted 1 times

Fez786 10 months, 1 week ago
1. Running processes
2. Entities
upvoted 2 times

donathon 10 months, 1 week ago
Running processes and Entities
upvoted 2 times

Marchiano 11 months, 3 weeks ago
I'll go with Info for the 2nd one, and this is because this tab will appear automatically after clicking on any of the displayed processes. The other options are available as well, so we can't select all of them.
upvoted 2 times

Marchiano 11 months ago
changed my mind to Entities, all the items involved in the alert are displayed after selecting Entities
upvoted 1 times

mimguy 12 months ago
On the exam July 7 2023

upvoted 2 times

Whatsamattr81 1 year, 10 months ago

Difficult call... I'd go with Entities for the second one.

upvoted 4 times

Sorrynotsorry 2 years, 3 months ago

items are entities..

Correct answer is Processes and Entities

upvoted 8 times

Contactfornitish 2 years, 4 months ago

Timeline != Items

upvoted 2 times

josepedroche 2 years, 4 months ago

Correct answers: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-incident-timeline/ba-p/2267683

upvoted 1 times

Ana22 2 years, 4 months ago

Based on the provided URL the given answer seems correct.

upvoted 2 times

Question #3 *Topic 3*

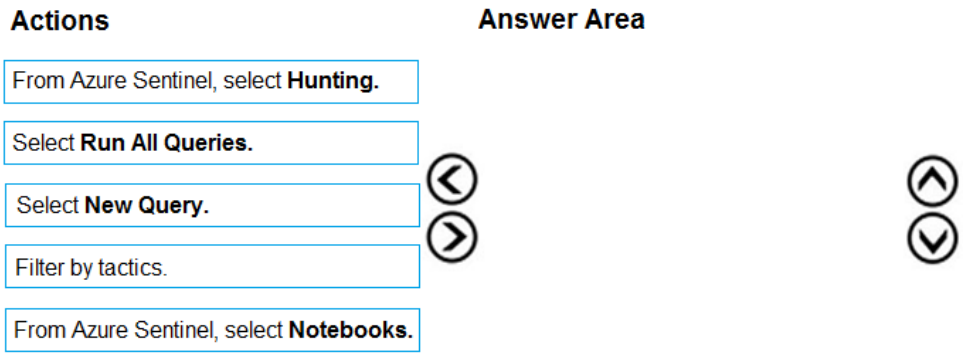
DRAG DROP -

You have an Azure Sentinel deployment.

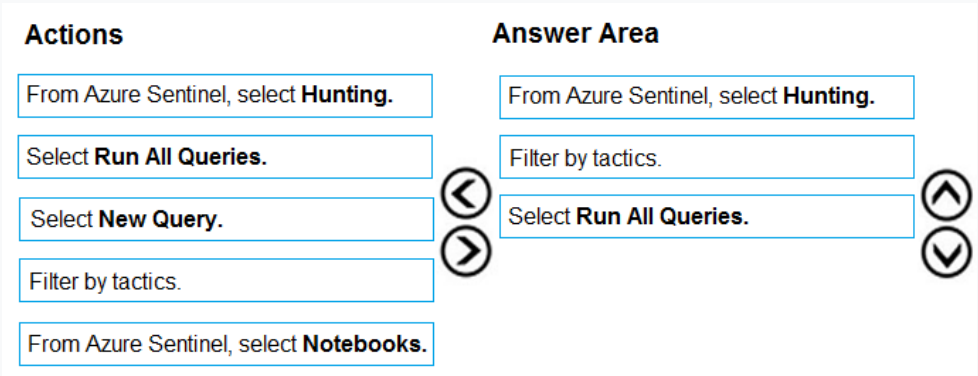
You need to query for all suspicious credential access activities.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Suggested Answer:



Reference:

https://davemccollough.com/2020/11/28/threat-hunting-with-azure-sentinel/

examkid Highly Voted 2 years, 5 months ago

Correct, in the hunting dashboard you can select the 'Credential Access' tactic

upvoted 19 times

rdy4u Highly Voted 1 year, 8 months ago

Microsoft Sentinel -> Hunting -> Add filter “Tactics”, select “Credential Access” -> Run All Queries

upvoted 12 times

chepeerick Most Recent 2 months, 1 week ago

Correct

upvoted 1 times

Marchiano 5 months, 3 weeks ago

Sentinel -> Hunting [1] -> Queries -> Credential Access (filter by tactics) [2] -> Run all queries [3]

upvoted 3 times

Lapatiser 1 year, 9 months ago

This is not correct. Its supposed to be select hunting -> select new query -> filter by tactics.

If you "filter by tactics" after "selecting hunting", the option available will be to "run selected queries" not "run all queries"

upvoted 2 times

StaxJaxson 1 year, 7 months ago

Microsoft Sentinel -> Hunting -> Add filter “Tactics”, select “Credential Access” -> Run All Queries

I have Sentinel and I'm looking at it now. This is exactly correct.

upvoted 15 times

Sik4nd4r 2 years, 6 months ago

Correct answer

upvoted 3 times

Question #4 *Topic 3*

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.
You deploy Azure Sentinel.
You need to use the existing logic app as a playbook in Azure Sentinel.
What should you do first?

A. And a new scheduled query rule.

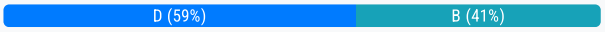
B. Add a data connector to Azure Sentinel.

C. Configure a custom Threat Intelligence connector in Azure Sentinel.

D. Modify the trigger in the logic app.

Suggested Answer: *B*

Community vote distribution



mmendozaf Highly Voted 3 years, 9 months ago
Personally i think that correct option is D.
upvoted 43 times

prabhjot 2 years, 9 months ago
yes as Logic app is already available and it pre configure to trigger manual based ... now when you connect it as Playbook you need to change the Trigger from manual to ..Sentinel based so Option is D
upvoted 9 times

Atun23 2 years, 2 months ago
But how do you search for that activation event if the logs aren't coming to sentinel? The key is "Fisrt", you need to get the events onboarded and then import the app or chanf the trigger.
upvoted 6 times

7c0a 1 year, 6 months ago
You are overcomplicating this question, You deploy Azure Sentinel which includes some connectors and related analytical rules. It's pretty sure D.
upvoted 3 times

JhnCanthern12 Highly Voted 3 years, 6 months ago
Some people are saying this is correct as a logic app connector, actually this is referring to that as you have literally just deployed Sentinel, you need to add the AAD Connector to get that in first before you do anything. Need the data there first.
upvoted 24 times

madhatter 3 years, 6 months ago
agreed, you are working with an already deployed logic app and you just created a NEW sentinel deployment. You need the AAD Connector to send the data first.

Provided answer "B" is correct.
upvoted 11 times

teehex 3 years, 5 months ago
No. There is nothing to do with AAD Connector. This is not about threat hunting against AAD. It is about how to integrate Azure Logic App to work with Azure Sentinel. You must modify existing Logic App and choose Azure Sentinel actions either the following ones:

- When a response to an Azure Sentinel Alert is triggered
- When Azure Sentinel incident creation rule was triggered
upvoted 12 times

PJR 3 years, 2 months ago
Before the alert can be triggered you need to ingest the source of the alert - ie connect Azure AD via a data connector.

Given answer is correct

upvoted 7 times

Tuitor01 Most Recent 3 weeks, 6 days ago

Selected Answer: D

If you think about it, this question is not even a technical question, it's more like a 'common sense' question. Answer D, your trigger is a manual trigger, I doubt it would be useful when triggered from a Playbook.

upvoted 1 times

wheeldj 8 months, 2 weeks ago

Selected Answer: D

Another poor question from MS I think. Define what 'deploy sentinel' means? if this implies you have literally just deployed a completely blank empty workspace then the answer is B.

But if "you deploy Sentinel" means you build the workspace with the basic connectors and config to start ingesting data, then D is the answer.

Working as a consultant if I told a customer I'd just 'Deployed Sentinel' but it had no data, no connectors, no rules I imagine they probably tell me to go back and finish the job!

So I'm voting D

upvoted 3 times

Sneekygeek 8 months, 3 weeks ago

Selected Answer: D

I was able to see my existing logic app under playbooks in Sentinel without creating a connector. Answer seems to be D

upvoted 1 times

Ramye 10 months, 1 week ago

Selected Answer: B

The Sentinel and AAD needs to integrate first before anything else, e.g. using the existing Logic App.

upvoted 1 times

estyj 11 months ago

B. It said you just deployed Sentinel, so you have to add data connector to allow communication first before you can modify trigger for the alert.

upvoted 2 times

ing_magc 11 months, 2 weeks ago

the D is correct

upvoted 1 times

estyj 11 months, 3 weeks ago

Think it is B. You have just deployed sentinel. Have to able to communicate to Sentinel first so need to add data connector before you can modify trigger in logic app.

upvoted 1 times

chepeerick 1 year, 2 months ago

D for me

upvoted 1 times

danb67 1 year, 2 months ago

Selected Answer: B

B for me

upvoted 1 times

mali1969 1 year, 3 months ago

Selected Answer: D

D. Modify the trigger in the logic app.

To use an existing logic app as a playbook in Azure Sentinel, you need to change the trigger from manual to When a response to an Azure Sentinel alert is triggered or When a response to an Azure Sentinel incident is triggered. This will allow the logic app to run automatically when an alert or incident occurs in Azure Sentinel.

upvoted 1 times

donathon 1 year, 4 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/sentinel/playbook-triggers-actions

The answers are split between B and D. I will go for D because I think the AAD is already connected to the logic app. Whether AAD is connected to

seninel or not does not really matters since the question is asking to add the logic app as a playbook. Which means D make more sense.
upvoted 2 times

promto 1 year, 6 months ago

Selected Answer: D

trigger
upvoted 1 times

haskelatchi 1 year, 8 months ago

Selected Answer: B

Everyone the answer is B, confirmed and tested. Let me explain:

Adding a data connector to Azure Sentinel is the first step to use the existing logic app as a playbook in Azure Sentinel. The data connector allows Azure Sentinel to trigger the Logic App as part of a playbook. Once the data connector is added, you can proceed to modify the trigger in the Logic App to ensure that it can be invoked by Azure Sentinel.

It's important to note that modifying the trigger in the Logic App (option D) is also a crucial step in the process. However, based on the provided information, adding a data connector (option B) should be the first step.
upvoted 4 times

evilprime 1 year, 9 months ago

asked gpt the exact question with the exact answers to choose from, it has chosen B
upvoted 1 times

wsrudmen 1 year, 10 months ago

Selected Answer: B

It's B

It's an exising logic App. If you want to modify the trigger, you will not find any trigger related to Sentinel (tested in lab). You have to add the connector before seeing the Sentinel Trigger.

NB: For Playbook created directly in Sentinel, everything is done by default.
upvoted 4 times

Question #5 *Topic 3*

Your company uses Azure Sentinel to manage alerts from more than 10,000 IoT devices.
A security manager at the company reports that tracking security threats is increasingly difficult due to the large number of incidents.
You need to recommend a solution to provide a custom visualization to simplify the investigation of threats and to infer threats by using machine learning.
What should you include in the recommendation?

A. built-in queries

B. livestream

C. notebooks

D. bookmarks

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Community vote distribution
C (100%)

sommy Highly Voted 3 years, 9 months ago
notebooks are for visualization
upvoted 7 times

a1dfaaa Most Recent 5 months, 2 weeks ago
Selected Answer: C
C is correct
upvoted 1 times

chepeerick 1 year, 2 months ago
Correct C
upvoted 2 times

Apocalypse03 2 years ago
Selected Answer: C
Jupyter notebooks allow you to supercharge your threat hunting and investigation by enabling documents that contain live code, visualizations, and narrative text. These documents can be codified and served for specialized visualizations, an investigation guide, and sophisticated threat hunting.

Additionally, notebooks can be used in security big data analytics for fast data processing on large datasets.
upvoted 4 times

Lion007 2 years, 6 months ago
Correct answer. Visualization + Machine Learning = Notebooks
upvoted 4 times

prabhjot 2 years, 9 months ago
Yes Data Scientist use Jupyter Note book (Python code) - worj with ML tools
so Ans is Notebook
upvoted 3 times

Tx4free 2 years, 10 months ago
Selected Answer: C
Best option
upvoted 3 times

Eltooth 3 years, 3 months ago
Correct - Notebooks
upvoted 3 times

somsom 3 years, 9 months ago

correct

upvoted 3 times

Question #6 *Topic 3*

You have a playbook in Azure Sentinel.
When you trigger the playbook, it sends an email to a distribution group.
You need to modify the playbook to send the email to the owner of the resource instead of the distribution group.
What should you do?

A. Add a parameter and modify the trigger.

B. Add a custom data connector and modify the trigger.

C. Add a condition and modify the action.

D. Add an alert and modify the action.

Suggested Answer: *D*
Reference:
https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/

Community vote distribution
A (38%) D (36%) C (26%)

Walaakb Highly Voted 1 year, 9 months ago
am I the only one that thinks its C ?????
upvoted 19 times

teehex Highly Voted 3 years, 6 months ago
The answer is correct. You need to add a new parameter in Send email action. That parameter specifies who you want to send to.
upvoted 15 times

Lion007 2 years, 6 months ago
Should the answer be A then, not D?
upvoted 5 times

Lion007 2 years, 6 months ago
Because the question states that there is already an alert that "sends an email to a distribution group", you should add a parameter and modify the existing one, right? I would go for A instead.
upvoted 4 times

ariania 2 years, 6 months ago
i think its because you dont want to modify the trigger, rather the action.
upvoted 1 times

Ramye 10 months, 2 weeks ago
why would you add another parameter? The question asked the email would go to Ownere rather than to a DL, so somehow the existing parameter needs to be updated, so the email only goes to the owner. Honestly not quite certain what would be the answer but am leaning toward C.
upvoted 2 times

D_PaW 1 year, 7 months ago
If you're just "replacing" the recipient when why would you "add a parameter"?? There is already one for the DL, just "replace" it's??
upvoted 2 times

talosDevbot Most Recent 2 months, 2 weeks ago
Selected Answer: C
Answer is C.

Your goal is to send it to the owner of the resource. So you can use multiple Condition statements in your Logic App workflow to achieve this.

https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-control-flow-conditional-statement?tabs=standard
upvoted 2 times

user636 4 months, 1 week ago
Selected Answer: A

Playbook is just a logic app. The trigger is already configured, so just add a parameter & use it in the action later.
upvoted 2 times

Sekpluz 6 months, 3 weeks ago

Selected Answer: A

To modify the playbook to send an email to the owner of the resource instead of the distribution group, you should choose Option A: Add a parameter and modify the trigger.

In Azure Sentinel, a playbook is essentially a Logic App. To change the recipient of the email, you would need to modify the action that sends the email. This can be done by adding a parameter to the action that specifies the owner of the resource as the recipient.

The trigger of the Logic App determines when the Logic App is run. If the trigger is currently set to run when an alert is generated, you would not need to modify the trigger to change the recipient of the email. However, if the trigger is not currently set to run when the resource owner changes, you would need to modify the trigger as well.
upvoted 3 times

oricgoldfinger 9 months, 1 week ago

Selected Answer: C

This should be C
upvoted 2 times

luisM14 11 months, 2 weeks ago

Selected Answer: A

A is the correct!!
https://techcommunity.microsoft.com/t5/microsoft-security-experts-blog/forensic-artifacts-in-office-365-and-where-to-find-them/ba-p/3634865
upvoted 1 times

CollabGuy 11 months, 2 weeks ago

Selected Answer: A

In order to save the email of the owner of that resource, we need to use a parameter. A is the only option that mentions the parameter.
upvoted 1 times

chepeerick 1 year, 2 months ago

Correct
upvoted 1 times

danb67 1 year, 2 months ago

Selected Answer: C

I have a playbook like this in my lab. The Condition>Action is where we tell the playbook that we want it to email out and who we want to email it out to. So if you edit the condition and then the action we can change who gets the email when the playbook is triggered.
upvoted 9 times

mali1969 1 year, 4 months ago

To modify the playbook to send the email to the owner of the resource instead of the distribution group, you should do the following:

Add a parameter and modify the trigger. This option allows you to define a custom value that the playbook uses, such as the email address of the resource owner. You can then use this parameter in the trigger condition or in the action settings4.
Add a condition and modify the action. This option allows you to check if the alert is related to the resource owner and then send an email to them using the Office 365 Outlook connector.
The other two options are not correct because:

Adding a custom data connector and modifying the trigger will not change the email recipient, but rather create a new source of data for Azure Sentinel.
Adding an alert and modifying the action will not change the email recipient, but rather create a new alert based on a condition or logic app action.
upvoted 3 times

mali1969 1 year, 3 months ago

Correct answer is C
To modify the playbook to send the email to the owner of the resource instead of the distribution group, you should do the following:

C. Add a condition and modify the action.
A condition is a logic app expression that evaluates to true or false. You can use conditions to control the flow of your playbook based on

certain criteria2. For example, you can add a condition that checks the owner of the resource from the alert or incident properties, and then use that value to modify the action that sends the email.

upvoted 3 times

donathon 1 year, 4 months ago

Selected Answer: A

I would think A make more sense then D since the question wants to change the email recipient and not add a new one. So changing the Trigger is required.

upvoted 2 times

donathon 1 year, 3 months ago

https://learn.microsoft.com/en-us/azure/sentinel/use-playbook-templates#customize-a-playbook-from-a-template >> Look under parameters. The notification email is there.

upvoted 1 times

danb67 1 year, 2 months ago

The answer this is not A. Why would we modify the trigger? I have a playbook like this in my lab. The Condition is where we tell the playbook that we want it to email out and who we want to email it out to. So if you edit the condition and then the action we can change who gets the email when the playbook is triggered.

upvoted 1 times

danb67 1 year, 2 months ago

Answer is therefore C

upvoted 1 times

donathon 1 year, 3 months ago

Remember the question asked to modify the playbook. Playbook does not have alerts.

upvoted 1 times

EM1234 1 year, 5 months ago

Selected Answer: D

It is D. Just go build a playbook.
https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents

The trigger would not need to change. So you are left with C and D. Adding a condition will not help you email the resource owner but an alert will.

You add a new alert that includes the resource owner and then set the action to use that alert based on the condition and trigger that were already working.

upvoted 4 times

D_PaW 1 year, 7 months ago

Selected Answer: C

I would Agree with @So_Surreall on this one. The most professional answer would be to validate is the owner is defined and send to it. If no owner is defined then send to the DL...

upvoted 4 times

[Removed] 1 year, 8 months ago

C. Add a condition and modify the action.

To modify the playbook to send the email to the owner of the resource instead of the distribution group, you need to add a condition to check whether the resource has an owner, and then modify the action to send the email to the owner.

Here are the steps to do this:

In the Azure Sentinel portal, open the playbook that you want to modify.
Add a condition to check whether the resource has an owner. You can use the "Get-AzureADObjectOwner" PowerShell command to get the owner of the resource. If the owner exists, continue to the next step. Otherwise, exit the playbook.
Modify the action to send the email to the owner of the resource. You can use the "Send Email" action to send an email to the owner of the resource.
By adding this condition and modifying the action, you can ensure that the email is sent to the owner of the resource instead of the distribution group.

upvoted 9 times

Ramye 10 months, 1 week ago

C makes sense. by doing this you are not adding any new parameter or anything.

upvoted 1 times

evilprime 1 year, 9 months ago

chatgpt says 'C' based on the exact question and exact answers..

upvoted 4 times

exmITQS 1 year, 10 months ago

Selected Answer: A

A. Add a parameter and modify the trigger.

To modify the playbook to send the email to the owner of the resource instead of the distribution group, you should add a parameter to the playbook that specifies the owner's email address. This will allow you to pass the email address as a parameter when you trigger the playbook.. Option B, adding a custom data connector, is not relevant to the task of modifying the playbook to send the email to the owner of the resource.

Option C, adding a condition and modifying the action, may be necessary if there are specific conditions that need to be met before sending the email to the owner of the resource, but it is not the first step in the process.

Option D, adding an alert and modifying the action, is also not relevant to the task of modifying the playbook to send the email to the owner of the resource.

upvoted 4 times

Question #7 *Topic 3*

You provision Azure Sentinel for a new Azure subscription.

You are configuring the Security Events connector.

While creating a new rule from a template in the connector, you decide to generate a new alert for every event.

You create the following rule query.

```
let timeframe = 1d;
SecurityEvent
| where TimeGenerated >= ago(timeframe)
| where EventID == 1102 and EventSourceName == "Microsoft-Windows-Eventlog"
| summarize StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated),
EventCount = count() by
Computer, Account, EventID, Activity
| extend timestamp = StartTimeUtc, AccountCustomEntity = Account,
HostCustomEntity = Computer
```

By which two components can you group alerts into incidents? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. user

B. resource group

C. IP address

D. computer

Suggested Answer: *CD*

Community vote distribution

AD (83%) CD (17%)

hyperion Highly Voted 3 years ago

Answer should be A, D. IP address data is removed from the query in the | summarize, and is not mapped to the IP custom entity.

upvoted 62 times

madperro 2 years, 7 months ago

Correct answer.

upvoted 1 times

NoNameP Highly Voted 2 years, 11 months ago

Correct answer A, D.

upvoted 10 times

Harryd82 Most Recent 2 months ago

A & D is correct

upvoted 1 times

chepeerick 8 months, 1 week ago

A and D as IP is removed

upvoted 1 times

jamclash 9 months, 2 weeks ago

in exam 9/20/23

upvoted 1 times

RV025 10 months, 1 week ago

Selected Answer: AD

"user" should be replaced with Account

upvoted 3 times

exmITQS 1 year, 4 months ago

Selected Answer: AD

A. user and D. computer.

To group alerts into incidents in Azure Sentinel, you can use any combination of the available grouping fields. In this case, since the rule query does not include information on resource groups or IP addresses, only user and computer can be used to group alerts into incidents.

Grouping alerts by user and computer can help you identify patterns of activity and better understand the scope and impact of potential security threats. By grouping alerts into incidents, you can also more easily manage and track your response to security incidents.

upvoted 5 times

Apocalypse03 1 year, 6 months ago

Selected Answer: AD

To group alerts into incidents in Azure Sentinel, you can use the "user" and "computer" components in the rule query.

upvoted 2 times

sainfosec 1 year, 11 months ago

Selected Answer: AD

AD correct

upvoted 2 times

Dumisoph 1 year, 11 months ago

A&D is Correct

upvoted 1 times

ariania 1 year, 12 months ago

Added the script to a analytic rule and get "Account" and "Host" as only options.

upvoted 1 times

M20200713 2 years, 2 months ago

Selected Answer: AD

Thinking top AD also

upvoted 1 times

Fishman22222 2 years, 2 months ago

Selected Answer: AD

A and D

upvoted 1 times

Muffen 2 years, 3 months ago

Selected Answer: AD

IP is not returned in the query. We can see that the Account and Computer were mapped to entities and were returned in the 'summarize' section.

upvoted 2 times

Tx4free 2 years, 3 months ago

Selected Answer: AD

You can group by user and computer

upvoted 1 times

Tx4free 2 years, 3 months ago

Selected Answer: AD

Best answer

upvoted 1 times

haykaybam 2 years, 3 months ago

Selected Answer: AD

Answer should be A and D. User and Host (computer)

upvoted 1 times

Question #8 *Topic 3*

Your company stores the data of every project in a different Azure subscription. All the subscriptions use the same Azure Active Directory (Azure AD) tenant.
Every project consists of multiple Azure virtual machines that run Windows Server. The Windows events of the virtual machines are stored in a Log Analytics workspace in each machine's respective subscription.
You deploy Azure Sentinel to a new Azure subscription.
You need to perform hunting queries in Azure Sentinel to search across all the Log Analytics workspaces of all the subscriptions.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add the Security Events connector to the Azure Sentinel workspace.

B. Create a query that uses the workspace expression and the union operator.

C. Use the alias statement.

D. Create a query that uses the resource expression and the alias operator.

E. Add the Azure Sentinel solution to each workspace.

Suggested Answer: *BE*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Community vote distribution
BE (59%) AB (29%) 12%

Eltooth Highly Voted 3 years, 3 months ago
Correct - every sentinel deployment must have a workspace - and the union command is used to join multiple workspaces together.
upvoted 23 times

Shared 2 years ago
Well option E says to add Sentinel, which seems to be wrong as there can be 1 Sentinel/tenant and works across subscriptions:
https://github.com/MicrosoftDocs/azure-docs/issues/85443
https://techcommunity.microsoft.com/t5/microsoft-sentinel/azure-sentinel-instances-per-subscription/m-p/2278936
upvoted 1 times

Ramye 10 months, 1 week ago
Actually, E says --> Add the Azure Sentinel solution to each workspace. And, having multiple workspaces for Sentinel in a tenant is very much doable, and in some cases, it is recommended, i.e. different regions or projects, for easier management. In this question, there are different projects in each Azure subscription so having Sentinel solutions in those workspaces makes sense.
upvoted 3 times

xRiot007 Most Recent 4 weeks ago
Selected Answer: BE
Answer is B and E - you install sentinel on each workspace and then query using an union. An alternative to this is to use Azure Lighthouse.
upvoted 1 times

talosDevbot 3 months ago
100% the answer is B and E
It's stated in Microsoft's documentation: https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Under the "Include cross-workspace queries in scheduled analytics rules" section:
"You must deploy Microsoft Sentinel on every workspace referenced in the query."

Under the "Hunt across multiple workspaces" section:
"Cross-workspace hunting capabilities enable your threat hunters to create new hunting queries, or adapt existing ones, to cover multiple workspaces, by using the union operator and the workspace() expression as shown above."
upvoted 2 times

4rk4n4 10 months ago

Selected Answer: BE

B AND E

upvoted 1 times

chepeerick 1 year, 2 months ago

Correct BE

upvoted 1 times

mali1969 1 year, 3 months ago

B and C. Here is why:

Option B is correct because you can query multiple workspaces in a single query by using the workspace() expression to refer to a table in a different workspace and the union operator to combine the results from multiple tables.
Option C is correct because you can use the alias statement to simplify cross-workspace queries by saving a long reference to a table in another workspace as a function.

Option A is not correct because adding the Security Events connector to the Azure Sentinel workspace does not enable you to query across multiple workspaces.

Option D is not correct because there is no such thing as the resource expression or the alias operator in Kusto Query Language (KQL)

Option E is not correct because adding the Azure Sentinel solution to each workspace does not allow you to perform cross-workspace hunting queries.

upvoted 1 times

emv 1 year, 3 months ago

You can include up to 20 workspaces in a single query. However, for good performance, we recommend including no more than 5.
You must deploy Microsoft Sentinel on every workspace referenced in the query.

upvoted 1 times

donathon 1 year, 4 months ago

Selected Answer: BE

According to the URL in the answer:
Use the union operator alongside the workspace( ) expression to apply a query across tables in multiple workspaces.
You must deploy Microsoft Sentinel on every workspace referenced in the query.

upvoted 1 times

EM1234 1 year, 5 months ago

Selected Answer: AB

I see no reason why you would need more sentinel instances. Follow the design decision tree here:
https://learn.microsoft.com/en-us/azure/sentinel/design-your-workspace-architecture#decision-tree
I think B is obviously part of the solution. The question is what other choice. I am going with A. It makes more sense to me than making additional Sentinel instances.

I wonder if you made all of them, which one would you be hunting in?

A and B for me.

upvoted 2 times

Mducks 10 months, 3 weeks ago

Given answer is correct.
https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants
Copied and pasted 4 sentences directly from link above:
You can query multiple workspaces, allowing you to search and correlate data from multiple workspaces in a single query.
Use the workspace( ) expression, with the workspace identifier as the argument, to refer to a table in a different workspace.
Use the union operator alongside the workspace( ) expression to apply a query across tables in multiple workspaces.
You must deploy Microsoft Sentinel on every workspace referenced in the query.

upvoted 1 times

evilprime 1 year, 9 months ago

chatgpt says 'B E' using exact question with given answers.
E. You need to add the Azure Sentinel solution to each Log Analytics workspace that you want to search. This allows Azure Sentinel to collect

data from the workspace and store it in the Azure Sentinel workspace.
upvoted 1 times

mangali84 1 year, 9 months ago
what is chatgpt? if i am ask.
upvoted 4 times

exmITQS 1 year, 10 months ago
Selected Answer: BD
. Create a query that uses the workspace expression and the union operator, and D. Create a query that uses the resource expression and the alias operator
Create a query that uses the workspace expression and the union operator to combine the data from all the Log Analytics workspaces. For example:
union *
| where TimeGenerated > ago(1d)
Create a query that uses the resource expression and the alias operator to query data from specific resources across all the subscriptions. For example
AzureActivity
| where ResourceProviderValue == "Microsoft.Compute"
| where OperationNameValue == "Microsoft.Compute/virtualMachines/delete"
| project SubscriptionId, ResourceGroup, Resource, Caller, TimeGenerated, ActivityStatus
| summarize count() by Resource
upvoted 2 times

daba_fcb 1 year, 10 months ago
Selected Answer: AB
I think it's A B,
A - security events connector is called "Security events via legacy agent" and it's Legacy version based on the Microsoft Monitor Agent / Log Analytics" and the question states that windows events of the VM's are stored in a log analytics workspace. Reference:
https://jeffreyappel.nl/collect-security-events-in-sentinel-with-the-new-ama-agent-and-dcr/
upvoted 3 times

[Removed] 1 year, 10 months ago
Should the answer include a data connector if it is a new Sentinel?
upvoted 1 times

Windy232 2 years ago
Your company has an Azure subscription that hosts resources in multiple Azure regions in different countries.
What are two primary drawbacks of implementing single-tenant with regional workspaces Microsoft Sentinel in your environment as compared to the single-tenant single workspace option? Each correct answer presents part of the solution.

Limited support for querying data across workspaces
Increased cost of network bandwidth
Lack of a single pane of glass
Increased cost of compute services
Increased deployment complexity
upvoted 1 times

Windy232 2 years ago
Which one should be chose?
Thanks all
upvoted 1 times

Cho 1 year, 10 months ago
I would choose increased cost and increased deployment complexity.
upvoted 2 times

midaoui 1 year, 11 months ago
I would answer:
- Lack of a single pane of glass
- Increased deployment complexity
https://charbelnemnom.com/top-best-practices-for-deploying-azure-sentinel/
upvoted 1 times

danb67 1 year, 2 months ago

According to the url you have provided its

Limited support for querying data accross workspaces
Lack of a single pane of glass

upvoted 1 times

Apocalypse03 2 years ago

Selected Answer: BE

let subscriptions = [subscription1, subscription2, ...];
union withsource=source
(
workspace("workspace1").SecurityEvent | where TimeGenerated >= ago(1d),
workspace("workspace2").SecurityEvent | where TimeGenerated >= ago(1d),
...
)

upvoted 1 times

AMZ 2 years, 2 months ago

Questions states, "All the subscriptions use the same Azure Active Directory (Azure AD) tenant" - from MS - Multiple Azure tenants Microsoft Sentinel supports data collection from Microsoft and Azure SaaS resources only within its own Azure Active Directory (Azure AD) tenant boundary. Therefore, each Azure AD tenant requires a separate workspace.

Since we are using the same AD the answer should be A and B.

Also it would be a pain to manage all these Sentinel instances.

https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

upvoted 4 times

Fukacz 2 years, 3 months ago

Selected Answer: BE

Correct. LAs need sentinels and then query with union

upvoted 1 times

Question #9 *Topic 3*

You have an Azure Sentinel workspace.
You need to test a playbook manually in the Azure portal.
From where can you run the test in Azure Sentinel?

A. Playbooks

B. Analytics

C. Threat intelligence

D. Incidents

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

Community vote distribution
D (64%) A (36%)

HSBNZ Highly Voted 3 years, 4 months ago
Manual triggering is available from the Azure Sentinel portal in the following blades:

In Incidents view, choose a specific incident, open its Alerts tab, and choose an alert.

In Investigation, choose a specific alert.

Click on View playbooks for the chosen alert. You will get a list of all playbooks that start with an When an Azure Sentinel Alert is triggered and that you have access to.

Click on Run on the line of a specific playbook to trigger it.

Select the Runs tab to view a list of all the times any playbook has been run on this alert. It might take a few seconds for any just-completed run to appear in this list.

Clicking on a specific run will open the full run log in Logic Apps.
upvoted 26 times

palito1980 Highly Voted 1 year, 11 months ago
Selected Answer: D
Clearly says to go to Incidents first.
https://learn.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC%2Cincidents#run-a-playbook-manually-on-an-alert
upvoted 8 times

EM1234 1 year, 5 months ago
I did not mean to upvote this. Where in the question does it say there has been an alert? Did you just add that in?
upvoted 1 times

EM1234 1 year, 5 months ago
also, where does it say first?
upvoted 1 times

EM1234 1 year, 5 months ago
I do not like this question and D is a good choice but when I read the specific doc about testing playbooks (which I had not seen anyone link yet):
https://learn.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks#run-a-playbook-manually

I see you can test the playbook three ways:
To run a playbook on a specific incident

To run a playbook on an alert
To run a playbook on an entity
upvoted 4 times

EM1234 1 year, 5 months ago
Sorry I did not mean to hit submit yet, I will continue.

So I see three ways to test but then this sentence:

In any of these panels, you'll see two tabs: Playbooks and Runs.

So then, I think in this poorly worded question you actually do click on "playbooks" to test.

If I see this on the exam I am not sure which one I would choose, it could be a lot more clear than it is IMO.
upvoted 1 times

talosDevbot Most Recent 3 months ago
Selected Answer: D
Sentinel > Incidents > click on an incident > Actions > Run Playbook
upvoted 1 times

Ramye 10 months, 1 week ago
Selected Answer: D
Confirmed from SC-200 Microsoft Practice Assessment

https://learn.microsoft.com/en-us/credentials/certifications/exams/sc-200/practice/assessment?assessment-type=practice&assessmentId=59
upvoted 6 times

xoe123 11 months, 1 week ago
You can test a playbook manually in Azure Sentinel from both A. Playbooks and B. Incidents.

A. Playbooks: You can run a playbook directly from the Playbooks blade in Azure Sentinel. This allows you to test the playbook independently of any incident or alert.

B. Incidents: You can also run a playbook from an incident in Azure Sentinel. This allows you to test the playbook in the context of a specific incident.
upvoted 1 times

estyj 11 months, 3 weeks ago
D: Incidents https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/run-microsoft-sentinel-playbooks-from-workbooks-on-demand/ba-p/3193074
upvoted 1 times

chepeerick 1 year, 2 months ago
Option A
upvoted 1 times

danb67 1 year, 2 months ago
Selected Answer: D
D for me. Click on an incident then click on action and then run playbook
upvoted 1 times

mali1969 1 year, 4 months ago
Selected Answer: A
The answer is A. Playbooks.

Playbooks are logic apps that allow you to automate and orchestrate your threat response in Azure Sentinel. You can create playbooks from templates or from scratch, and assign them to alerts or incidents to run automatically when triggered by an automation rule. You can also run playbooks manually on-demand, on a particular entity or alert, to test their functionality or perform a specific action.
upvoted 3 times

Ramye 10 months, 1 week ago

But the questions asked ---> From where can you run the test in Azure Sentinel?
Your last sentence says - the answer is Incident.
upvoted 1 times

Anil0512 1 year, 3 months ago
bang on answer, cheers
upvoted 1 times

donathon 1 year, 4 months ago
Selected Answer: A
In the Playbooks tab, you'll see a list of all the playbooks that you have access to and that use the appropriate trigger - whether Microsoft Sentinel Incident, Microsoft Sentinel Alert, or Microsoft Sentinel Entity. Each playbook in the list has a Run button which you select to run the playbook immediately.
upvoted 3 times

sergioandreslq 3 months ago
Agree:
In Microsoft Sentinel, you can manually test a playbook from the "Playbooks" blade. Here's how to do it:

1. Navigate to Microsoft Sentinel in the Azure portal.
2. Select the appropriate workspace.
3. In the left-hand menu, click on "Configuration" and then select "Playbooks."
4. Find the playbook you want to test and click on it to open its details.
5. At the top, you'll see an option to "Run playbook." Click this to start a manual test.

upvoted 1 times

itsadel 1 year, 5 months ago
Selected Answer: D
correct
upvoted 1 times

mimguy 1 year, 5 months ago
On the exam July 7 2023
upvoted 1 times

evilprime 1 year, 9 months ago
i think keyword is here is "test" why test a playbook on a actual incident.. go to playbooks and from there you can test it.
upvoted 1 times

7c0a 1 year, 6 months ago
Cause you need parameters(an array with entities), which are provided by the Sentinel trigger.
Please stop using chatGPT for this matter, it is very unreliable approach, ChatGPT is good for other things, like generating basic code for most common/popular scenarios and languages, doing conversions, parsing, etc...
upvoted 4 times

exmITQS 1 year, 10 months ago
Selected Answer: A
A. Playbooks.

To test a playbook manually in Azure Sentinel, you can use the "Test" feature in the Playbooks section of the Azure Sentinel workspace.

To do this, navigate to the Azure Sentinel workspace in the Azure portal, click on "Playbooks" in the left-hand menu, and then select the playbook that you want to test. From there, click the "Test" button at the top of the page
upvoted 4 times

billo79152718 1 year, 6 months ago
You give chatgpt answers everytime. So many people here have commented on your alomst every time incorrect answers.
upvoted 6 times

teouba 1 year, 11 months ago
Selected Answer: A
You can run the test in Azure Sentinel from the "Playbooks" blade.
upvoted 4 times

kushagrasharma172 2 years ago

Given answer is correct. Option D

upvoted 1 times

subhuman 2 years, 10 months ago

Selected Answer: D

Answer is Correct

upvoted 2 times

Question #10 *Topic 3*

You have a custom analytics rule to detect threats in Azure Sentinel.
You discover that the analytics rule stopped running. The rule was disabled, and the rule name has a prefix of AUTO DISABLED.
What is a possible cause of the issue?

A. There are connectivity issues between the data sources and Log Analytics.

B. The number of alerts exceeded 10,000 within two minutes.

C. The rule query takes too long to run and times out.

D. Permissions to one of the data sources of the rule query were modified.

Suggested Answer: *D*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

Community vote distribution
D (85%) Other

PJR Highly Voted 3 years, 7 months ago
D - https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#issue-a-scheduled-rule-failed-to-execute-or-appears-with-auto-disabled-added-to-the-name
upvoted 16 times

g_man_rap 4 months, 1 week ago
somebody checked this link? is nothing about AUTO DISABLED or permissions? please check
upvoted 3 times

subhuman Highly Voted 2 years, 9 months ago
Selected Answer: D
Correct answer is D
Permanent failure - rule auto-disable due to the following reasons
The target workspace (on which the rule query operated) has been deleted.
The target table (on which the rule query operated) has been deleted.
Microsoft Sentinel had been removed from the target workspace.
A function used by the rule query is no longer valid; it has been either modified or removed.
Permissions to one of the data sources of the rule query were changed.
One of the data sources of the rule query was deleted or disconnected.
upvoted 6 times

talosDevbot Most Recent 3 months ago
Answer is D
As per Microsoft's own documentation on troubleshooting analytics rules: A rule is never autodisabled due to a transient failure

One of their examples of transient failure is "A rule query takes too long to run and times out."

The only rules that are auto-disabled are queries that have permanent failure.
List as an example of permanent failure is "Permissions to one of the data sources of the rule query were changed"

Link: https://learn.microsoft.com/en-us/azure/sentinel/troubleshoot-analytics-rules
upvoted 1 times

b9cf0e5 3 months, 3 weeks ago
C- In Microsoft Sentinel, if an analytics rule is automatically disabled and the rule name is prefixed with "AUTO DISABLED," it typically indicates that the query within the rule has failed repeatedly. One common cause of this issue is that the query takes too long to execute or times out, which can lead to the rule being automatically disabled to avoid consuming excessive resources.
upvoted 3 times

g_man_rap 4 months, 3 weeks ago

C. The rule query takes too long to run and times out:

Explanation: This is a common reason for Azure Sentinel to automatically disable a custom analytics rule. If a query takes too long to execute (usually due to complexity or large data volumes), it can lead to performance issues. Azure Sentinel may automatically disable such a rule to prevent it from impacting the overall performance of the system.
Relevance: This is the most likely cause of the rule being automatically disabled and the name being prefixed with "AUTO DISABLED."
upvoted 1 times

Avaris 6 months ago

Selected Answer: C

answer is C not D
upvoted 2 times

Sneekygeek 8 months, 3 weeks ago

Selected Answer: D

A permanent failure occurs due to a change in the conditions that allow the rule to run, which without human intervention can't return to their former status. The following are some examples of failures that are classified as permanent:

The target workspace (on which the rule query operated) was deleted.
The target table (on which the rule query operated) was deleted.
Microsoft Sentinel was removed from the target workspace.
A function used by the rule query is no longer valid; it was either modified or removed.
Permissions to one of the data sources of the rule query were changed (see example).
One of the data sources of the rule query was deleted.
https://learn.microsoft.com/en-us/azure/sentinel/troubleshoot-analytics-rules
upvoted 1 times

xoe123 11 months, 1 week ago

A function used by the rule query is no longer valid; it has been either modified or removed. Permanent failure - rule auto-disabled Correct. For Transient failure there are two reasons and both are listed A rule query takes too long to run and times out.
Connectivity issues between data sources and Log Analytics, or between Log Analytics and Microsoft Sentinel.
Any other new and unknown failure is considered transient.
upvoted 1 times

xoe123 11 months, 2 weeks ago

Option D.
I think it is option D as both option A and C are for transient and question asked to pick one option. Also question says stopped while with transient failure it tries again to run the rule
upvoted 1 times

DCT 12 months ago

Selected Answer: D

Correct D.
upvoted 1 times

chepeerick 1 year, 2 months ago

Correct
upvoted 1 times

mali1969 1 year, 3 months ago

Selected Answer: D

The possible cause of the issue is D. Permissions to one of the data sources of the rule query were modified.
Option C is not correct because the rule query timeout does not cause a rule to be disabled. The default timeout for a rule query is 10 minutes, but it can be extended up to 60 minutes by using the query_timeout parameter in the advanced settings. If a query exceeds the timeout limit, it will fail and generate an error, but it will not disable the rule.
upvoted 1 times

donathon 1 year, 4 months ago

Selected Answer: D

https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom#permanent-failure---rule-auto-disabled
upvoted 1 times

D_PaW 1 year, 7 months ago

Selected Answer: A

Correct: ACD

Transient reasons:

* A rule query takes too long to run and times out.
* Connectivity issues between data sources and Log Analytics, or between Log Analytics and Microsoft Sentinel.
* Any other new and unknown failure is considered transient.

Permanent reasons:

* The target workspace (on which the rule query operated) has been deleted.
* The target table (on which the rule query operated) has been deleted.
* Microsoft Sentinel had been removed from the target workspace.
* A function used by the rule query is no longer valid; it has been either modified or removed.
* Permissions to one of the data sources of the rule query were changed.
* One of the data sources of the rule query was deleted.

Source:
https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom#issue-a-scheduled-rule-failed-to-execute-or-appears-with-auto-disabled-added-to-the-name

upvoted 1 times

stromnessian 2 years, 10 months ago

Selected Answer: D

D is correct.

upvoted 1 times

Eltooth 3 years, 3 months ago

Correct answer - D. Permission change stopped rule from connecting.

upvoted 2 times

Domza 3 years, 5 months ago

From the article:
Permanent failure - rule auto-disabled:
- Permissions to one of the data sources of the rule query were changed.

upvoted 3 times

Question #11 *Topic 3*

Your company uses Azure Sentinel.
A new security analyst reports that she cannot assign and resolve incidents in Azure Sentinel.
You need to ensure that the analyst can assign and resolve incidents. The solution must use the principle of least privilege.
Which role should you assign to the analyst?

A. Azure Sentinel Responder

B. Logic App Contributor

C. Azure Sentinel Contributor

D. Azure Sentinel Reader

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

Community vote distribution
A (100%)

Eltooth Highly Voted 2 years, 9 months ago
Roles for working in Azure Sentinel
Azure Sentinel-specific roles

All Azure Sentinel built-in roles grant read access to the data in your Azure Sentinel workspace.

Azure Sentinel Reader can view data, incidents, workbooks, and other Azure Sentinel resources.

Azure Sentinel Responder can, in addition to the above, manage incidents (assign, dismiss, etc.)

Azure Sentinel Contributor can, in addition to the above, create and edit workbooks, analytics rules, and other Azure Sentinel resources.

Azure Sentinel Automation Contributor allows Azure Sentinel to add playbooks to automation rules. It is not meant for user accounts.

Correct answer is Azure Sentinel Responder.
upvoted 23 times

subhuman Highly Voted 2 years, 3 months ago
Selected Answer: A
Answer is correct.
Using the least privilege principle Microsoft Sentinel Responder is the best role to assign this user
upvoted 5 times

Ramye Most Recent 4 months, 2 weeks ago
Selected Answer: A
https://learn.microsoft.com/en-us/azure/sentinel/roles
upvoted 1 times

chepeerick 8 months, 1 week ago
Responder
upvoted 1 times

stromnessian 2 years, 4 months ago
Selected Answer: A
IMHO the answer is A.
upvoted 1 times

NoNameP 2 years, 10 months ago
Correct!
upvoted 1 times

somsom 2 years, 10 months ago

correct

upvoted 1 times

Question #12 *Topic 3*

You recently deployed Azure Sentinel.
You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.
You need to ensure that the Fusion rule can generate alerts.
What should you do?

A. Disable, and then enable the rule.

B. Add data connectors

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

Community vote distribution
B (100%)

Eltooth Highly Voted 2 years, 9 months ago
Correct - add data connectors to bring in source data for rules, notebooks, playbooks to query/take action against.
upvoted 15 times

karlEzio Highly Voted 2 years, 9 months ago
The answer is Correct. By default, fusion is enabled. But to generate the alert, the data connectors must be configured.
upvoted 9 times

luisM14 Most Recent 5 months, 1 week ago
Selected Answer: B
correct
upvoted 1 times

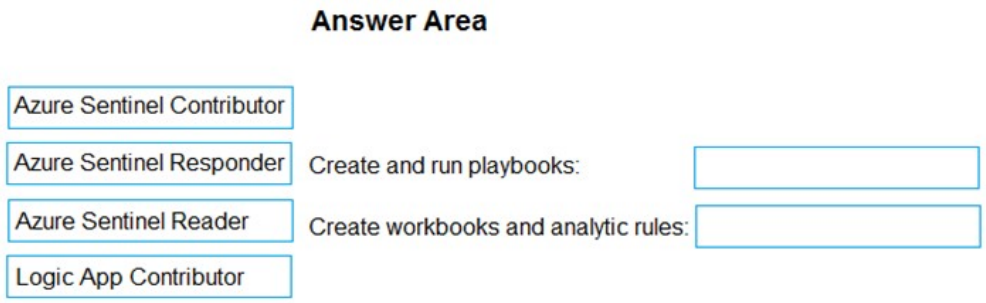
chepeerick 8 months, 1 week ago
Correct
upvoted 1 times

amsioso 1 year, 9 months ago
https://docs.microsoft.com/en-us/azure/sentinel/configure-fusion-rules
upvoted 2 times

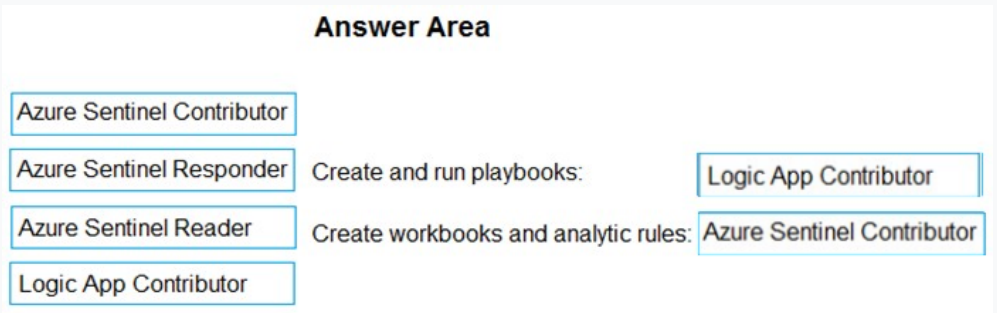
Mockento 1 year, 10 months ago
Selected Answer: B
Best Option
upvoted 4 times

Question #13 *Topic 3*

DRAG DROP -
Your company deploys Azure Sentinel.
You plan to delegate the administration of Azure Sentinel to various groups.
You need to delegate the following tasks:
✑ Create and run playbooks
✑ Create workbooks and analytic rules.
The solution must use the principle of least privilege.
Which role should you assign for each task? To answer, drag the appropriate roles to the correct tasks. Each role may be used once, more than once, or not at all.
You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
Select and Place:



Suggested Answer:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/roles

Eltooth Highly Voted 2 years, 9 months ago
Correct - logic app contributor and sentinel contributor.
upvoted 9 times

Ramye Most Recent 4 months, 2 weeks ago
Given answers are correct.
But note: it's now called Microsoft Sentinel and not Azure Sentinel
https://learn.microsoft.com/en-us/azure/sentinel/roles
upvoted 4 times

be9z 7 months, 2 weeks ago
Once you've assigned the "Logic App Contributor" role, the designated users or service principals will have the necessary permissions to create, modify, and run Logic Apps, including the Logic Apps associated with Azure Sentinel playbooks. Keep in mind that role assignments may take a few minutes to propagate.
upvoted 1 times

chepeerick 8 months, 1 week ago
Correct, Logic app to playbooks
upvoted 2 times

ExamTopicsTST 1 year, 4 months ago
Answer is correct: https://learn.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-permissions-and-allowed-actions
upvoted 4 times

Ramkid 1 year, 5 months ago

Given answers are (not) correct.
Only Logic App Contributor role is allowed to create and edit the play books as per the link below
https://learn.microsoft.com/en-us/azure/sentinel/roles#microsoft-sentinel-roles-permissions-and-allowed-actions
The question is about the “Create and run playbooks”. Logic App contributor role is not sufficient to Run the play book. You need atleast “Microsoft Sentinel Playbook Operator” to run the play book as per the below link.
https://learn.microsoft.com/en-us/azure/sentinel/roles#other-roles-and-permissions
upvoted 1 times

herta 1 year, 5 months ago

i think you are wrong based on this https://learn.microsoft.com/en-us/azure/sentinel/roles
logic app contributor can view and run playbooks
This table summarizes the Microsoft Sentinel roles and their allowed actions in Microsoft Sentinel.
upvoted 6 times

ACSC 1 year, 7 months ago

Answer is correct
https://learn.microsoft.com/en-us/azure/sentinel/roles#other-roles-and-permissions
upvoted 3 times

amsioso 1 year, 9 months ago

https://docs.microsoft.com/en-us/azure/sentinel/roles#other-roles-and-permissions
upvoted 1 times

Fury 1 year, 10 months ago

https://docs.microsoft.com/en-us/azure/sentinel/roles
Logic Apps Contributor - Attach playbooks to analytics and automation rules and run playbooks.
Note: This role also allows users to modify playbooks.
Logic apps contributor cannot be the right answer as it can't create playbooks.
Sentinel contributor for both.
upvoted 2 times

prabhjot 2 years, 3 months ago

Playbook is nothing but Logic App (so the ans is absolutely Correct)
upvoted 4 times

Andreew883 2 years, 5 months ago

Correct!
upvoted 1 times

NoNameP 2 years, 10 months ago

Correct!
upvoted 1 times

somsom 2 years, 10 months ago

correct
upvoted 1 times

Question #14 *Topic 3*

A company uses Azure Sentinel.
You need to create an automated threat response.
What should you use?

A. a data connector

B. a playbook

C. a workbook

D. a Microsoft incident creation rule

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Community vote distribution
B (100%)

Eltooth Highly Voted 2 years, 9 months ago
Correct - Playbook
upvoted 9 times

DChilds Most Recent 2 months, 3 weeks ago
Selected Answer: B
Playbook.
upvoted 1 times

chepeerick 8 months, 1 week ago
Correct
upvoted 1 times

kevin23699 9 months, 1 week ago
It must be 0,0
upvoted 1 times

ACSC 1 year, 7 months ago
Selected Answer: B
Use playbooks together with automation rules to automate your incident response and remediate security threats detected by Microsoft Sentinel
upvoted 2 times

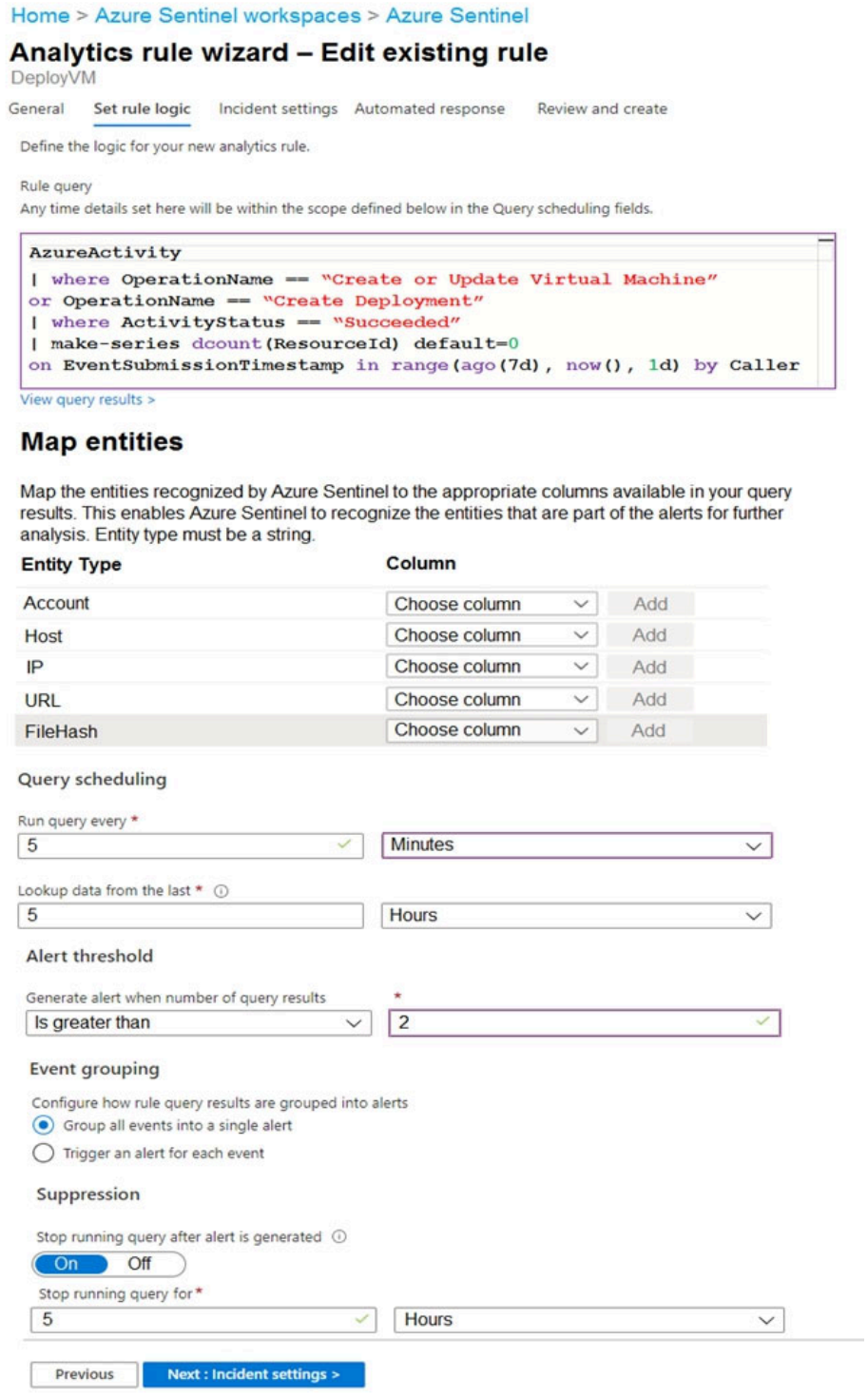
NoNameP 2 years, 10 months ago
Correct
upvoted 4 times

somsom 2 years, 10 months ago
correct
upvoted 4 times

HOTSPOT -

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.

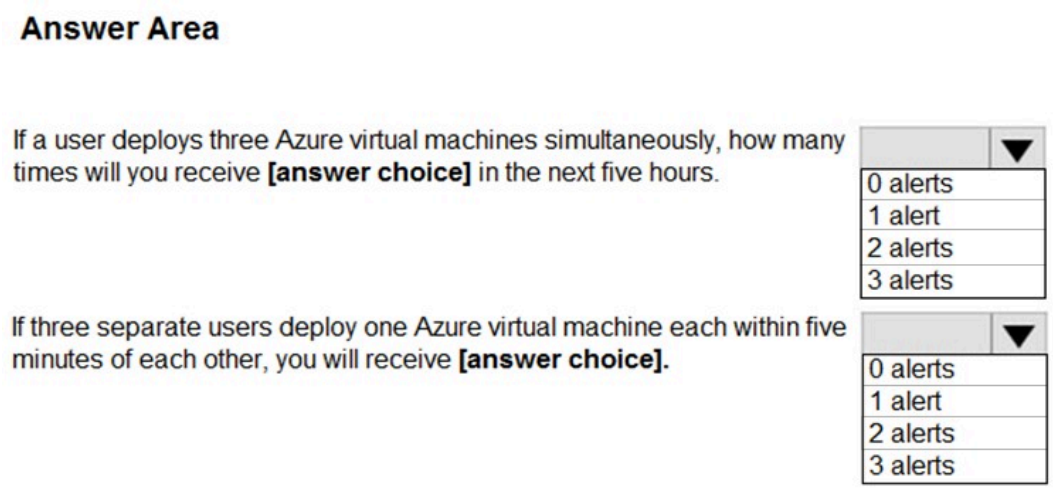


You do NOT define any incident settings as part of the rule definition.

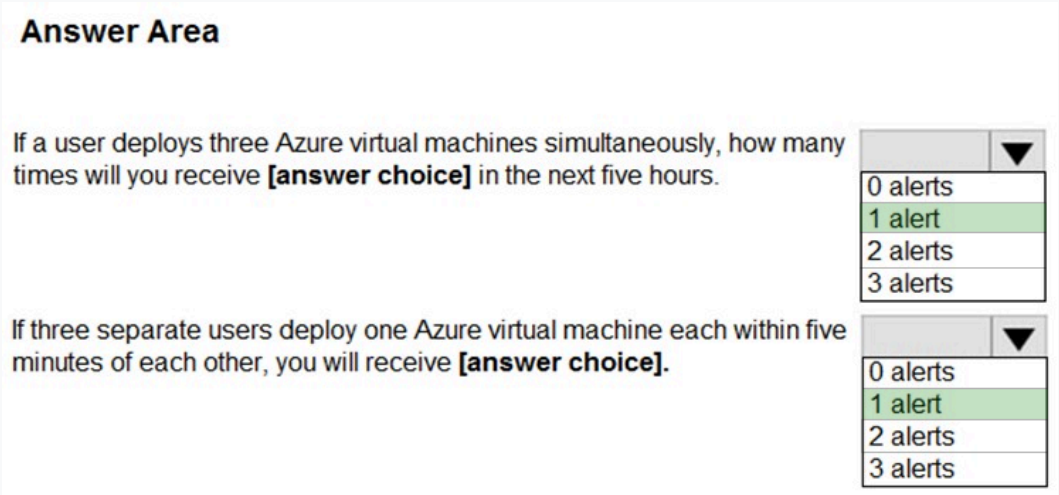
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Suggested Answer:



Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

stromnessian Highly Voted 1 year, 10 months ago

0,1

The first scenario will not generate any alerts, as each series by Caller generates a single result; there is only one caller, therefore 1 result, which is below the threshold (results > 2).

In the second scenario, there will be 3 results (one for each caller), so one alert will be generated (as this is above the threshold and the results are grouped into a single alert).

upvoted 50 times

liberty123 1 year, 10 months ago

Thanks for the explanation, I agree with you

upvoted 3 times

Muffen Highly Voted 1 year, 9 months ago

0,1

make-series is going to make lists of all the EventSubmissionTimestamp values for each user, with each user being on a separate row. This means that if 1 user creates 3 machines, it will aggregate them all into 1 row. And if 3 users create 1 virtual machine we will see 3 separate rows.

https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/make-seriesoperator#examples

upvoted 9 times

chepeerick Most Recent 2 months, 1 week ago

correct

upvoted 1 times

donathon 4 months, 4 weeks ago

0, 1. The key really is make-series.

upvoted 1 times

mimguy 5 months, 4 weeks ago
On the exam July 7 2023
upvoted 2 times

Atun23 1 year, 2 months ago
I think answer should be 0 and 1.

The make-series operator creates a series of specified aggregated values along a specified axis. In this case the "Caller", this will make 3 rows, 1 row.

This will create a table that shows arrays of the ResourceID's of each query result from each "Caller" ordered by specified time range.

The rule specifies when the query returns 2 results in a 5 minute timespan, trigger the alert, in this case the first scenario would only trigger 1 row on the results table as it uses "DCOUNT".

In the second scenario it will trigger 1 alert as the threshold is 2 results and group results on a single alert option is selected.

https://learn.microsoft.com/en-us/azure/data-explorer/kusto/query/make-seriesoperator
upvoted 2 times

j888 1 year, 7 months ago
I think the answer 1,1 is correct.
The alert will be based on 5 hours and it will only trigger when it is having 2 counts.
You will end up with 3 counts of computers been created through a single deployment, regardless this should be visible under the 5 hours log.
upvoted 4 times

Eltooth 2 years, 3 months ago
I would say if all 3 individual users created a VM within 5 minutes of each other i.e. 3 VM's created within the 5 minute window, then an alert would be triggered/generated.
Correct answer would then be 1 and 1 alert.
upvoted 4 times

AlaReAla 2 years, 3 months ago
I wonder if 2nd answer should be 0. Please correct me with appropriate justification. Thanks.
upvoted 4 times

zaqwsx 2 years, 2 months ago
but query looks on data for the last 5 hours,
upvoted 2 times

Eltooth 2 years, 3 months ago
Agreed - see above.
upvoted 2 times

JohnAvlakiotis 2 years, 2 months ago
@Eltooth you agree but in your comments it reads "1 and 1" not "1 and 0"? I mean WT..?
upvoted 1 times

JohnAvlakiotis 2 years, 2 months ago
Ah... now I see... clarity came upon me :-)
upvoted 1 times

Startkabels 2 years, 2 months ago
So which ones?
upvoted 2 times

Question #16 *Topic 3*

You have an Azure Sentinel deployment in the East US Azure region.
You create a Log Analytics workspace named LogsWest in the West US Azure region.
You need to ensure that you can use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest.
What should you do first?

A. Deploy Azure Data Catalog to the West US Azure region.

B. Modify the workspace settings of the existing Azure Sentinel deployment.

C. Add Azure Sentinel to a workspace.

D. Create a data connector in Azure Sentinel.

Suggested Answer: *C*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants

Community vote distribution
C (56%) D (44%)

Eltooth Highly Voted 3 years, 3 months ago
Correct answer - C.

Cross-workspace queries can now be included in scheduled analytics rules. You can use cross-workspace analytics rules in a central SOC, and across tenants (using Azure Lighthouse) as in the case of an MSSP, subject to the following limitations:

* Up to 20 workspaces can be included in a single query.
* Azure Sentinel must be deployed on every workspace referenced in the query.
* Alerts generated by a cross-workspace analytics rule, and the incidents created from them, exist only in the workspace where the rule was defined. They will not be displayed in any of the other workspaces referenced in the query.

https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants#cross-workspace-workbooks
upvoted 28 times

xRiot007 Most Recent 3 weeks, 4 days ago
Selected Answer: C
Unless you are using a central SOC or Lighthouse, you need to deploy Sentinel on every workspace referenced in the query:
https://learn.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants#include-cross-workspace-queries-in-scheduled-analytics-rules
upvoted 1 times

g_man_rap 4 months, 3 weeks ago
Selected Answer: D
C. Add Azure Sentinel to a workspace.
Why this is incorrect: Adding Azure Sentinel to a workspace is the initial step to enable Sentinel capabilities on that particular Log Analytics workspace. However, since the existing deployment is already in the East US region and you need to work with the LogsWest workspace, this option doesn't solve the problem of querying across regions.
D. Create a data connector in Azure Sentinel.
Why this is correct: To use data from the LogsWest Log Analytics workspace within your Azure Sentinel deployment in the East US, you need to create a data connector in Azure Sentinel. A data connector allows you to ingest data from various sources, including other Log Analytics workspaces, into Azure Sentinel. Once the data connector is set up, Azure Sentinel can generate alerts based on queries to the LogsWest workspace.
upvoted 2 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

mali1969 1 year, 3 months ago

Selected Answer: D

To use scheduled analytics rules in the existing Azure Sentinel deployment to generate alerts based on queries to LogsWest, you need to first create a data connector in Azure Sentinel. A data connector is a way to connect data sources to Azure Sentinel, so that you can collect and analyze data from various sources such as Azure services, Microsoft 365, or other cloud or on-premises solutions. By creating a data connector, you can enable Azure Sentinel to ingest data from LogsWest and use it for scheduled analytics rules.

Therefore, the correct answer is D. Create a data connector in Azure Sentinel

upvoted 1 times

donathon 1 year, 4 months ago

Selected Answer: C

https://learn.microsoft.com/en-us/azure/sentinel/quickstart-onboard >> So since you need create the workspace first then logically you should do C first followed by D. So my answer is C.

upvoted 3 times

exmITQS 1 year, 10 months ago

Selected Answer: D

To use scheduled analytics rules in an existing Azure Sentinel deployment to generate alerts based on queries to a Log Analytics workspace in a different region, you need to create a data connector in Azure Sentinel.

Therefore, the correct answer is: D. Create a data connector in Azure Sentinel.

upvoted 2 times

wsrudmen 1 year, 10 months ago

This account "exmITQS" seems to me a little bit strange.
A lot of wrong answer and explanations in different questions.
If it's not the intent, I'm really sorry for my message. But other take care to not be confused.

upvoted 10 times

stredovek 1 year, 10 months ago

I dare say that exmITQS posting answers from https://chat.openai.com/

upvoted 7 times

7c0a 1 year, 6 months ago

Indeed, and using ChatGPT for this matter is very unreliable.

upvoted 5 times

stromnessian 2 years, 10 months ago

Selected Answer: C

I'm going for C here.

upvoted 4 times

Question #17 *Topic 3*

You create a custom analytics rule to detect threats in Azure Sentinel.
You discover that the rule fails intermittently.
What are two possible causes of the failures? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. The rule query takes too long to run and times out.

B. The target workspace was deleted.

C. Permissions to the data sources of the rule query were modified.

D. There are connectivity issues between the data sources and Log Analytics

Suggested Answer: *AD*
Incorrect Answers:
B: This would cause it to fail every time, not just intermittently.
C: This would cause it to fail every time, not just intermittently.

Community vote distribution
AD (100%)

Eltooth Highly Voted 1 year, 3 months ago
Correct - A & D.
upvoted 9 times

makovec25 Highly Voted 5 months, 1 week ago
Selected Answer: AD
intermittently is a key word here, so A and D is correct
upvoted 6 times

stromnessian Most Recent 10 months, 3 weeks ago
Selected Answer: AD
Looks right to me.
upvoted 5 times

liberty123 11 months ago
Selected Answer: AD
Agree AD
upvoted 3 times

Soldier 1 year ago
Correct. A and D are transient failures. B and C are permanent.
upvoted 5 times

Muffen 9 months, 3 weeks ago
Reference: https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom#troubleshooting
upvoted 2 times

NoNameP 1 year, 4 months ago
correct
upvoted 2 times

Question #18 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a scheduled query rule for a data connector.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Community vote distribution
A (64%) B (36%)

stromnessian Highly Voted 2 years, 10 months ago
You can create scheduled rules from Data connector pages (Next steps tab). But the bottom line is whoever wrote this question should be fired on the spot.
upvoted 44 times

Tuitor01 3 weeks, 6 days ago
I agree if the "for a data connector" means using logs/data coming from a data connector.
upvoted 1 times

fnwilliamson Most Recent 2 months ago
Selected Answer: B
Answer is B
upvoted 2 times

talosDevbot 2 months, 3 weeks ago
Selected Answer: B
Answer is: No

You write a schedule analytics rule for a table (like SecurityEvents table).

The "Windows Security Events via AMA" connector write to the SecurityEvents table. This connector collects security events from Windows machines such as sign in events.

You will write a scheduled/NRT analytics rule that will have a KQL query on the SecurityEvents table, looking for IP addresses in sign in events.
upvoted 2 times

dyavlito 3 months, 3 weeks ago
ChatGPT 4:
Yes, this solution meets the goal.

Creating a scheduled query rule in Azure Sentinel for a data connector can help detect specific conditions, such as sign-ins from malicious IP addresses. You can configure the query to monitor sign-ins to Azure virtual machines and set the rule to trigger an incident when a sign-in is detected from a malicious IP, which is aligned with the goal.
upvoted 1 times

scfitzp 5 months, 3 weeks ago

Just creating a scheduled query rule doesn't inherently meet the req's. Creating an NRT rule or an incident creation rule by default put you CLOSER to a correct answer; and another answer option in this specific series of questions is "creating an incident creation rule"
upvoted 1 times

DChilds 8 months, 1 week ago
B

You create a Microsoft incident creation rule for a data connector.
upvoted 3 times

Mducks 10 months, 3 weeks ago
Selected Answer: A
I think correct answer is B:
https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts
See heading:
Enable incident generation automatically during connection
upvoted 1 times

Ramye 10 months, 2 weeks ago
Which one?
You selected A and then saying correct answer B
upvoted 5 times

im20batman 1 year, 1 month ago
Selected Answer: A
A is Correct
upvoted 3 times

chepeerick 1 year, 2 months ago
Correct
upvoted 1 times

donathon 1 year, 4 months ago
Selected Answer: B
I think the answer is no.
upvoted 2 times

JoeP1 1 year, 5 months ago
Selected Answer: B
I think the correct answer is B because the incident will be created when the query is scheduled to run, not at the time that the sign-in from the malicious IP was detected.
upvoted 2 times

evilprime 1 year, 9 months ago
CHATGPT:
No.

Creating a scheduled query rule for a data connector will not directly meet the goal of creating an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

To achieve the goal, you would need to create an analytics rule that queries the relevant logs for sign-ins to Azure virtual machines and uses a detection algorithm to identify malicious IP addresses. This rule should then be set up to trigger an incident when a malicious sign-in is detected.
upvoted 3 times

Fez786 1 year, 3 months ago
we dont care what chatGPT thinks. stop posting answers form chatGPT. kids.....
upvoted 18 times

antoniokt 1 year, 10 months ago
Selected Answer: A
A is Correct
upvoted 2 times

wsrudmen 1 year, 10 months ago
Selected Answer: A

When you configure a scheduled query on "Set rule logic" and "incident settings", you can define if raise alert and how you group into incident.
NB: create a Microsoft incident creation rule is part of a scheduled query.

Microsoft wording for this question is weird...

I don't understand why all these NO in the discussion.
If someone have a good explanation, please don't hesitate.
upvoted 4 times

amsioso 2 years, 3 months ago
NO
After connecting your data sources to Microsoft Sentinel, create custom analytics rules to help discover threats and anomalous behaviors in your environment.

Analytics rules search for specific events or sets of events across your environment, alert you when certain event thresholds or conditions are reached, generate incidents for your SOC to triage and investigate, and respond to threats with automated tracking and remediation processes.
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom
upvoted 1 times

Whatsamattr81 2 years, 4 months ago
I dunno... You can create alerts from scheduled queries. You can the create incidents from alerts. Question doesn't suggest you cant. Pretty sure (in preview) you can now create incidents based on this alone.
upvoted 2 times

kakakayayaya 3 years ago
"You create a scheduled query rule for a data connector."
Looks weird. We can't create scheduled query for data connectors. But we can analyze some tables and raise incident.
upvoted 2 times

Question #19 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a hunting bookmark.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Community vote distribution
B (100%)

chepeerick 2 months, 1 week ago
Correct
upvoted 1 times

exmITQS 10 months, 2 weeks ago
Selected Answer: B
you need to create a custom analytics rule in Azure Sentinel that detects sign-ins from malicious IP addresses and triggers an incident.
upvoted 1 times

Metasploit 1 year, 2 months ago
Selected Answer: B
B. NO.

Hunting Bookmarks:
https://learn.microsoft.com/en-us/azure/sentinel/bookmarks
upvoted 1 times

Eltooth 2 years, 3 months ago
Correct - No.
upvoted 1 times

Question #20 *Topic 3*

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are configuring Azure Sentinel.
You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.
Solution: You create a Microsoft incident creation rule for a data connector.
Does this meet the goal?

A. Yes

B. No

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-security-center

Community vote distribution
A (67%) B (33%)

eddz25 Highly Voted 1 year, 11 months ago
No
Creating a Microsoft incident creation rule for a data connector will not meet the goal of creating an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

An incident creation rule is used to create incidents in Azure Sentinel based on specific criteria, such as when a certain number of alerts are triggered within a certain timeframe. While an incident creation rule can be used in conjunction with data connectors to analyze data from other sources, it does not directly detect sign-ins from malicious IP addresses.

To detect sign-ins from malicious IP addresses, you would need to create an analytics rule that looks for specific signs of a malicious IP address, such as a high number of failed login attempts or login attempts from a known malicious IP. Once the rule detects a sign-in from a malicious IP, it can trigger an alert, which can then be used to create an incident in Azure Sentinel.
upvoted 14 times

uday1985 8 months ago
link supporting your answer ?
upvoted 2 times

Metasploit Highly Voted 2 years, 2 months ago
Selected Answer: A
YES.

https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-custom#configure-the-incident-creation-settings
upvoted 5 times

cdtplug Most Recent 3 months, 4 weeks ago
Yes according to Copilot
Yes, creating a scheduled query rule for a data connector in Azure Sentinel can meet the goal of creating an incident when a sign-in to an Azure virtual machine from a malicious IP address is detected. Here's why:

Scheduled Query Rule: This rule can be configured to run at regular intervals and check for specific conditions, such as sign-ins from malicious IP addresses.
Data Connector: By using a data connector, you can ingest relevant log data (e.g., Azure Activity logs, Sign-in logs) into Azure Sentinel.
Incident Creation: When the query detects a sign-in from a malicious IP address, it can trigger an alert, which can then be configured to create an incident in Azure Sentinel
upvoted 1 times

CollabGuy 11 months, 2 weeks ago

Selected Answer: B

No. Microsoft Incident Creation rule is to "pull" the incidents created by other Microsoft products (Defender for Endpoint, Defender for Cloud, etc) into Sentinel.

This alone would not create an incident from a sign-in from a malicious IP address

upvoted 3 times

chepeerick 1 year, 2 months ago

Correct

upvoted 1 times

mali1969 1 year, 4 months ago

Selected Answer: A

The answer is A. Yes. Creating a Microsoft incident creation rule for a data connector is a valid way to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

upvoted 2 times

RV025 1 year, 4 months ago

this question is duplicate of question 18 and doesn't make sense

upvoted 1 times

tonatiuhop 1 year, 5 months ago

Selected Answer: A

Yes

https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts

upvoted 2 times

D_PaW 1 year, 7 months ago

Selected Answer: B

B - No. The key word is the "Creation" in "Incident Creation Rule"

In Azure Sentinel, an Incident Creation Rule and an Incident Rule are two different components used in the incident management workflow:

Incident Creation Rule: An Incident Creation Rule is responsible for identifying and creating incidents based on specific conditions or triggers. It is typically used to detect specific patterns, events, or anomalies in the collected data. When the conditions defined in the rule are met, an incident is automatically generated.

Incident Rule: An Incident Rule, also known as an Analytics Rule, is responsible for performing analysis on the collected data to identify potential security threats or suspicious activities. It applies specific logic or queries to the data to identify notable events or behavior. When the rule's conditions are met, it generates a notable event, which can later be investigated and potentially escalated to an incident.

upvoted 1 times

omar_alhajsalem 1 year, 7 months ago

Selected Answer: B

not meet the goal

upvoted 2 times

evilprime 1 year, 9 months ago

Yes.

Creating a Microsoft incident creation rule for a data connector can meet the goal of creating an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

You can create a query that searches for sign-ins to Azure virtual machines from suspicious or malicious IP addresses, and then use that query in a Microsoft incident creation rule. When the rule detects a match, it can create an incident in Azure Sentinel that contains details about the suspicious sign-in. This can enable security teams to investigate the incident and take appropriate actions to mitigate any threats.

upvoted 2 times

exmITQS 1 year, 10 months ago

Selected Answer: A

A. Yes, creating a Microsoft incident creation rule for a data connector can meet the goal of creating an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

upvoted 2 times

amsioso 2 years, 3 months ago

YES

https://docs.microsoft.com/en-us/azure/sentinel/connect-defender-for-cloud

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-security-center-auto-connect-to-sentinel/ba-p/1387539

upvoted 1 times

Andreew883 2 years, 11 months ago

Correct - yes.

upvoted 2 times

DigitalNomad 3 years, 1 month ago

I think this is the correct answer , as this kind of alert is generated by ASC , so we need the Microsoft incident creation rule to create incidents from ASC into sentinel. see https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-reference

upvoted 4 times

Question #21 *Topic 3*

You plan to create a custom Azure Sentinel query that will track anomalous Azure Active Directory (Azure AD) sign-in activity and present the activity as a time chart aggregated by day.
You need to create a query that will be used to display the time chart.
What should you include in the query?

A. extend

B. bin

C. makeset

D. workspace

Suggested Answer: *B*
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries

Community vote distribution
B (100%)

werbinich Highly Voted 2 years, 3 months ago
Grouping results can also be based on a time column, or another continuous value. Simply summarizing by TimeGenerated, though, would create groups for every single millisecond over the time range, because these are unique values.

To create groups that are based on continuous values, it's best to break the range into manageable units by using bin.

Thus correct answer.
upvoted 15 times

Murtuza Most Recent 1 month ago
Perf
| where TimeGenerated > ago(7d)
| where Computer == "ContosoAzADDS2"
| where CounterName == "Available MBytes"
| summarize avg(CounterValue) by bin(TimeGenerated, 1h)
upvoted 1 times

chepeerick 2 months, 1 week ago
Correct
upvoted 1 times

ACSC 1 year, 1 month ago
Selected Answer: B
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/get-started-queries#summarize-by-a-time-column
upvoted 3 times

stromnessian 1 year, 10 months ago
Selected Answer: B
B for bin. Simples.
upvoted 3 times

Eltooth 2 years, 3 months ago
Correct - bin.
upvoted 2 times

tk3 2 years, 4 months ago
correct
upvoted 2 times

Task 2 years, 7 months ago
Correct Answer

upvoted 4 times

Question #22 *Topic 3*

You are configuring Azure Sentinel.
You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.
Which two actions should you perform in Azure Sentinel? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Add a playbook.

B. Associate a playbook to an incident.

C. Enable Entity behavior analytics.

D. Create a workbook.

E. Enable the Fusion rule.

Suggested Answer: *AB*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Community vote distribution
AB (100%)

werbinich Highly Voted 2 years, 9 months ago
Playbooks are collections of procedures that can be run from Azure Sentinel in response to an alert or incident. A playbook can help automate and orchestrate your response, and can be set to run automatically when specific alerts or incidents are generated, by being attached to an analytics rule or an automation rule, respectively. It can also be run manually on-demand.

Playbooks in Azure Sentinel are based on workflows built in Azure Logic Apps, which means that you get all the power, customizability, and built-in templates of Logic Apps.

Thus correct answer
upvoted 25 times

aman1782 2 years, 1 month ago
Correct A&B
upvoted 1 times

AlaReAla 2 years, 9 months ago
keep up the good stuff @werbinich. Hope you crack the certification soon. All the best.
upvoted 6 times

chepeerick Most Recent 8 months, 1 week ago
Correct
upvoted 1 times

kevin23699 9 months, 1 week ago
It should be B,C
upvoted 1 times

Ramye 4 months, 1 week ago
Please explain why..
upvoted 1 times

JoeP1 11 months, 2 weeks ago
Selected Answer: AB
It is worded poorly to say you need to associate the playbook with the incident instead of setting the incident as a trigger, but options C, D and E make even less sense.
upvoted 2 times

eddz25 1 year, 5 months ago
Selected Answer: AB

A. Add a playbook
B. Associate a playbook to an incident

To send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected in Azure Sentinel, you will need to perform two actions:

Add a playbook: A playbook is a set of actions that can be triggered in response to an incident, such as sending a message to a channel in Microsoft Teams. To add a playbook, you will need to navigate to the Playbooks tab in Azure Sentinel and create a new playbook that includes an action to send a message to a Microsoft Teams channel.

Associate a playbook to an incident: After creating the playbook, you will need to associate it with an incident in Azure Sentinel. This can be done by navigating to the Incidents tab in Azure Sentinel and selecting the incident that you want to associate the playbook with. Then, select the "Associate Playbook" button and select the playbook that you created.

upvoted 2 times

subhuman 2 years, 3 months ago

Selected Answer: AB

Correct answer A&B

upvoted 1 times

stromnessian 2 years, 4 months ago

Selected Answer: AB

AB IMHO.

upvoted 2 times

liberty123 2 years, 4 months ago

Selected Answer: AB

A & B is correct

upvoted 1 times

kakakayayaya 2 years, 7 months ago

For me B is a wrong choice. We can NOT associate a playbook to an incident! We can:
- trigger playbook when incident happens
- associate playbook to an ANALYTIC RULE
Fusion rule is important to catch Multistage attacks not suspicious sign-in.
So A - ok
B - weird.

upvoted 3 times

Eltooth 2 years, 9 months ago

Correct - A & B

upvoted 3 times

tk3 2 years, 10 months ago

i agree with the answer

upvoted 1 times

Task 3 years, 1 month ago

Correct

upvoted 2 times

Question #23 *Topic 3*

You need to visualize Azure Sentinel data and enrich the data by using third-party data sources to identify indicators of compromise (IoC). What should you use?

A. notebooks in Azure Sentinel

B. Microsoft Cloud App Security

C. Azure Monitor

D. hunting queries in Azure Sentinel

Suggested Answer: *A*
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/notebooks

Community vote distribution
A (100%)

werbinich Highly Voted 2 years, 9 months ago
The Azure portal and all Azure Sentinel tools use a common API to access this data store.

The same API is also available for external tools such as Jupyter notebooks and Python. While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data. It combines full programmability with a huge collection of libraries for machine learning, visualization, and data analysis. These attributes make Jupyter a compelling tool for security investigation and hunting.

Thus Correct Answer.
upvoted 31 times

Soldier 2 years, 6 months ago
Great explanation @werbinich
upvoted 1 times

chepeerick Most Recent 8 months, 1 week ago
Correct option
upvoted 1 times

creed8171 1 year, 1 month ago
Selected Answer: A
Visualize = Notebooks
upvoted 2 times

Ramye 4 months, 1 week ago
adding a bit further ...
Visualize = Notebooks = Workbook
upvoted 1 times

eddz25 1 year, 5 months ago
Selected Answer: A
A. notebooks in Azure Sentinel

To visualize Azure Sentinel data and enrich it by using third-party data sources to identify indicators of compromise (IoC), you can use notebooks in Azure Sentinel.

Notebooks in Azure Sentinel are interactive documents that allow you to run queries, create visualizations, and perform data analysis on your Azure Sentinel data. They also allow you to connect to other data sources, such as third-party threat intelligence feeds, to enrich the data and identify indicators of compromise (IoCs).

Once you have connected to the third-party data source, you can use Azure Sentinel notebook to blend the data, and create visualizations, and perform data analysis to identify the potential attack.
upvoted 1 times