Question #1 *Topic 1*

Which two advanced attributes can be applied to incident fields when editing? (Choose two.)

A. Set a field trigger script

B. Associate to an incident type

C. Change field type

D. Change field name

Correct Answer: *AB*

Community vote distribution

AB (100%)

[Removed] 4 months, 1 week ago

Selected Answer: AB

The correct answers are:

A. Set a field trigger script
B. Associate to an incident type

upvoted 1 times

chucklepie 12 months ago

You can also change the type under certain circumstances so while correct this question is bad

upvoted 1 times

jbender72 2 years ago

correct

upvoted 2 times

thorodp 2 years, 3 months ago

Selected Answer: AB

These are correct

upvoted 2 times

Question #2 *Topic 1*

Given an incident with three files, how could the name of the second file be referenced?

A. ${Files.[2].Name}

B. ${Files.Name.[2]}

C. ${File.[1].Name}

D. ${File.Name.[1]}

Correct Answer: *D*

Community vote distribution

D (60%) C (40%)

Branodn Highly Voted 3 years, 1 month ago

The answer is C ${File.[1].Name}

upvoted 14 times

Jai_ke Most Recent 4 months, 1 week ago

Selected Answer: C

C, This is because most indexing in arrays starts at 0, so the first file would be at index 0, and the second file would be at index 1.

upvoted 1 times

[Removed] 4 months, 1 week ago

Selected Answer: D

The correct answer is:

D. ${File.Name.[1]}

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: D

The answer is D. ${File.Name.[1]}

For example, when retrieving parameters in a playbook, the first parameter is specified as File.Name.[0].

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: C

C is Correct

upvoted 1 times

chucklepie 12 months ago

Why can't answers be changed? The answer is C

upvoted 2 times

TcanCmon 1 year, 11 months ago

I just tested, File.[1].Name it is. Therefore, C

(And the index is starting from 0)

upvoted 3 times

thorodp 2 years, 3 months ago

Selected Answer: D

D is correct, index starts from 0.

upvoted 1 times

cptcoggsworth 1 year, 7 months ago

D is incorrect because it is not the correct JSON path

upvoted 1 times

rmurugan 3 years, 2 months ago

A is the correct answer

upvoted 1 times

⊟ **rafemuhammed** 2 years, 5 months ago

Could you please confirm it? Index starts with 0 right so second file means index 1.

upvoted 3 times

Question #3 *Topic 1*

Which component can be part of a load balancing group?

A. Distributed database

B. D2 agent

C. Engine

D. Load balancing server

Correct Answer: *C*

Community vote distribution

C (100%)

[Removed] 4 months, 1 week ago

Selected Answer: C

The correct answer is:

C. Engine

upvoted 1 times

MarcoS10 1 year, 9 months ago

Selected Answer: C

Engine is the correct answer

upvoted 1 times

thorodp 2 years, 3 months ago

Selected Answer: C

Correct

upvoted 2 times

Question #4 *Topic 1*

Which method accesses a field called `˜User Mail' in a playbook?

A. ${incident.usermail}

B. ${incident.User Mail}

C. ${incident.UserMail}

D. ${usermail}

Correct Answer: *A*

Community vote distribution

A (88%) 13%

thorodp Highly Voted 2 years, 3 months ago

Selected Answer: A

Correct

upvoted 5 times

[Removed] Most Recent 4 months, 1 week ago

Selected Answer: A

The correct answer is:

A. ${incident.usermail}

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: A

this answer is A.This can be confirmed by specifying incident details in the playbook.

upvoted 1 times

commonflavor 5 months, 1 week ago

this answer is A.This can be confirmed by specifying incident details in the playbook.

upvoted 1 times

john1208 1 year, 8 months ago

Selected Answer: C

i think its C

upvoted 1 times

Question #5 Topic 1

A SOC manager built a dashboard and would like to share the dashboard with other team members.
How would the SOC manager create a dashboard that meets this requirement?

A. Manually share the dashboard through user emails

B. Dashboard is shared to all XSOAR users

C. Propagate the dashboard based on SAML authentication

D. Dashboard is shared to all XSOAR users in a selected role

Correct Answer: *D*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/dashboards/share-a-dashboard.html

Community vote distribution

D (100%)

thorodp 3 months ago

Selected Answer: D

Correct

upvoted 2 times

Question #6 *Topic 1*

Which two methods will allow data to be saved in incident fields within a playbook? (Choose two.)

A. setFields

B. Field mapping

C. setIncident

D. Layout inline editing

Correct Answer: *BC*

Community vote distribution

BC (100%)

john1208 2 months ago

Selected Answer: BC

correct

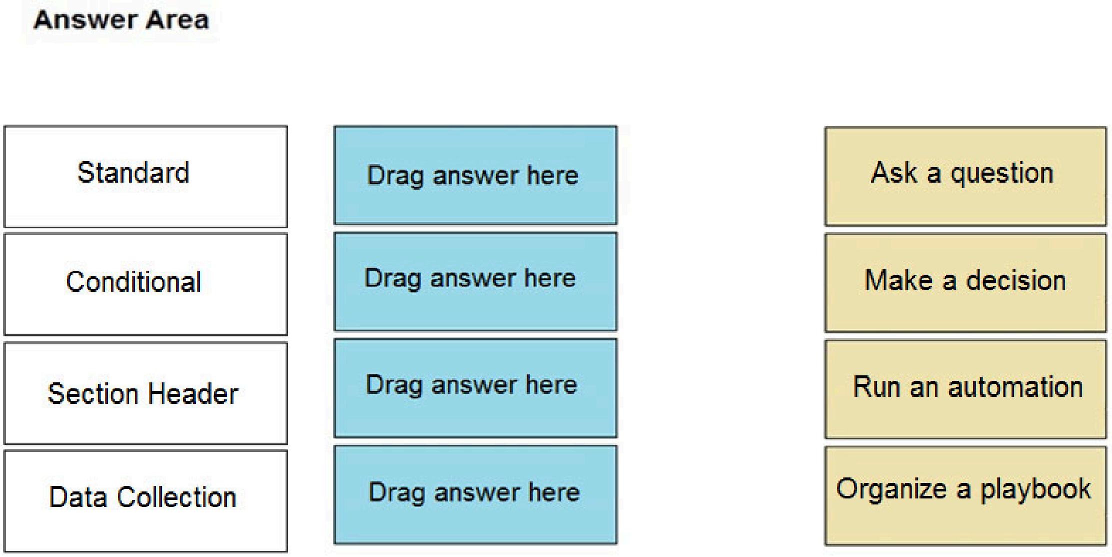
upvoted 1 times

Question #7 *Topic 1*

DRAG DROP -

Match the action with the most appropriate playbook task type.

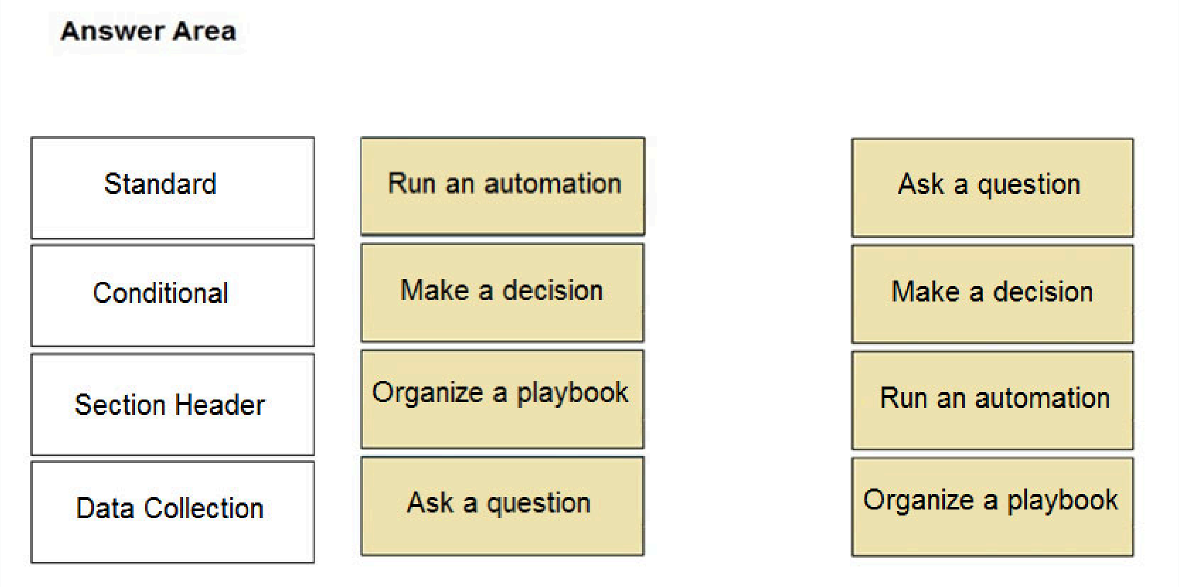
Select and Place:



Answer Area

Standard	Drag answer here	Ask a question
Conditional	Drag answer here	Make a decision
Section Header	Drag answer here	Run an automation
Data Collection	Drag answer here	Organize a playbook

Correct Answer:



Answer Area

Standard	Run an automation	Ask a question
Conditional	Make a decision	Make a decision
Section Header	Organize a playbook	Run an automation
Data Collection	Ask a question	Organize a playbook

https://www.jaacostan.com/2021/02/palo-alto-cortex-xsoar-playbook-icons.html

⊟ **john1208** 2 months ago

correct

upvoted 1 times

Question #8 *Topic 1*

Which built-in automation/command cab be used to change an incident's type?

A. setIncident

B. Set

C. GetFieldsByIncidentType

D. modifyIncidentFields

Correct Answer: *A*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/incidents/incidents-management/incident-fields/field-trigger-scripts.html

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

An engineer notices that playbooks only start once the user clicks the `˜investigate' button and he/she would like the playbook to start automatically.
How can this be implemented?

A. Add the playbook to the integration's settings

B. Select 'Run playbook automatically' from the incident type settings

C. Add the !startinvestigation automation to the beginning of the playbook

D. Select 'Run playbook automatically' from the integration settings

Correct Answer: *B*

Community vote distribution

B (100%)

rmurugan Highly Voted 3 years, 2 months ago

B is the answer

upvoted 10 times

jasminsurani Highly Voted 2 years, 1 month ago

B is the answer.

upvoted 5 times

Jai_ke Most Recent 4 months, 1 week ago

Selected Answer: B

This option allows playbooks to start automatically when an incident of a specified type is created, eliminating the need for manual intervention.

upvoted 1 times

Monitor2 5 months, 1 week ago

Selected Answer: B

B os the correct One. Please update the answer

upvoted 1 times

Monitor2 5 months, 1 week ago

B is the correct! There are a lot of mistakes

upvoted 1 times

john1208 1 year, 8 months ago

Selected Answer: B

B is the answer, dont mislead please

upvoted 1 times

MarcoS10 1 year, 8 months ago

B is the correct answer, from Settings/Object Setup/Incident Types/select your own type and edit/flag the option "run automatically playbook"

upvoted 1 times

momo_tree 1 year, 11 months ago

B as in Cardi B

upvoted 1 times

Uggie 1 year, 11 months ago

Selected Answer: B

b it is

upvoted 2 times

TcanCmon 1 year, 11 months ago

B Indeed

upvoted 2 times

Question #10 *Topic 1*

Which two causes may be occurring if an integration test is working, but the integration is not fetching incidents? (Choose two.)

A. The 'Fetches Incidents' option may not have been enabled

B. There are no new events from the external service

C. The first fetch should be manually triggered to start the fetching process

D. It can take up to 1-hour before incidents are initially fetched

Correct Answer: *AC*

Community vote distribution

AB (100%)

randomnametester Highly Voted 2 years, 8 months ago

Pretty sure its AB

upvoted 14 times

Monitor2 Most Recent 5 months, 1 week ago

Selected Answer: AB

AB is the correct One. There are many errors

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: AB

Answer is AB

upvoted 1 times

momo_tree 1 year, 11 months ago

A as in Automation and B as in Cardi B

upvoted 2 times

TcanCmon 1 year, 11 months ago

Wrong answer. It's AB

upvoted 3 times

Question #11 *Topic 1*

Which two capabilities do Automation script settings include? (Choose two.)

A. Define 'parameters'

B. Correlate to incident types

C. Define 'outputs'

D. Set password protection

Correct Answer: *CD*

Community vote distribution

CD (80%) AC (20%)

Jai_ke 4 months, 1 week ago

Selected Answer: CD

There is no parameters settings, its called arguments.

upvoted 1 times

Monitor2 4 months, 4 weeks ago

Selected Answer: AC

In Cortex XSOAR, an automation script is a key component that allows users to execute specific tasks and logic within their incident response workflows. The settings for these scripts typically include various options to define how the script interacts with other components within the system.

For your question regarding the two capabilities included in Automation script settings, the correct options are:

A. Define 'parameters'
C. Define 'outputs'

upvoted 1 times

Serpaldom 7 months, 2 weeks ago

CD
There's no parameters, only "Arguments" which includes arguments, importants and outputs.

upvoted 2 times

Gab99 1 year, 2 months ago

Selected Answer: CD

CD is correct

upvoted 3 times

PANW 1 year, 5 months ago

please provide justification/links for answers

upvoted 1 times

momo_tree 1 year, 11 months ago

C as in Cardi B and D as in Demisto

upvoted 1 times

TcanCmon 1 year, 11 months ago

CD is the answer, nothing to do for inc. types.

upvoted 2 times

jbender72 2 years ago

SHOULD BE C AND D

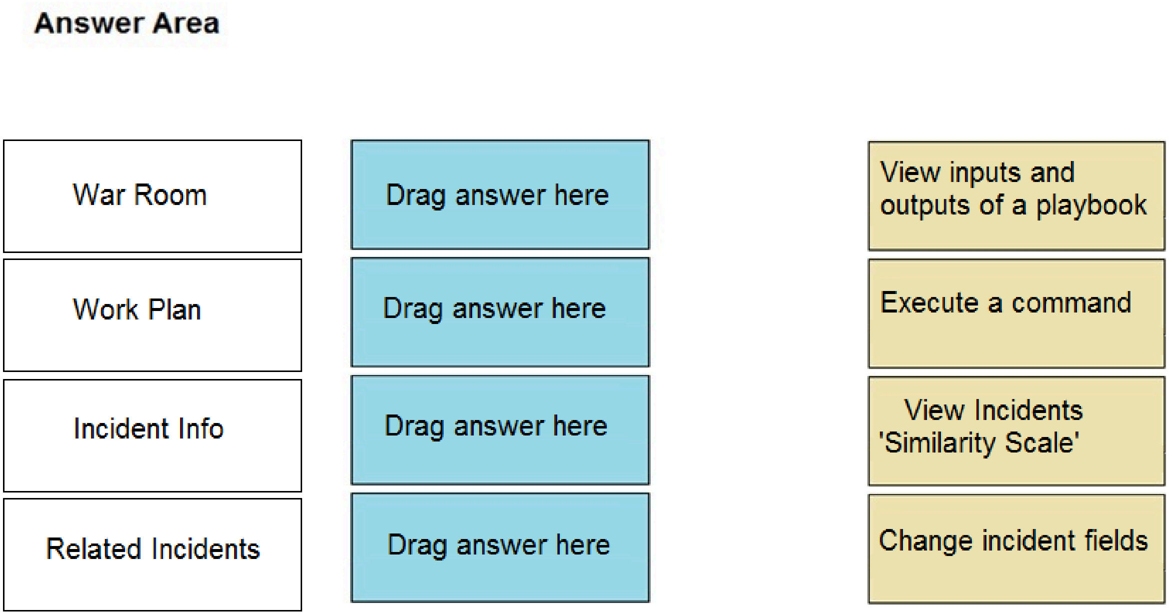
upvoted 1 times

Question #12 *Topic 1*

DRAG DROP -

Match the appropriate action to the layout type.

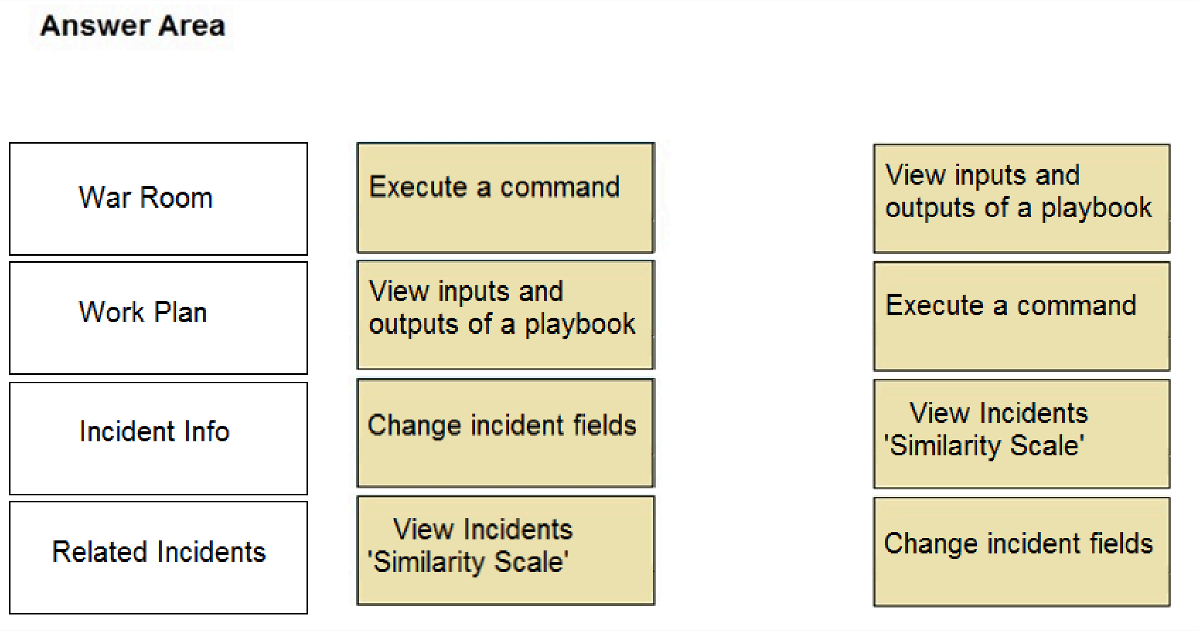
Select and Place:



Answer Area

War Room	Drag answer here	View inputs and outputs of a playbook
Work Plan	Drag answer here	Execute a command
Incident Info	Drag answer here	View Incidents 'Similarity Scale'
Related Incidents	Drag answer here	Change incident fields

Correct Answer:



Answer Area

War Room	Execute a command	View inputs and outputs of a playbook
Work Plan	View inputs and outputs of a playbook	Execute a command
Incident Info	Change incident fields	View Incidents 'Similarity Scale'
Related Incidents	View Incidents 'Similarity Scale'	Change incident fields

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

What is a primary use case of data collection tasks?

A. To allow multi-question surveys without authentication restrictions

B. To automate tasks such as parsing a file or enriching indicators

C. To generate new widgets for a dashboard

D. To determine different paths in a playbook

Correct Answer: *A*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/playbook-tasks/communication-tasks/create-a-data- collection-task.html

Community vote distribution

A (100%)

Monitor2 5 months, 1 week ago

Selected Answer: A

It si ok

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: A

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/8/Cortex-XSOAR-Administrator-Guide/Create-a-Data-Collection-Task

upvoted 1 times

TcanCmon 1 year, 11 months ago

Its A, regardless of auth, its the primary use-case. Also, authentication is supported on Xsoar starting from a 6.6ish version. Hence, all is good

upvoted 2 times

jbender72 2 years ago

"The survey resides on an external site that does not require authentication, thereby allowing survey recipients to respond without restriction." From XSOAR...This shows that A is not the correct answer. The above is not the primary use.

upvoted 1 times

Question #14 *Topic 1*

In which three locations can an engineer try to find information, when troubleshooting a failed integration instance error produced by the test button? (Choose three.)

A. The audit log

B. The log bundle

C. The source code for an integration

D. The error message returned directly below the button

E. The playground war room

Correct Answer: *BDE*

Community vote distribution

BDE (80%) ABD (20%)

Jai_ke 4 months, 1 week ago

Selected Answer: BDE

B. The log bundle
It provides comprehensive logs for detailed error analysis.

D. The error message returned directly below the button
It offers immediate feedback on the specific error encountered.

E. The playground war room
It can show relevant context and additional debugging information when running tests in the playground environment.

So, the correct choices would be B, D, and E.

upvoted 1 times

Monitor2 4 months, 4 weeks ago

Selected Answer: ABD

These sources provide detailed logs and error messages that can help diagnose and resolve the issue.

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: BDE

E:https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Server-Post-Installation-Health-Check

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: BDE

Answer is BDE

upvoted 2 times

Sarppp 1 year, 4 months ago

BDE is correct, you may find it on War Room (after fetch incident command), you may also find it in log bundle as well.

upvoted 2 times

appopay 1 year, 6 months ago

A-B-D is the correct answer

upvoted 1 times

Question #15

Topic 1

Which two statements describe how timers are configured to start and stop automatically in a playbook? (Choose two.)

A. Use a field of Number to count the number of seconds elapsed between two tasks

B. After the playbook has run, calculate the total time taken and set the timer field with this value

C. To begin counting time taken, add a task in the playbook with automation startTimer. To end the counting, add a task with automation stopTimer

D. From the Timers tab of the playbook task, choose the action for the timer and the timer field to perform the action on

Correct Answer: *BD*

Community vote distribution

CD (100%)

samtron 2 months, 2 weeks ago

Selected Answer: CD

it should be CD

upvoted 2 times

momo_tree 5 months ago

C as in Cardi B and D as in DBot

upvoted 2 times

TcanCmon 5 months, 3 weeks ago

It should be CD

upvoted 3 times

Question #16 *Topic 1*

How long is the trial period for paid content packs?

A. 30 days

B. 14 days

C. 7 days

D. 60 days

Correct Answer: *A*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/marketplace/marketplace-subscriptions.html

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

After enriching a username using Active Directory, an engineer would like to send an email to the user's manager. However, this functionality is not part of the command output. The engineer checks with raw-response=true and notices that the manager's email is returned, but not saved in the context.
How can the engineer save the data so it will be accessible?

A. Mark ignore output = true

B. Use extend-context

C. Use raw-response = save

D. Mark ignore input = true

Correct Answer: *B*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/extend-context/extend-context-using-the-command-line.html

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Where can engineers add the post-processing scripts to incidents?

A. The post-processing tag must be added to the automation

B. Post-processing scripts must be added at the end of playbooks

C. Post-processing scripts must be added from the Incident Type editor

D. Post-processing scripts must be added from the Post-Process Rules editor

Correct Answer: *C*

Community vote distribution

C (100%)

Monitor2 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: C

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.12/Cortex-XSOAR-Administrator-Guide/Add-a-Post-Processing-Script-to-the-Incident-Type

upvoted 1 times

Question #19

Topic 1

An engineer would like to present a trend using widgets to compare to a previous week's data.
Which two methods will allow the engineer to meet the requirement? (Choose two.)

A. Create widget of type Line, check 'Display Trend' and define as 7 days ago

B. Create a custom widget using a new incident query

C. Create widget of type Number, check 'Display Trend' and define as 7 days ago

D. Create a custom widget using a script

Correct Answer: *AD*

Community vote distribution

AB (50%) CD (50%)

Jai_ke 4 months, 1 week ago

Selected Answer: AB

A. Create widget of type Line, check 'Display Trend' and define as 7 days ago
A Line widget can display trends over time, and setting it to compare to data from 7 days ago will show the trend and comparison effectively.

B. Create a custom widget using a new incident query
A custom widget with a specific query can be designed to compare current data with historical data, such as the previous week's data, allowing for a tailored trend analysis.

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: CD

this answer is C,D.

upvoted 1 times

Sarppp 1 year, 4 months ago

BC is correct, there is no display trend opiton in line type when you create a widget.

upvoted 2 times

> **Sarppp** 1 year, 4 months ago
>
> CD will be correct sorry for the typo.
>
> upvoted 4 times

Question #20 *Topic 1*

What happens when an integration is deprecated?

A. The integration commands in a playbook can no longer be used

B. The integration commands can be used, but it is recommended to update to the latest content pack

C. The configuration settings will be lost and the integration will no longer function

D. The integration commands in a playbook can be used, but it will fail at runtime

Correct Answer: *B*

Community vote distribution

B (100%)

Monitor2 5 months, 1 week ago

Selected Answer: B

It os B

upvoted 1 times

momo_tree 1 year, 11 months ago

Selected Answer: B

B as in Cardi B

upvoted 3 times

TcanCmon 1 year, 11 months ago

It is B. Though, it just means that version is out of support from the developer

upvoted 2 times

piipo 2 years, 8 months ago

Selected Answer: B

You can also use it with deprecated.

upvoted 4 times

Question #21 *Topic 1*

Which investigation element is best suited for collaboration among users?

A. Work Plan

B. Related Incidents

C. War Room

D. Context Data

Correct Answer: *C*

Community vote distribution

C (100%)

lucaboban Highly Voted 3 years, 6 months ago

C - Correct

upvoted 15 times

Jai_ke Most Recent 4 months, 3 weeks ago

Selected Answer: C

LOL the reference link for D is cr*p.

upvoted 1 times

Monitor2 5 months, 1 week ago

Selected Answer: C

C is correct

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: C

it is C

upvoted 1 times

appopay 1 year, 6 months ago

C as in Cardi B

upvoted 2 times

samtron 1 year, 8 months ago

Selected Answer: C

It is C

upvoted 2 times

TcanCmon 1 year, 11 months ago

War room - C

upvoted 3 times

Question #22

Topic 1

Which three support types are included in the Marketplace Content Packs? (Choose three.)

A. Customer supported

B. Contex XSOAR supported

C. Community supported

D. Partner supported

E. Prisma Cloud supported

Correct Answer: *BCD*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/marketplace/marketplace-overview/content-packs-support-types.html

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Which three authentication methods are supported when logging into XSOAR? (Choose three.)

A. OTP token

B. User name and password

C. SAML

D. Active Directory authentication

E. RADIUS

Correct Answer: *BCD*

Community vote distribution

BCD (100%)

zoinx Highly Voted 3 years, 5 months ago

No radius but username / password instead

upvoted 8 times

randomnametester Highly Voted 2 years, 8 months ago

answer is BCD

upvoted 7 times

Jai_ke Most Recent 3 months, 2 weeks ago

Selected Answer: BCD

No RADIUS

upvoted 1 times

Monitor2 5 months, 1 week ago

Selected Answer: BCD

No radius si possible

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: BCD

no radius

upvoted 1 times

samtron 1 year, 8 months ago

Selected Answer: BCD

It is BCD

upvoted 2 times

TcanCmon 1 year, 11 months ago

BCD, no raidus

upvoted 4 times

Question #24 Topic 1

Which two components have their own context data? (Choose two.)

A. Sub-playbook

B. Task

C. Field

D. Incident

Correct Answer: *AD*

Community vote distribution

AD (100%)

Jai_ke 4 months, 1 week ago

Selected Answer: AD

B. Task & C. Field do not have their own context data independently. Tasks and fields are components of playbooks and incidents, respectively, and their data is usually derived from or tied to the playbook or incident context.

upvoted 1 times

Question #25 *Topic 1*

What are two main uses of context data? (Choose two.)

A. Store incident information in JSON format

B. Store incident information in XML format

C. Pass data between playbook tasks

D. Pass data between to-do tasks

Correct Answer: *AC*

Reference:

https://xsoar.pan.dev/docs/integrations/context-and-outputs#:~:text=The%20main%20use%20of%20the,the%20Context%20and%20uses%20it

.

Currently there are no comments in this discussion, be the first to comment!

Question #26 Topic 1

Multiple company assets were reported by vulnerability scanners as being vulnerable to CVE-2017-11882. This vulnerability affects applications installed on workstations. The SOC team needs to take action and apply the new vulnerability patch that was just released. The team must first create a cause for each of the identified assets in ServiceNow IT Service Management (ITSM), in order to notify the IT department. Next, the team creates a task in the main playbook, which extracts the list of assets from the scanner report.
After the list of assets are created, what are the two solutions that the SOC team could take so that a case could be created and a patch installed? (Choose two.)

A. Create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Condition: AreValuesEqual ג€" Exit on yes ג€" left:1, right 1) and perform the following tasks: - Active Directory User Enrichment based on the computerName - Create the ServiceNow Record by adding the enrichment information - Mark the ticket severity as Urgent

B. Create a sub-playbook with a single input containing the computer names that will loop 'For Each Input' and perform the following tasks: - Active Directory User Enrichment based on the computerName - Create the ServiceNow Record by adding the enrichment information - Mark the ticket severity as Urgent

C. Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator contains the count of the number of items in the list) and perform the following tasks: - Active Directory User Enrichment based on the computerName - Create the ServiceNow Record by adding the enrichment information - Mark the ticket severity as Urgent

D. Set a key for storing the iteration number and create a sub-playbook with a single input containing the computer names that will loop until the last item from the asset list (Exit condition: iterator equal to count of the number of item in the list) and perform the following tasks: - Increase the iterator value by one each time - Active Directory User Enrichment based on the computerName - Create the ServiceNow Record by adding the enrichment information - Mark the ticket severity as Urgent

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

When creating a new tab in the layout, which section cannot be added?

A. Retrieve widget chart based on script

B. Related incidents

C. War room entries picked by entry query

D. Incident team members

Correct Answer: *A*

Community vote distribution

A (50%) B (50%)

Monitor2 4 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: B

Related incidents

upvoted 1 times

jbender72 2 years ago

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Customize-Incident-Layouts B is the answer.

upvoted 3 times

yuvalhal 2 years, 8 months ago

B - Related Incidents

upvoted 3 times

randomnametester 2 years, 8 months ago

You can retrieve a widget chart based on a script

upvoted 2 times

randomnametester 2 years, 8 months ago

I don't think you can make another related incidents page

upvoted 1 times

Question #28 *Topic 1*

In which two ways can data be transferred between playbooks and sub-playbooks? (Choose two.)

A. Inputs and outputs

B. Through integration context

C. Automatically extracted by sub-playbooks

D. From context data, if context is shared globally

Correct Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

By default, which components does an XSOAR implementation include?

A. XSOAR server, XSOAR engine

B. Application server, distributed DB server

C. Application server, distributed DB server, Backup server

D. All in one server

Correct Answer: *D*

Community vote distribution

D (92%) 8%

piipo Highly Voted 2 years, 8 months ago

Selected Answer: D

All in One

upvoted 8 times

commonflavor Most Recent 5 months, 1 week ago

Selected Answer: B

reference:Single Server Deployment - System Requirements

upvoted 1 times

momo_tree 1 year, 11 months ago

D as in Distributed Databases

upvoted 1 times

TcanCmon 1 year, 11 months ago

D is correct

upvoted 2 times

jasminsurani 2 years, 1 month ago

Selected Answer: D

D is the correct.

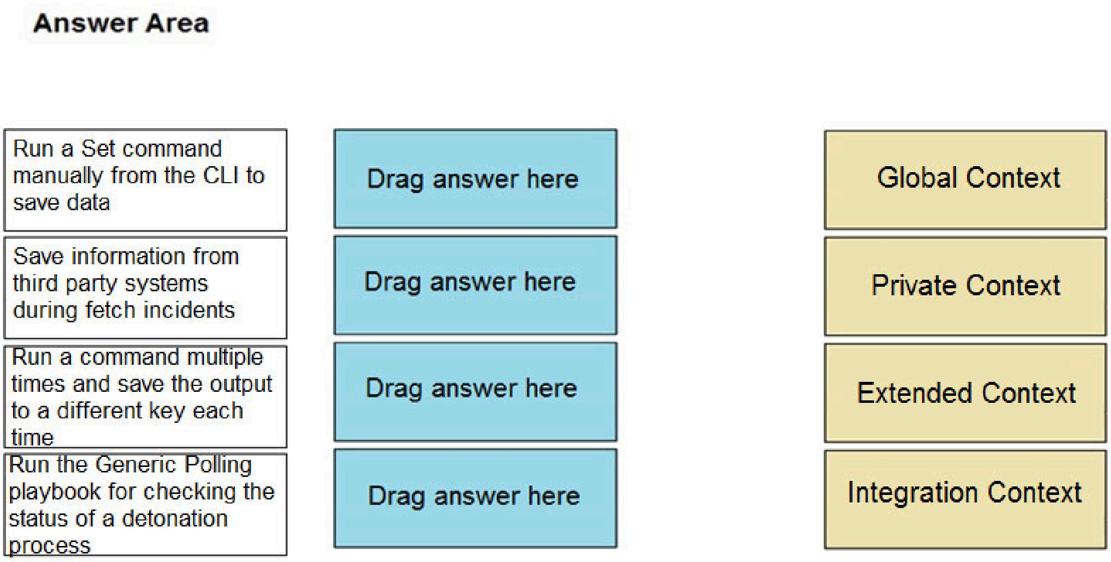
upvoted 3 times

Question #30 *Topic 1*

DRAG DROP -

Match the operations with the appropriate context.

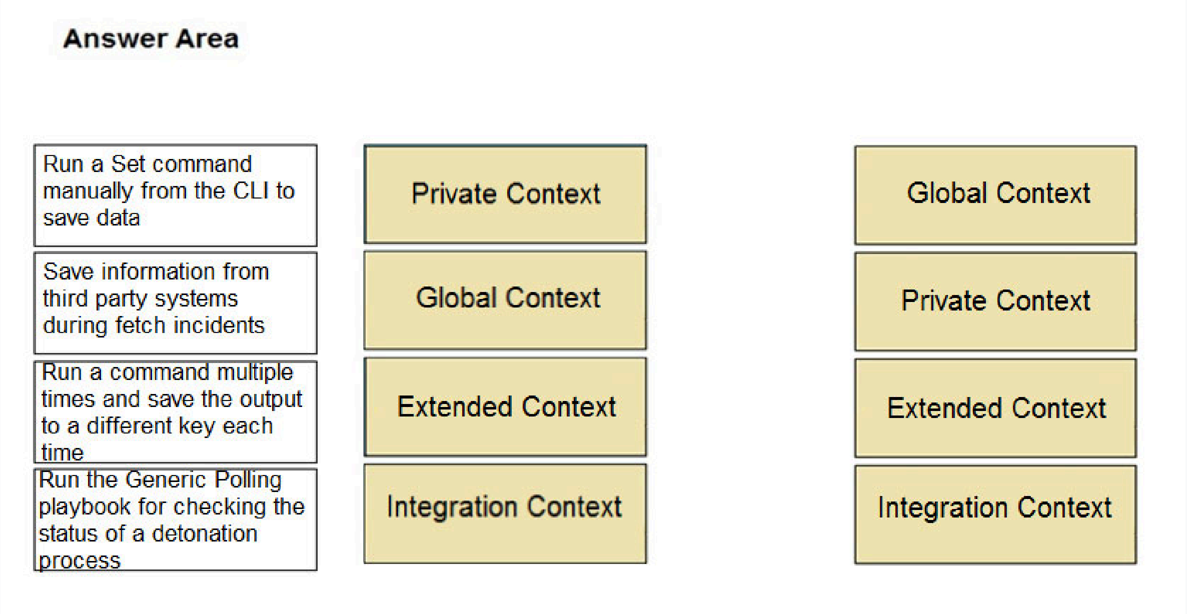
Select and Place:



Answer Area

Run a Set command manually from the CLI to save data	Drag answer here	Global Context
Save information from third party systems during fetch incidents	Drag answer here	Private Context
Run a command multiple times and save the output to a different key each time	Drag answer here	Extended Context
Run the Generic Polling playbook for checking the status of a detonation process	Drag answer here	Integration Context

Correct Answer:



Answer Area

Run a Set command manually from the CLI to save data	Private Context	Global Context
Save information from third party systems during fetch incidents	Global Context	Private Context
Run a command multiple times and save the output to a different key each time	Extended Context	Extended Context
Run the Generic Polling playbook for checking the status of a detonation process	Integration Context	Integration Context

carad 2 months, 4 weeks ago

Correct Answer is:

1. Run a set command manually from the cli to save data - Global context
2. Save information from third party systems during fetch incident - Integration Context
3. Run a command multiple times and save the output to a different key each time - Extended Context
4. Run the Generic polling playbook for checking the status of a detonation process - Private Context

Justification:

1 - war room command outputs save to the global context of an incident after you run them

2 - fetch incidents is handled at the integration level

3 - extend context is used to map task outputs to keys in the context

4 - Global context is not supported by generic polling playbook as specified in the XSOAR Admin Guide

upvoted 1 times

news088 1 year, 2 months ago

from 3rd party system during fetch incidents....should be integration

Run generic polling playbook for checking status of a detonation process....should be global context.

upvoted 1 times

Question #31 *Topic 1*

Which three statements are true about the Marketplace? (Choose three.)

A. Allows reverting back to a previous version of a content pack

B. Enables users to participate in the community by sharing content

C. Publishes content without additional review from the Cortex XSOAR team

D. Allows uploading of content in additional languages

E. Offers granularity in installation through content packs

Correct Answer: *ABE*

Community vote distribution

ABE (100%)

Jai_ke 4 months, 1 week ago

Selected Answer: ABE

The other options, C and D, are not generally accurate in the context of the Marketplace:

C. Publishes content without additional review from the Cortex XSOAR team: Typically, content is reviewed before being published to ensure quality and security.
D. Allows uploading of content in additional languages: The Marketplace does not typically handle content localization or additional language support directly.

upvoted 1 times

Monitor2 5 months, 1 week ago

Selected Answer: ABE

ABE is the correct one

upvoted 1 times

jasminsurani 2 years, 1 month ago

Selected Answer: ABE

languages are not supported, content always validated by XSOAR team.

upvoted 3 times

zoinx 3 years, 5 months ago

C is not true, it should be A instead.

upvoted 4 times

Question #32 *Topic 1*

What can be added to offload integration instance processing from the main server?

A. Database node

B. Application server

C. Engine

D. Development server

Correct Answer: *A*

Community vote distribution

C (100%)

⊟ **Max359** Highly Voted 👍 2 years, 5 months ago

The answer should be C

upvoted 8 times

⊟ **randomnametester** Highly Voted 👍 2 years, 2 months ago

Engine

upvoted 6 times

⊟ **piipo** Most Recent ⏲ 3 months, 2 weeks ago

Selected Answer: C

Offload is Engine

upvoted 2 times

Question #33 *Topic 1*

Which XSOAR architecture would be recommended for Managed Security Service Providers (MSSP)?

A. Multi-region

B. Dev-Prod

C. Multi-tenant

D. Distributed database

Correct Answer: *C*

Reference:

https://www.ncsi.com/wp-content/uploads/2020/11/cortex-xsoar.pdf

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

An incident field is created having the display name as Source_IP.
How can the field be accessed?

A. ${incident.sourceip}

B. ${incident.Source_IP}

C. ${incident.srcip}

D. ${incident.Source IP}

Correct Answer: *A*

Community vote distribution

A (80%) B (20%)

Monitor2 4 months, 4 weeks ago

Selected Answer: B

B is the correct.

upvoted 1 times

commonflavor 5 months, 1 week ago

Selected Answer: A

Check in demo environment:${incident.sourceip}

upvoted 2 times

piipo 9 months, 3 weeks ago

Selected Answer: A

lowercase with no space

upvoted 2 times

MarcoS10 1 year, 8 months ago

A is correct

upvoted 4 times

randomnametester 2 years, 8 months ago

The correct answer is A. Machine name is lowercase with no space

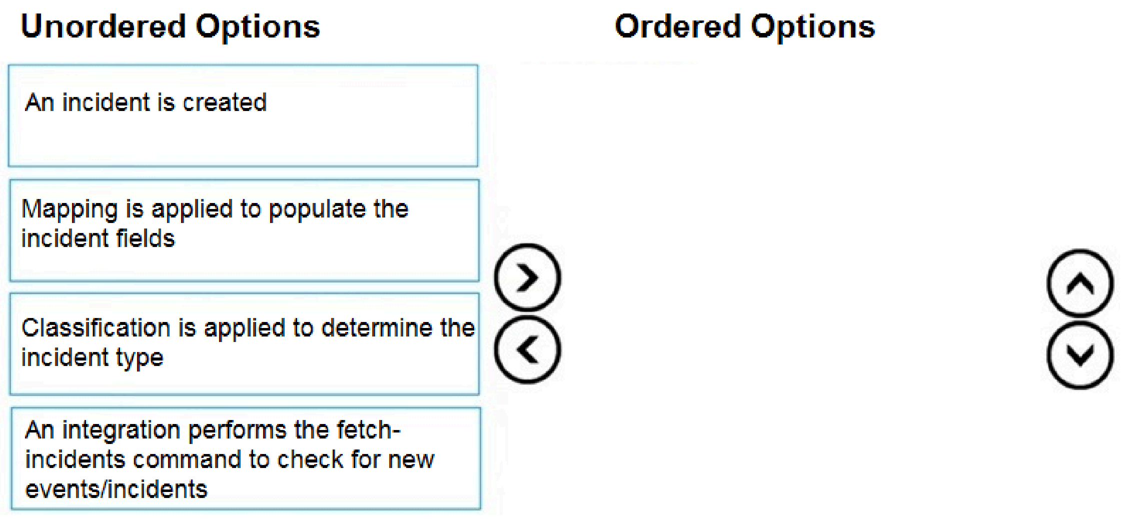
upvoted 4 times

Question #35 *Topic 1*

DRAG DROP -

Arrange these steps in the order that they occur during an incident fetch.

Select and Place:



Unordered Options

An incident is created

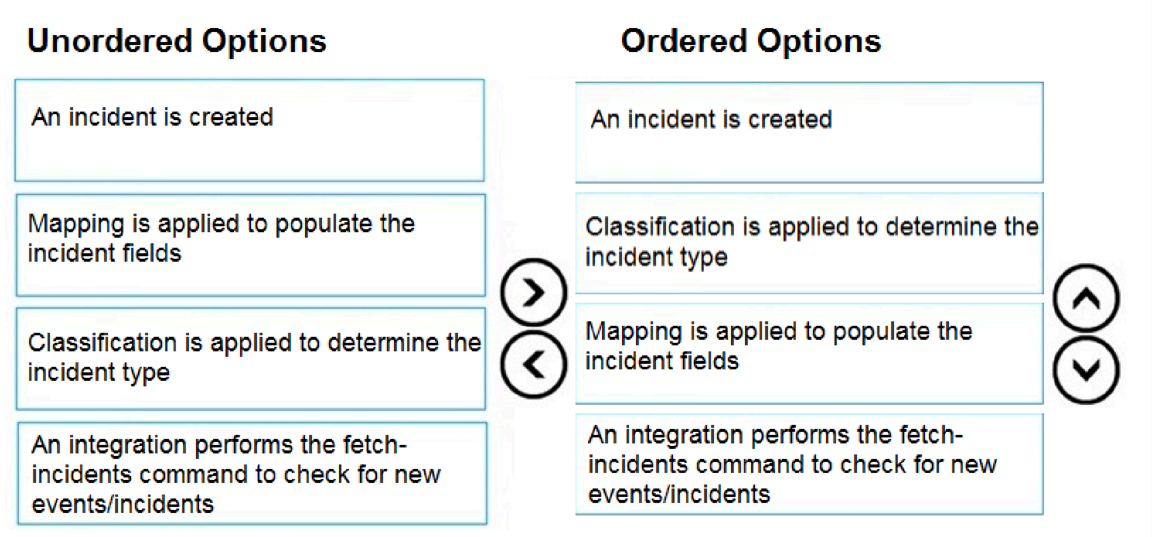
Mapping is applied to populate the incident fields

Classification is applied to determine the incident type

An integration performs the fetch-incidents command to check for new events/incidents

Ordered Options

Correct Answer:



Unordered Options

An incident is created

Mapping is applied to populate the incident fields

Classification is applied to determine the incident type

An integration performs the fetch-incidents command to check for new events/incidents

Ordered Options

An incident is created

Classification is applied to determine the incident type

Mapping is applied to populate the incident fields

An integration performs the fetch-incidents command to check for new events/incidents

pawkers Highly Voted 11 months, 2 weeks ago

I do not think so. It should be like that:

Integration performs

Classification is applied

Mapping is applied

Incident is created (before incident creation it should be also pre-process rule step)

upvoted 13 times

Sarppp 4 months, 2 weeks ago

Wrong, when you just search 'lifecycle of an incident in xsoar' you will see that in order:

1)Event Data Ingestion

2)Incident-Object Creation

3)Classification

4)Mapping

5)Pre-Process

6)Incident Process

7)Incident Management

upvoted 1 times

⊟ **appopay** 6 months ago

the incident object is created right after the integration performs, after the mapping and pre-process, the incident is made to be available. but in fact it is created right after the integration performs. source beacon: Palo Alto Networks Certified Security Automation Engineer (PCSAE) -> Cortex XSOAR: SOAR Engineer Training -> Incident Classification and Mapping

upvoted 1 times

⊟ **thorodp** Highly Voted 👍 1 year, 3 months ago

For future reference. This is wrong. The correct order is:

Integration performs
Incident is created
Classification is applied
Mapping is applied

upvoted 10 times

⊟ **PenguPC** 1 year, 3 months ago

I agree
https://xsoar.pan.dev/docs/integrations/fetching-incidents

upvoted 3 times

⊟ **franko_72** Most Recent ⊙ 5 months, 2 weeks ago

Stage One: Event-Data Ingestion
The incident lifecycle begins when an integration fetches an event. You can configure integrations in Cortex XSOAR to fetch event data from various sources, such as a SIEM, EDR, a firewall, and other security systems and services.

Stage Two: Incident Object Creation
Cortex XSOAR uses the event data fetched by an integration to create an incident object and populates it with raw event data.

Stage Three: Classification
Cortex XSOAR identifies the type of incident based on the classifier object selected in the integration configuration settings. If you have not selected any classifier, then the integration uses the default classifier of the integration. Cortex XSOAR will identify an incident as Unclassified if no default classifier exists or if the type of an incident cannot be identified.

Stage Four: Mapping
The raw event data ingested by an integration gets mapped to existing fields in Cortex XSOAR. The fields display incident data to analysts in the Cortex XSOAR graphical user interface (GUI).
Ingestion >> Incident Creation >> Classification >> Mapping is the 100% correct answer

upvoted 4 times

⊟ **randomnametester** 1 year, 8 months ago

This is wrong

upvoted 1 times

Question #36 *Topic 1*

An engineer deployed two different instances of Active Directory for each organization site. As part of account enrichment use case, the engineer would like to delete a user from one specific site.
Which command will accomplish this?

A. run 'ad-delete-user' command with 'user-dn' arg and using-brand=ג€Active Directory Query v2ג€

B. run 'ad-delete-user' command with 'user-dn' arg and raw-response=true

C. run 'ad-delete-user' command with 'user-dn' arg and ignore-outputs=true

D. run 'ad-delete-user' command with 'user-dn' arg and using=ג€Active Directory Query v2_instance_1ג€

Correct Answer: *D*

Community vote distribution

D (100%)

franko_72 Highly Voted 👍 1 year, 5 months ago

D is correct, here is the command for a user names frank on my dummy Windows server

!ad-delete-user user-dn="CN=frank,CN=Users,DC=xsoar,DC=local" using="Active Directory Query v2_instance_1"

upvoted 5 times

> **PANW** 1 year, 5 months ago
>
> Thanks Franko for adding a comment that makes sense and explain the answer
>
> Too many people give answers without explanation, which isn't really useful
>
> upvoted 1 times

Monitor2 Most Recent 🕒 5 months, 1 week ago

Selected Answer: D

D is the correct One

upvoted 1 times

Monitor2 8 months ago

Selected Answer: D

D is the correct one

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: D

D is the correct

upvoted 1 times

MarcoS10 1 year, 8 months ago

D because you select instance by "Advanced tab in the task/Using"

upvoted 2 times

randomnametester 2 years, 8 months ago

Using Brand would delete from both orgs

upvoted 1 times

rmurugan 3 years, 2 months ago

D is the correct answer

upvoted 3 times

amkoppad 3 years, 5 months ago

D is the correct answer

upvoted 3 times

Question #37 *Topic 1*

An engineer is developing a playbook that will be run multiple times for testing purposes.
What is the recommended first task to be used in the playbook?

A. DeleteContext

B. GenerateTest

C. PrintContext

D. SetContext

Correct Answer: *A*
Reference:
https://xsoar.pan.dev/docs/integrations/test-playbooks

⊟ **lucaboban** Highly Voted 👍 6 months ago

A - Correct

upvoted 5 times

Question #38 *Topic 1*

What is the most effective way to correlate multiple raw events coming from a SIEM and link them together?

A. Process all alerts by running the respective playbook and link related incidents during post-processing

B. Ingest all raw events, run a custom script to find the relationship between them and proceed to link them together

C. Configure a pre-process rule to link related events as they are ingested

D. Manually go through the incidents created by the raw events and link related incidents

Correct Answer: *C*

Community vote distribution

C (100%)

jasminsurani Highly Voted 2 years, 1 month ago

Selected Answer: C

C is a answer.

upvoted 6 times

randomnametester Highly Voted 2 years, 8 months ago

Answer is C

upvoted 5 times

Monitor2 Most Recent 5 months, 1 week ago

Selected Answer: C

It is C

upvoted 1 times

Monitor2 8 months ago

Selected Answer: C

c is the correct one

upvoted 1 times

Question #39 *Topic 1*

Which two incident search queries are valid? (Choose two.)

A. created:>=ג€7 daysג€

B. owner===admin

C. role is Analyst

D. status:closed ג€"category:job

Correct Answer: *AD*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortex-xsoar-overview/how-to-search-in-cortex-xsoar.html

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

What is the correct expression to use when filtering only PDF files?

A. Use File.Extension that does not equal (string comparison) PDF

B. Use File.Name contains PDF

C. Use File.Extension contains (general) PDF

D. Use File.Extension equals (string comparison) PDF

Correct Answer: *D*

Community vote distribution

D (100%)

amkoppad Highly Voted 3 years, 5 months ago

D is correct answer

upvoted 6 times

Jai_ke Most Recent 4 months, 1 week ago

Selected Answer: D

This expression ensures that you are specifically filtering files with the .pdf extension, making it the most precise and accurate way to target PDF files.

upvoted 1 times

Monitor2 8 months ago

Selected Answer: D

D is correct

upvoted 1 times

piipo 9 months, 3 weeks ago

Selected Answer: D

D is correct

upvoted 1 times

MarcoS10 1 year, 8 months ago

D is the cotrrect

upvoted 1 times

pawkers 1 year, 11 months ago

Most precise will be D but C also will be ok and do the work

upvoted 1 times

rmurugan 3 years, 2 months ago

D is the best answer than B

upvoted 3 times

Question #41 *Topic 1*

Whar are possible war room result (entry) types?

A. Context, file, error, image

B. Note, indicator, error, image

C. Video, file, error, image

D. Note, file, error, image

Correct Answer: *D*

Community vote distribution

D (100%)

amkoppad Highly Voted 11 months, 2 weeks ago

D is the correct answer

upvoted 7 times

DarioGabriel Highly Voted 3 months, 2 weeks ago

Selected Answer: D

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-6/cortex-xsoar-admin/incidents/incident-management/war-room-overview

upvoted 5 times

Question #42 *Topic 1*

An engineer asked for a specific command in an integration but the capability does not exist. The engineer decided to edit the existing integration by copying the integration and adding the needed commands.
What is the main concern when adding these commands?

A. The commands must return a proper result to the war room for the analysts to understand

B. The code may not be written to XSOAR standards

C. The integrations are locked and cannot be edited with additional commands

D. The custom integration will not be maintained and updated by XSOAR content team

Correct Answer: *D*

Community vote distribution

D (91%) 9%

DarioGabriel Highly Voted 2 years, 9 months ago

Selected Answer: D

Custom content are not supported

upvoted 8 times

zoinx Highly Voted 3 years, 5 months ago

D is the correct answer

upvoted 6 times

franko_72 Most Recent 1 year, 6 months ago

Selected Answer: D

A, B and C don't really make much sense to me. The one that does is D as once an integration has been "detached" it cannot be updated by XSOAR

upvoted 2 times

jasminsurani 2 years, 1 month ago

Selected Answer: C

You can never edit and develop the command for any integration. Automations can only be developed or edited.

upvoted 1 times

Jai_ke 3 months, 2 weeks ago

You can duplicate then edit the duplicate

upvoted 1 times

rmurugan 3 years, 2 months ago

D is the best answer

upvoted 3 times

Question #43 *Topic 1*

How is data transferred between playbook tasks?

A. Read/Write from context data

B. Over war room results

C. Input from the indicator page

D. Directly from a previous task

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

A large number of incidents were deleted by mistake.
Which two architecture components can be used to recover the lost data? (Choose two.)

A. Live backup

B. Engine

C. Distributed database

D. Local backup

Correct Answer: *AD*

Community vote distribution

AD (100%)

⊟ **DarioGabriel** Highly Voted 👍 1 year, 3 months ago

Selected Answer: AD

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-6/cortex-xsoar-admin/disaster-recovery-and-live-backup/backup-the-database.html

upvoted 8 times

⊟ **MarcoS10** Most Recent 🕒 2 months, 2 weeks ago

AD no other possibilities

upvoted 1 times

⊟ **randomnametester** 1 year, 2 months ago

I could see AB or AD. Depending on if you consider the live backup server to be an engine. Which probably it should not be.

upvoted 1 times

Question #45 *Topic 1*

Which two statements accurately describe layouts? (Choose two.)

A. Layouts override classification and mapping

B. New tabs can be added to the incident layout

C. Layouts can display incident information and custom fields

D. Layouts add or remove custom fields from an incident type

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

An engineer's organization system is registered in the following manner: <SiteName-SystemID-Username>. The engineer created a new indicator type for detecting systems using regex. The engineer would now like the username to be created as a separate `˜User' indicator automatically once a system is found.
What is the most efficient way for the engineer to achieve this?

A. Create a custom indicator field named 'username' and link it to the internal system indicator

B. Change the reputation command for the internal system indicator type

C. Create a new indicator type of the internal username and set a formatting script to extract only the username

D. Create a new indicator type of the internal username and have the regex included on any string that has dash at the beginning

Correct Answer: *B*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-threat-intel-management-guide/manage-indicators/understand-indicators/ indicator-types/indicator-type-profile

Community vote distribution
C (100%)

randomnametester Highly Voted 👍 2 years, 2 months ago
C is best answer. System message does not start with dash so it will not come up in regex of D
upvoted 7 times

piipo Most Recent 🕓 3 months, 2 weeks ago
Selected Answer: C
C is Correct
upvoted 1 times

rmurugan 2 years, 8 months ago
D seems the best answer
upvoted 3 times

Question #47 *Topic 1*

Which two options are the most effective for moving content between two environments? (Choose two.)

A. Remote repository based content sharing

B. UI based content import/export button

C. Copy the content backup from one environment file system (/var/lib/demisto/backup/content-backup-*) and move it to the other environment

D. Download the content items separately and upload them to the other environment

Correct Answer: *AC*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/manage-data/migrate-data-to-another-server-for-multi-tenant.html

Community vote distribution

AB (100%)

amkoppad Highly Voted 3 years, 5 months ago

A,B is correct.

upvoted 7 times

Jai_ke Most Recent 4 months, 1 week ago

Selected Answer: AB

C. Copying the content backup and D. Downloading and uploading content items separately can be more cumbersome and error-prone compared to the other options, especially if dealing with a large volume of content.

upvoted 1 times

franko_72 1 year, 5 months ago

A,C surely?

upvoted 1 times

samtron 1 year, 8 months ago

Why you tell a,b? i think it is righ, AC

upvoted 2 times

Question #48 *Topic 1*

Which three options can be defined in the layout settings? (Choose three.)

A. Set of fields to present

B. Permission to view the tab based on 'Users'

C. Permission to view the tab based on 'Roles'

D. Delete built-in tabs including the war room

E. Dynamic sections

Correct Answer: *ACE*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/incidents/customize-incident-view-layouts/customize-incident- layouts.html

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

What can be used as integration parameters?

A. URL, API key, port

B. URL, certificate, image

C. Token, query, playbook

D. User-password, csv file, query

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

Which two features does XSOAR offer to help recover from a server failure? (Choose two.)

A. Live backup (disaster recovery)

B. Distributed database

C. Backup data to XSOAR engines

D. Local backup

Correct Answer: *AD*

Community vote distribution

AD (100%)

amkoppad Highly Voted 👍 3 years, 5 months ago

A,D is the correct answer

upvoted 9 times

Jai_ke Most Recent 3 months, 2 weeks ago

Selected Answer: AD

It is not C because XSOAR engines are used for distributed execution of tasks and integrations but not for data backup. They don't store backup data for disaster recovery.

upvoted 1 times

franko_72 1 year, 6 months ago

Selected Answer: AD

Seems like A and D are correct. I Engines are used to off-load processing not to backup as far as I know.

upvoted 3 times

Question #51 *Topic 1*

When uploading content, which two options could the upload include? (Choose two.)

A. Indicators

B. Incidents

C. Reports

D. Fields

Correct Answer: *AB*

Community vote distribution

CD (50%) AC (50%)

Jai_ke 4 months, 2 weeks ago

Selected Answer: CD

Reports: You can upload custom reports as part of content packs or individual uploads. These reports are templates or preconfigured reports that can be used to visualize and analyze incident data, performance, or other metrics.

Fields: Custom fields are frequently included when uploading content. These are user-defined fields that extend the default incident, indicator, or other objects in XSOAR to capture specific information relevant to the organization's processes.

Why not Indicators or Incidents?

Indicators and Incidents are typically data that Cortex XSOAR ingests or processes dynamically, rather than content you would upload as part of a content pack or configuration. Content packs are generally used to upload custom layouts, playbooks, reports, scripts, and fields—not the actual data (indicators or incidents) which are ingested and processed in real time.

upvoted 1 times

piipo 9 months, 2 weeks ago

Selected Answer: AC

A and C

upvoted 1 times

chucklepie 12 months ago

AC. you have upload option for these two. ignore the others that do not say AC

upvoted 1 times

appopay 1 year, 5 months ago

think it's B and D. indicators aren't considered "content" in xsoar

upvoted 1 times

> **appopay** 1 year, 5 months ago
>
> C and D , appologies for the typo
>
> upvoted 3 times

Deepu2710 1 year, 6 months ago

A,C in reports it's showing upload option and inside threat intel in xsoar indicators tab also there is upload option. Correct me if I am wrong. I verified this from xsoar

upvoted 3 times

amkoppad 3 years, 5 months ago

A,D is correct

upvoted 3 times

Question #52 *Topic 1*

An engineer defined a dashboard which allows important metrics to be displayed. The engineer would like to make this dashboard the default dashboard.
How can it be accomplished?

A. Default Dashboard can be defined by 'Role'

B. Use the server configuration key: default.dashboards

C. Save the dashboard as a widget and apply it to all users

D. Right click on the dashboard tab and 'Set as Default'

Correct Answer: *D*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/monitoring/cortex-xdr-dashboard/manage-dashboards.html

Community vote distribution
A (100%)

⊟ **zoinx** Highly Voted 3 years, 5 months ago
Correct answer is A
upvoted 6 times

⊟ **kunalgupta** 3 years, 3 months ago
D is right as per the reference link
upvoted 3 times

⊟ **jasminsurani** 2 years, 1 month ago
Link is for Cortex XDR, not for XSOAR.
upvoted 3 times

⊟ **franko_72** Most Recent 1 year, 6 months ago
Yep, when you create a Dashboard, you Share it, specify who to share it with and Read/Write or Read Only and once shared, you can add it to a Default Dashboard. Answer is 100% A
upvoted 3 times

⊟ **franko_72** 1 year, 6 months ago
Having trouble finding the answer but A would be the most logical. Under Settings >> Users and Roles >> Scroll down to Default Dashboards and select the default dashboard for that role. You can choose the positions for all dashboards by clicking on them in the order you want them. However, I don't see custom dashboards in this field.
upvoted 1 times

⊟ **MarcoS10** 1 year, 8 months ago
B is correct
https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Automation-Server-Configurations
upvoted 1 times

⊟ **jasminsurani** 2 years, 1 month ago
Selected Answer: A
In Production, you can do define default dashboard under the roles.
upvoted 2 times

⊟ **yuvalhal** 2 years, 8 months ago
Correct answer is B.
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/dashboards/configure-a-default-dashboard
upvoted 2 times

⊟ **Jai_ke** 4 months, 1 week ago
This link doesn't work anymore.
upvoted 1 times

Question #53 *Topic 1*

How would context data be filtered to receive only malicious indicator values with DBotScore?

A. Get DBotScore.value where DBotScore.Score (Larger or equals) 4

B. Get DBotScore.value where DBotScore.Score (equals (int)) 3

C. Get DBotScore where DBotScore.Score (Larger than) 1

D. Get DBotScore where DBotScore.Score (Larger or equals) 2

Correct Answer: *B*
Reference:
https://github.com/demisto/content/blob/master//Packs/DeprecatedContent/Integrations/PaloAlto_MineMeld/README.md

chucklepie 5 months, 4 weeks ago

This question makes no sense. 'Malicious' is not a dbotscore. Bad is so if you equate malicious to bad it is '3'. However there is no property 'value' for DBotScore. So there are no answers correct. So the question is just badly worded. So A if you think dbotscore.value (which does not exist) or D but value 2 equates to 'Suspicious'...

upvoted 2 times

chucklepie 5 months, 4 weeks ago

Whoops, B if you want to use '3' as the answer and D for Suspicious.

upvoted 1 times

news088 8 months, 3 weeks ago

some info about dbot score. 0-1-2-3
https://xsoar.pan.dev/docs/integrations/dbot

upvoted 2 times

Question #54 *Topic 1*

Can an automation script execute an integration command and an integration command execute an automation script?

A. An automation script cannot execute an integration command and an integration command cannot execute an automation script

B. An automation script can execute an integration command and an integration command cannot execute an automation script

C. An automation script cannot execute an integration command and an integration command can execute an automation script

D. An automation script can execute an integration command and an integration command can execute an automation script

Correct Answer: *B*

Sarppp 1 year, 4 months ago

Correct answer is D.

upvoted 1 times

Jai_ke 4 months, 2 weeks ago

B is the right answer

upvoted 1 times

duduic 1 year, 3 months ago

go and try it. You'll see that it's B

upvoted 5 times

Question #55 *Topic 1*

Which two options will troubleshoot an integration's fetch incidents command? (Choose two.)

A. In the instance settings, enable the fetch incidents parameter and wait for one minute

B. Create a one task playbook with a fetch-incident command

C. execute !<integration_instance_name>-fetch

D. execute !<integration_name>-fetch

Correct Answer: *AC*
Reference:
https://xsoar.pan.dev/docs/integrations/fetching-incidents

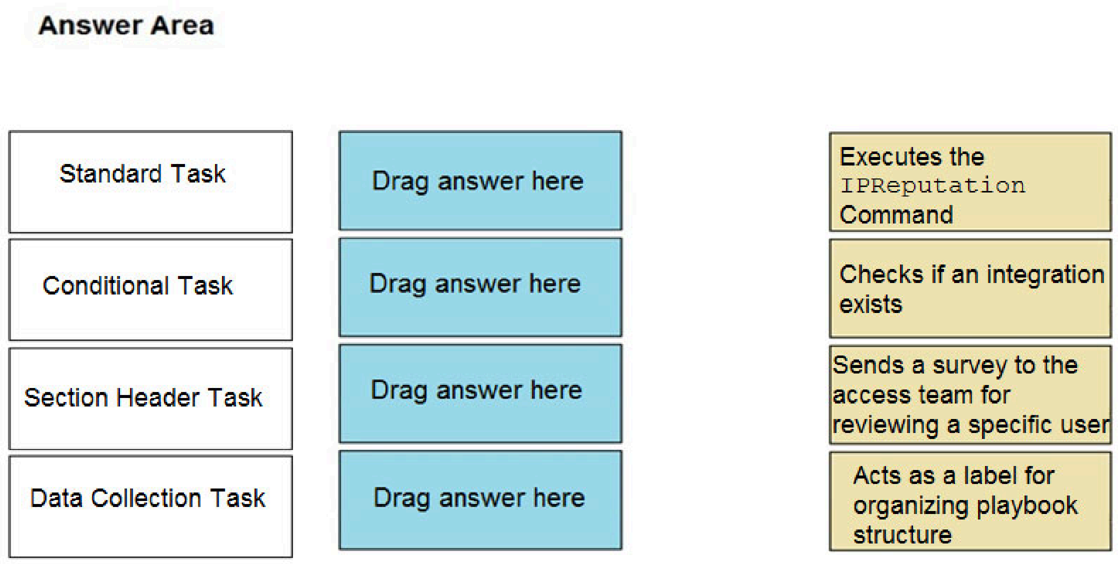
franko_72 6 months ago
Probably AC. When you run an instance to fetch, assuming it's set for 1 minute and not days etc, when it "attempts" to fetch it will show a result on the integrations page which you can click on to determine if successful or not.
upvoted 3 times

Question #56 *Topic 1*

DRAG DROP -

Match the corresponding action with the appropriate playbook tasks.

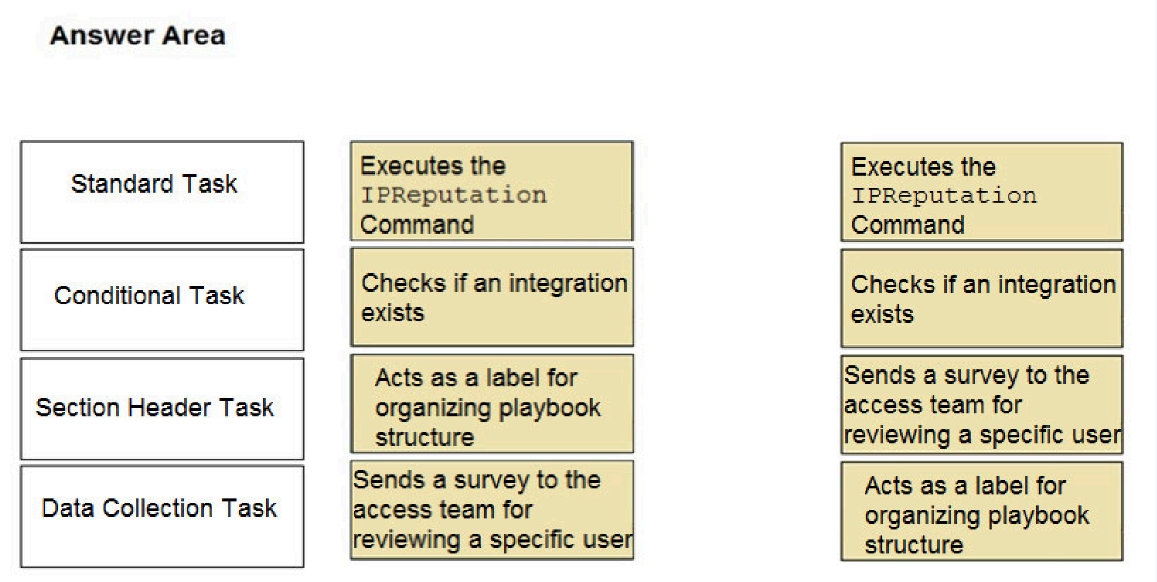
Select and Place:



Answer Area

Standard Task	Drag answer here	Executes the `IPReputation` Command
Conditional Task	Drag answer here	Checks if an integration exists
Section Header Task	Drag answer here	Sends a survey to the access team for reviewing a specific user
Data Collection Task	Drag answer here	Acts as a label for organizing playbook structure

Correct Answer:



Answer Area

Standard Task	Executes the `IPReputation` Command	Executes the `IPReputation` Command
Conditional Task	Checks if an integration exists	Checks if an integration exists
Section Header Task	Acts as a label for organizing playbook structure	Sends a survey to the access team for reviewing a specific user
Data Collection Task	Sends a survey to the access team for reviewing a specific user	Acts as a label for organizing playbook structure

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/playbooks-overview.html

Currently there are no comments in this discussion, be the first to comment!

Question #57 Topic 1

Incidents need to be filtered by all of the following criteria:
1. Status `" Pending
2. Exclude Category `" Job
3. Severity `" High
4. Owner `" None (No owner assigned)
5. Type `" Phishing
6. Email Subject `" `You have won a million dollars`
What is the correct query syntax for the above incident search filter?

A. status==ג€Pendingג€ && category!=ג€jobג€ && severity==ג€Highג€ && owner==ג€Noneג€ && type==ג€Phishingג€ && emailsubject==ג€You have won a million dollarsג€

B. Status:Pending and ג€"Category:job and Severity:High and Owner:ג€ג€ and Type:Phishing and Email Subject:You have won a million dollars

C. status:Pending and ג€"category:job and severity:High and owner:ג€ג€ and type:Phishing and emailsubject:ג€You have won a million dollarsג€

D. status:Pending or ג€"category:job or severity:High or owner:ג€ג€ or type:Phishing or emailsubject:ג€You have won a million dollarsג€

Correct Answer: *C*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/cortex-xsoar-overview/how-to-search-in-cortex-xsoar.html#idcd7fe505- c1c1-42f5-a698-08b5710196d3

Community vote distribution
C (100%)

Jai_ke 4 months, 1 week ago
Selected Answer: C
C is correct.
upvoted 1 times

franko_72 1 year, 5 months ago
I think it should look something like this:
status:Pending -category:job and severity:High owner: type:Phishing emailsubject:"You have won a million dollars"
upvoted 4 times

Question #58 *Topic 1*

What does Script helper contain?

A. Available commands

B. Permission settings

C. Automation version history

D. Automation timeout configuration

Correct Answer: *A*

Reference:

https://xsoar.pan.dev/docs/concepts/xsoar-ide

franko_72 5 months, 2 weeks ago

To see this, go to Automation, New Automation, Slick on Script Helper, choose the section/commands/script you need help with, for example, ad-add-to-group, click on it and select Copy to Script and >>demisto.executeCommand("ad-add-to-group", {"group-cn":"<group-cn>"})<< will be copied over, this can assist in building out your script!

upvoted 1 times

lucaboban 2 years, 6 months ago

A - Correct

upvoted 4 times

Question #59 *Topic 1*

When mapping incoming data to incident fields, which statement is correct?

A. Data that is not mapped is placed under labels

B. Only text fields are classified

C. Classification cannot be used if mapping is enabled

D. Every incoming field must be mapped

Correct Answer: *A*

Community vote distribution

A (100%)

amkoppad Highly Voted 3 years, 5 months ago

A is correct answer

upvoted 10 times

Jai_ke Most Recent 4 months, 2 weeks ago

Selected Answer: A

When incoming data is mapped to incident fields, any data that is not explicitly mapped to a predefined incident field is placed under labels

upvoted 1 times

duduic 1 year, 3 months ago

Selected Answer: A

a is the answer. I really don't know who pickes those answers...

upvoted 3 times

MarcoS10 1 year, 8 months ago

A is correct

upvoted 2 times

Question #60 *Topic 1*

Which two situations would an engineer consider when configuring classification and mapping for an incident type? (Choose two.)

A. When creating incidents from the XSOAR REST API

B. When manually creating an incident from the UI

C. When adding a new analyst account to XSOAR

D. When fetching many different incident types from a single mailbox

Correct Answer: *AB*

Community vote distribution

AD (100%)

amkoppad Highly Voted 👍 3 years, 5 months ago

A,D is the correct answer

upvoted 7 times

Jai_ke Most Recent 4 months, 1 week ago

Selected Answer: AD

A and D, as they directly relate to the incident creation and classification process

upvoted 1 times

Question #61 *Topic 1*

Which two options may be added when a content pack is being installed? (Choose two.)

A. Lists

B. Roles

C. Other content packs

D. Indicator layouts

Correct Answer: *CD*

Community vote distribution

CD (100%)

Jai_ke 4 months, 1 week ago

Selected Answer: CD

C. Other content packs:

Some content packs do require additional content packs as dependencies. While the content pack itself doesn’t contain other packs, the platform may prompt you to install these related packs to ensure full functionality.

D. Indicator layouts:

Content packs can include indicator layouts that adjust how indicators are viewed and managed within the platform.

upvoted 1 times

duduic 1 year, 3 months ago

Selected Answer: CD

c as in cardy and D as in not B

upvoted 3 times

MarcoS10 1 year, 8 months ago

CD is correct

upvoted 1 times

amkoppad 3 years, 5 months ago

Lol, C,D is the correct answer

upvoted 4 times

Question #62 *Topic 1*

Which three scripting languages can an engineer use to write XSOAR automations? (Choose three.)

A. Python

B. Perl

C. Go

D. JavaScript

E. Powershell

Correct Answer: *ADE*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/playbooks/automations.html

Community vote distribution

ADE (100%)

piipo 3 months, 2 weeks ago

Selected Answer: ADE

Correct

upvoted 1 times

lucaboban 3 years ago

ADE - Correct

upvoted 1 times

Question #63 *Topic 1*

What are two primary uses of standard tasks? (Choose two.)

A. To highlight different paths in a playbook

B. To generate new widgets for a dashboard

C. To create an incident or escalate an existing incident

D. To automate tasks such as parsing a file or enriching indicators

Correct Answer: *BD*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/playbooks/playbooks-overview.html

Community vote distribution

CD (100%)

amkoppad Highly Voted 👍 2 years, 11 months ago

C,D is correct

upvoted 6 times

piipo Most Recent ⏱ 3 months, 2 weeks ago

Selected Answer: CD

CD is correct

upvoted 2 times

Question #64 *Topic 1*

An engineer would like to change an incident's SLA according to the severity field changes.
How can the engineer achieve this task?

A. Use a field trigger script

B. Use a field display script

C. Create a job that queries for incident severity changes

D. Change the SLA manually every time the severity changes

Correct Answer: *A*

Community vote distribution

A (100%)

⊟ **amkoppad** Highly Voted 👍 3 years, 5 months ago

A is correct

upvoted 9 times

⊟ **Jai_ke** Most Recent 🕘 4 months, 2 weeks ago

Selected Answer: A

A field trigger script can be set up to automatically respond to changes in the severity field by updating the SLA based on predefined rules.

upvoted 1 times

⊟ **news088** 1 year, 2 months ago

A is correct. https://www.youtube.com/watch?v=UgkEVkdP5iY

upvoted 3 times

⊟ **MarcoS10** 1 year, 8 months ago

Selected Answer: A

A is correct

upvoted 3 times

⊟ **MarcoS10** 1 year, 8 months ago

A is correct

upvoted 3 times

Question #65 *Topic 1*

What are three different loop types in a playbook? (Choose three.)

A. Automation

B. Built-in

C. Data collection

D. Conditional

E. For-each

Correct Answer: *ABE*

Community vote distribution

ABE (100%)

patdiguangco 8 months ago

Selected Answer: ABE

https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.x/Cortex-XSOAR-Playbook-Design-Guide/Configure-a-Sub-playbook-Loop

upvoted 1 times

Jai_ke 4 months, 2 weeks ago

This is correct. A-B-E

upvoted 1 times

Deepu2710 1 year, 6 months ago

ABE IS CORRECT

upvoted 4 times

MarcoS10 1 year, 8 months ago

Selected Answer: ABE

ABE is correct

upvoted 2 times

Eruza89 2 years, 6 months ago

Agreed with lucaboban. ABE the answer

upvoted 3 times

amkoppad 3 years, 5 months ago

B,D,E is the correct answer

upvoted 1 times

lucaboban 3 years, 6 months ago

ABE - Correct

upvoted 4 times

Question #66 *Topic 1*

What are two common use cases for conditional tasks? (Choose two.)

A. They are used for branching paths in a playbook

B. They are used to interact with users through survey functionality

C. They are used to determine which incident will be executed

D. They are used for sending a specific question to a person or team

Correct Answer: *AC*

Reference:

https://docs-new.paloaltonetworks.com/cortex/cortex-xsoar/5-5/cortex-xsoar-admin/cortex-xsoar-overview/use-cases.html#id7b31e50b-5aca-4d65- bdb5-ba61b4eac0b4

Community vote distribution

AC (50%) AD (50%)

Jai_ke 4 months, 2 weeks ago

Selected Answer: AC

Why C? Conditional tasks can help decide which actions or incidents should be processed next based on predefined criteria or conditions.

upvoted 1 times

piipo 9 months, 2 weeks ago

Selected Answer: AD

AD is correct

upvoted 1 times

franko_72 1 year, 5 months ago

Yep, A,D

Conditional tasks can also be used to communicate with users through a **single** question survey, the answer to which determines how a playbook will proceed.

upvoted 1 times

john1208 1 year, 8 months ago

Agreed. A,D

upvoted 1 times

zoinx 3 years, 5 months ago

A,D is the correct answer

upvoted 2 times

Question #67 *Topic 1*

An engineer wants to customize the regex for the default IP indicator type.
How can this change be implemented?

A. Create a new indicator type and disable the built-in IP indicator

B. Edit the regex of the default IP Indicator

C. Add a new server configuration key that will overwrite the default regex of the IP indicator

D. Delete the default IP indicator

Correct Answer: *A*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/manage-indicators/understand-indicators/indicator-types/indicator-type- profile.html

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

In which two scenarios would it be appropriate to implement a loop for a sub-playbook? (Choose two.)

A. In repetitive process flows to iterate for each playbook input

B. When continuously ingesting incidents from third-party systems

C. In repetitive process flows with no more than 10 loops

D. In repetitive processes that requires sub-playbook re-execution

Correct Answer: *AD*

Community vote distribution

AD (100%)

amkoppad Highly Voted 3 years, 5 months ago

A,D is correct

upvoted 10 times

gabriel.alarcon0730 Most Recent 5 months, 1 week ago

Selected Answer: AD

A,D is correct

upvoted 2 times

MarcoS10 1 year, 8 months ago

Selected Answer: AD

AD is correct

upvoted 4 times

Question #69 *Topic 1*

Which configuration is a valid distributed database (DB) implementation?

A. 2 main DBs, 1 application server, 2 node servers

B. 1 main DB, 1 application server, 3 node servers

C. 2 application servers, 1 main DB, 1 node server

D. 1 application server, 2 main DBs, 1 node server

Correct Answer: *B*

Community vote distribution

B (100%)

amkoppad Highly Voted 👍 3 years, 5 months ago

B is correct

upvoted 7 times

Jai_ke Most Recent 🕒 4 months, 1 week ago

Selected Answer: B

Configurations like A, C, and D may not represent standard distributed database implementations due to their mix of components that do not align well with common practices in distributed database architecture. For instance, having two main databases might suggest replication or high availability setups, but this alone doesn't fit the typical distributed model as cleanly as option B.

upvoted 1 times

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: B

B is correct

upvoted 2 times

piipo 9 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

news088 1 year, 2 months ago

B is correct. https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.6/Cortex-XSOAR-Administrator-Guide/Best-Practices

upvoted 2 times

franko_72 1 year, 5 months ago

Answer is B. Not matter how many node servers you have there is always ONE app server. There only ever ONE main database server and the rest are NODE servers.

Search for Admin Guide 6.0-1.pdf page 79

upvoted 2 times

Question #70 *Topic 1*

An engineer would like to add a custom field to the New Job form for a job triggered from a threat intel feed.
How would the engineer implement this?

A. The new job form changes based on the threat intel feed integration configuration

B. The new job form can be edited from the Indicator Feed incident type editor

C. The new job form for a threat intel feed job cannot be edited

D. The new job form can be edited from the threat intel feeds integration settings

Correct Answer: *B*
Reference:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-threat-intel-management-guide/manage-indicators/understand-indicators/ create-a-feed-based-job.html

Community vote distribution
B (100%)

piipo 3 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

news088 8 months, 2 weeks ago

B is correct:
You can customize the new job form by editing the Indicator Feed incident type.
https://docs-cortex.paloaltonetworks.com/r/Cortex-XSOAR/6.5/Cortex-XSOAR-Threat-Intel-Management-Guide/Feed-Integrations

upvoted 3 times

nitishpop8895 10 months, 1 week ago

b is correct

upvoted 2 times

franko_72 11 months, 2 weeks ago

I think the answer is actually C. From the link below "The following table lists the fields available when defining a job, and their descriptions" There is no option to create a custom field.

https://xsoar.pan.dev/docs/incidents/incident-jobs

upvoted 2 times

Question #71 *Topic 1*

An automation returned an output called: csvReport.
What filter would be used to check if the automation returned results?

A. Contains/Includes

B. Equals/Matches

C. In/In list

D. Is defined/Exist

Correct Answer: *D*

Community vote distribution

D (100%)

amkoppad Highly Voted 3 years, 5 months ago

D is correct.

upvoted 7 times

[Removed] Most Recent 3 months, 3 weeks ago

Selected Answer: D

D is correct.

upvoted 1 times

Jai_ke 4 months, 1 week ago

Selected Answer: D

D is defined/Exist is the most appropriate choice.

upvoted 1 times

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 2 times

piipo 9 months, 2 weeks ago

Selected Answer: D

D Exist

upvoted 1 times

chucklepie 12 months ago

D, outputs only exist if they return something

upvoted 2 times

Question #72 *Topic 1*

What is the difference between labels and fields?

A. Fields can be used in playbooks and labels cannot

B. Fields are indexed in the database and labels are not

C. Labels can be used in queries and fields cannot

D. Labels are indexed in the database and fields are not

Correct Answer: *B*

Community vote distribution

B (100%)

Jai_ke 4 months, 2 weeks ago

Selected Answer: B

Fields are indexed and designed for efficient querying and processing, while labels are used more for categorization and tagging.

upvoted 1 times

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: B

Once you classify the incident, you can map the fields from the 3rd party integration to the fields that you defined in the incident layout. Any fields that you do not map, are automatically mapped to Cortex XSOAR labels.

https://xsoar.pan.dev/docs/incidents/incident-classification-mapping#map-event-attributes-to-fields

upvoted 1 times

duduic 1 year, 3 months ago

Selected Answer: B

B. Fields are indexed in the database and labels are not

this is correct

upvoted 2 times

duduic 1 year, 3 months ago

B. Fields are indexed in the database and labels are not

this is correct

upvoted 2 times

Question #73 *Topic 1*

What is the default task type when creating an empty task?

A. Standard (Manual)

B. Conditional

C. Section header

D. Standard (Automated)

Correct Answer: *A*

Community vote distribution

A (100%)

amkoppad Highly Voted 👍 3 years, 5 months ago

A is the correct answer.

upvoted 11 times

gabriel.alarcon0730 Most Recent ⊙ 5 months, 1 week ago

Selected Answer: A

Standard (Manual) is correct

upvoted 1 times

Monitor2 5 months, 1 week ago

A is the correct one

upvoted 1 times

chucklepie 12 months ago

Who is putting in these answers and why can't they be changed. this answer given is ridiculous

upvoted 2 times

duduic 1 year, 3 months ago

Selected Answer: A

A - Standard (Manual)

upvoted 3 times

SYZZY 1 year, 4 months ago

A is correct

upvoted 1 times

franko_72 1 year, 6 months ago

It's A - Standard (Manual)

A new task is Standard and unless you choose an automation, by default, the task when created has Manual Task Settings therefore it is Standard (Manual)

upvoted 2 times

PenguPC 2 years, 3 months ago

Is there a reference to which answer would be right?

upvoted 1 times

lucaboban 3 years, 6 months ago

B - Correct

upvoted 1 times

Question #74 *Topic 1*

Which two methods are used to add new content to the XSOAR Content Repository? (Choose two.)

A. Create content and add it to the standard content by contributing through the Marketplace

B. Use the XSOAR GitHub Contribution Guide to add the contribution to the standard content

C. Create a support ticket with the custom content for review by the support team

D. Any custom content will be automatically uploaded to the content repository

Correct Answer: *AB*

Community vote distribution

AB (100%)

amkoppad Highly Voted 3 years, 5 months ago

A,B is correct

upvoted 8 times

Jai_ke Most Recent 4 months, 2 weeks ago

Selected Answer: AB

Options C and D are not typical methods for adding new content to the repository.

upvoted 1 times

duduic 1 year, 3 months ago

Selected Answer: AB

A,B is correct

upvoted 3 times

Question #75 *Topic 1*

In which two options can an automation script be executed? (Choose two.)

A. Engine

B. Integration

C. War room

D. Playbook

Correct Answer: *CD*

Community vote distribution

CD (100%)

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: CD

C,D correct

upvoted 1 times

chucklepie 12 months ago

CD are correct, but there is nothing stopping you running an executeCommand inside an integration...

upvoted 1 times

duduic 1 year, 3 months ago

Selected Answer: CD

C,D Correct.

finally a correct answer...

upvoted 3 times

Jai_ke 4 months, 2 weeks ago

I know right?

upvoted 1 times

franko_72 1 year, 5 months ago

C,D Correct.

upvoted 2 times

Question #76 *Topic 1*

By default, automation written in which language will be executed in a Docker container?

A. Python

B. Go

C. JavaScript

D. Perl

Correct Answer: *A*

Community vote distribution

A (100%)

lucaboban Highly Voted 3 years, 6 months ago

A - Correct

upvoted 8 times

[Removed] Most Recent 3 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: A

A is correct

upvoted 1 times

duduic 1 year, 3 months ago

Selected Answer: A

A - Correct

GO isn't even supported

upvoted 4 times

asett 1 year, 3 months ago

Selected Answer: A

Go is not a supported XSOAR automation language

upvoted 2 times

SYZZY 1 year, 4 months ago

A. Python

upvoted 2 times

PenguPC 2 years, 3 months ago

A. Python

https://xsoar.pan.dev/docs/integrations/docker

upvoted 4 times

Question #77 *Topic 1*

What is the correct definition regarding integration parameters and command arguments?

A. Parameters are global variables which means that every command can use these configurable options in order to run. Arguments are shared with other commands and must be present for each command.

B. Parameters are local variables which means that every command can use these configurable options in order to run. Arguments are shared with other commands and must be present for each command.

C. Parameters are local variables which means that every command can use these configurable options in order to run. Arguments are specific to only one command.

D. Parameters are global variables which means that every command can use these configurable options in order to run. Arguments are specific to only one command.

Correct Answer: *D*

Community vote distribution

D (100%)

lucaboban Highly Voted 3 years, 6 months ago

D - Correct

upvoted 5 times

gabriel.alarcon0730 Most Recent 5 months, 1 week ago

Selected Answer: D

D is correct

upvoted 1 times

jasminsurani 2 years, 1 month ago

Selected Answer: D

D is the correct option.

upvoted 4 times

Question #78 *Topic 1*

In which two locations can filters and transformers be used in XSOAR? (Choose two.)

A. Classification and Mapping

B. Playbook Tasks

C. Evidence Fields

D. Incident Fields

Correct Answer: *BD*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/playbooks/filters-and-transformers.html

Community vote distribution

AB (100%)

⊟ **zoinx** Highly Voted 3 years, 5 months ago

A, B seems correct to me.

upvoted 9 times

⊟ **gabriel.alarcon0730** Most Recent 5 months, 1 week ago

Selected Answer: AB

A and B are correct

upvoted 1 times

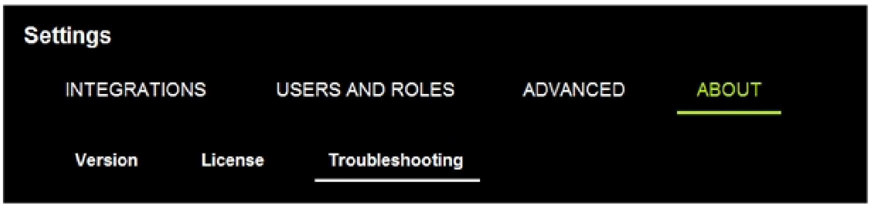
⊟ **news088** 1 year, 2 months ago

A, B test it on lab. No filter options for incidents fields nor evidence fields. Only under classification and mappings options.

upvoted 3 times

Question #79 Topic 1

Which three actions can an engineer take on the troubleshooting page? (Choose three.)



Settings

INTEGRATIONS USERS AND ROLES ADVANCED ABOUT

Version License Troubleshooting

A. Download the debug log bundle

B. Put the XSOAR server in maintenance mode

C. View and modify server configuration settings

D. Export and import custom content

E. View a list of server administrators

Correct Answer: *ACD*

Community vote distribution

ACD (100%)

amkoppad Highly Voted 3 years, 5 months ago

A,C,D is the correct answer

upvoted 8 times

franko_72 Highly Voted 1 year, 6 months ago

Yep A,C,D for sure.

upvoted 6 times

gabriel.alarcon0730 Most Recent 5 months, 1 week ago

Selected Answer: ACD

ACD is correct

upvoted 2 times

piipo 9 months, 2 weeks ago

Selected Answer: ACD

ACD is correct

upvoted 1 times

Question #80 *Topic 1*

An XSOAR Engineer has developed a playbook and would like to contribute it to the XSOAR Marketplace to share with other users.
Which two options are available to the Engineer for contributing to the Marketplace? (Choose two.)

A. Open a ticket with the XSOAR support team

B. Create a pull request directly on Github

C. Contribute through the XSOAR UI

D. Send an email to contributions@xsoar.com

Correct Answer: *BC*

Community vote distribution

BC (100%)

piipo 3 months, 1 week ago

Selected Answer: BC

BC is Correct

upvoted 1 times

franko_72 1 year ago

B and C

https://xsoar.pan.dev/docs/contributing/contributing

upvoted 3 times

PenguPC 1 year, 9 months ago

B and C|

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-1/cortex-xsoar-admin/marketplace/content-pack-contributions

upvoted 2 times

Question #81 *Topic 1*

Which two input requirements are needed to train a machine learning model? (Choose two.)

A. 3000 Incidents

B. Incident Field

C. Verdict Label

D. Incident Type

Correct Answer: *BD*

Reference:

https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/machine-learing-models/machine-learning-models-overview.html

Community vote distribution

BD (67%) BC (33%)

lucaboban Highly Voted 3 years, 6 months ago

B&D - Correct

upvoted 7 times

Jai_ke Most Recent 4 months, 1 week ago

Selected Answer: BC

While having a large dataset like A. 3000 Incidents can be beneficial for training a robust model, the specific fields and labels (B and C) are essential for the model to learn and make predictions. D. Incident Type might be relevant in some contexts, but it is not typically a direct input requirement for training a machine learning model.

upvoted 1 times

Jai_ke 4 months, 1 week ago

Sorry, I revise my answer. It is B and D.

upvoted 1 times

piipo 9 months, 2 weeks ago

Selected Answer: BD

Incident Field & Type

upvoted 2 times

franko_72 1 year, 6 months ago

It's B & D. In XSOAR click on Settings >> Advanced >> ML Models >> New Model >> and you need to specify the Incident Type and the Incident field which is B,D

upvoted 3 times

zoinx 3 years, 5 months ago

B, C is correct

upvoted 1 times

Question #82 *Topic 1*

Which two solutions are available to scale an overloaded XSOAR environment? (Choose two.)

A. Add a distributed database server

B. Add an indexing server

C. Add a live backup server (disaster recovery)

D. Add an engine

Correct Answer: *AD*

Community vote distribution

AD (100%)

amkoppad Highly Voted 👍 3 years, 5 months ago

A,D are the correct answers.

upvoted 7 times

[Removed] Most Recent 3 months, 3 weeks ago

Selected Answer: AD

AD correct

upvoted 1 times

Jai_ke 4 months, 2 weeks ago

Selected Answer: AD

Options B and C are not directly related to scaling but rather focus on indexing and disaster recovery.

upvoted 1 times

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: AD

AD correct

upvoted 1 times

piipo 9 months, 2 weeks ago

Selected Answer: AD

AD is correct

upvoted 1 times

Question #83 *Topic 1*

Management would like to get an incident report automatically following an incident's closure.
How would this be accomplished?

A. Define a task in a playbook to generate an incident report before the closure occurs

B. Manually create an 'Incident Report'

C. Configure post-processing using a script

D. Create an 'Incident Report' from the Reports page

Correct Answer: *D*

Community vote distribution

C (100%)

amkoppad Highly Voted 2 years, 11 months ago

C is the correct answer

upvoted 6 times

piipo Most Recent 3 months, 1 week ago

Selected Answer: C

post-processing

upvoted 1 times

Question #84 *Topic 1*

Which two reasons would lead an engineer to create a custom widget? (Choose two.)

A. To visualize server configuration keys

B. To visualize XSOAR list data

C. To visualize complex incident data calculations

D. To visualize context data

E. To visualize a custom query

Correct Answer: *CE*

Community vote distribution

CE (100%)

gabriel.alarcon0730 5 months, 1 week ago

Selected Answer: CE

C,E is correct

upvoted 1 times

piipo 9 months, 2 weeks ago

Selected Answer: CE

CE is correct

upvoted 2 times

Sarppp 1 year, 4 months ago

Answer is C,E

Admin guide page 6.0 329

you can create dynamic widgets using automation scripts for more complex calculations, such as calculating the percentage of incidents that DBot close

upvoted 4 times