Question #1 *Topic 1*

The Add-On Builder creates Splunk Apps that start with what?

A. DA-

B. SA-

C. TA-

D. App-

Suggested Answer: *C*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

javo_dlg 2 years, 2 months ago
C is the correct answer
upvoted 2 times

andy73 2 years, 12 months ago
C is correct
upvoted 2 times

BMO 3 years, 6 months ago
C is correct answer
upvoted 3 times

Question #2 *Topic 1*

Which of the following are examples of sources for events in the endpoint security domain dashboards?

A. REST API invocations.

B. Investigation final results status.

C. Workstations, notebooks, and point-of-sale systems.

D. Lifecycle auditing of incidents, from assignment to resolution.

Suggested Answer: *D*

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

Community vote distribution

C (100%)

kkrises 1 year, 10 months ago

C is correct

upvoted 1 times

Bittu22 1 year, 11 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

huu_nguyen 2 years, 1 month ago

Selected Answer: C

C for sure

upvoted 1 times

niuksas 2 years, 1 month ago

Selected Answer: C

The correct answer is C

upvoted 3 times

andy73 2 years, 12 months ago

C is correct

upvoted 2 times

ectomorph 3 years, 1 month ago

Correct Answer = C

upvoted 2 times

oksey 4 years, 1 month ago

C is the correct Ans

upvoted 4 times

Question #3 *Topic 1*

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?

A. $fieldname$

B. ג€fieldnameג€

C. %fieldname%

D. _fieldname_

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

Community vote distribution
A (100%)

prich1111 Highly Voted 3 years, 3 months ago
Answer is A
upvoted 8 times

bpareja Most Recent 1 year, 9 months ago
Selected Answer: A
Answer is A
upvoted 1 times

kkrises 1 year, 10 months ago
A is the correct answer and is called variable substitution. $value$
upvoted 2 times

niuksas 2 years, 1 month ago
Selected Answer: A
The correct answer is A
upvoted 1 times

andy73 2 years, 12 months ago
A is correct
upvoted 1 times

ectomorph 3 years, 1 month ago
Correct answer is A
upvoted 2 times

Question #4 *Topic 1*

What feature of Enterprise Security downloads threat intelligence data from a web server?

A. Threat Service Manager

B. Threat Download Manager

C. Threat Intelligence Parser

D. Threat Intelligence Enforcement

Suggested Answer: *B*

andy73 2 years, 12 months ago

B is correct

upvoted 1 times

BMO 3 years, 6 months ago

B is correct

Admin ES - Slide 356

upvoted 3 times

SandMan 3 years, 9 months ago

Answer is B

"The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files & data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called “threatlist”."

upvoted 2 times

Question #5 *Topic 1*

The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data.
What data model should be checked for potential errors such as skipped searches?

A. Web

B. Risk

C. Performance

D. Authentication

Suggested Answer: *A*
Reference:
https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

Community vote distribution
D (100%)

dinesh_splunk Highly Voted 3 years, 2 months ago
correct answer is D authentication.
upvoted 8 times

dohatelo Most Recent 7 months, 2 weeks ago
This is the search powering this dashboard, so it's a clear answer D "Authentication" :

| tstats `summariesonly` count from datamodel=Authentication.Authentication where Authentication.user=$ds_input_tokens:result.user$ $ds_input_tokens:result.remote_user_bunit$ by Authentication.src,Authentication.user | `drop_dm_object_name("Authentication")`| `get_identity4events(user)` | rename user_watchlist as watchlist | search $ds_input_tokens:result.watchlist_raw$ | `get_asset(src)` | iplocation src | eval session_city=if(isnull(src_city), City,src_city) | eval session_country=if(isnull(src_country), Country,src_country) | where isnotnull(session_city) AND isnotnull(user_work_city) AND (lower(user_work_city)!=lower(session_city) OR lower(user_work_country)!=lower(session_country)) | fields user, src, session_city, session_country, user_work_city, user_work_country | sort 100 -count
upvoted 1 times

Brilliantel2 10 months, 2 weeks ago
Selected Answer: D
The Correct answer is D
upvoted 1 times

esdee3 1 year, 1 month ago
Selected Answer: D
D is the correct answer
upvoted 1 times

niuksas 2 years, 1 month ago
Selected Answer: D
The correct answer is D
upvoted 2 times

jassthefab 2 years, 5 months ago
The correct answer is D. Verified in the Splunk ES app.
upvoted 1 times

andy73 2 years, 12 months ago
D is correct
upvoted 1 times

mi5 3 years ago
User Activity dashboard uses multiple DM, but remote access panel is using Authentication datamodel so D is correct option.
upvoted 1 times

Question #6 *Topic 1*

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?

A. Save the settings.

B. Apply the correct tags.

C. Run the correct search.

D. Visit the CIM dashboard.

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata

Community vote distribution

B (100%)

BMO Highly Voted 3 years, 6 months ago

B is correct

Admin ES - Slide 215

upvoted 11 times

wasssss Most Recent 3 months, 3 weeks ago

B is correct

upvoted 1 times

adamsca 6 months, 3 weeks ago

Selected Answer: B

B is Correct

upvoted 1 times

huu_nguyen 2 years, 1 month ago

B is correct.

The order would be: Eventtypes -> Tags -> Data model definition -> Data model acceleration -> Searches

upvoted 3 times

andy73 2 years, 12 months ago

C is correct

upvoted 1 times

Hudda 3 years, 4 months ago

Friends, could you please confirm this answer?

upvoted 1 times

QueenNile 3 years, 5 months ago

Correct answer is C.

upvoted 2 times

ames 4 years, 2 months ago

Correct. This is done to verify that your field extractions function correctly.

upvoted 3 times

Question #7 *Topic 1*

What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A. ess_user

B. ess_admin

C. ess_analyst

D. ess_reviewer

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Triagenotableevents

Community vote distribution
C (100%)

pock3ts Highly Voted 2 years, 5 months ago
Selected Answer: C
C is correct
upvoted 5 times

vasudvn Most Recent 11 months, 1 week ago
Selected Answer: C
ess_analyst can own the notable
upvoted 1 times

Bittu22 1 year, 11 months ago
The ability to change notable event statuses is available to the ess_analyst and ess_admin roles by default.
upvoted 1 times

brockmoon56 1 year, 11 months ago
Should be C. Technically an Admin can be able to do it all, but the responsibility should lie with the ess_analyst. The admin would inherit it as a higher role.
upvoted 1 times

niuksas 2 years, 1 month ago
Selected Answer: C
The correct answer is C
upvoted 4 times

andy73 2 years, 12 months ago
C is correct
upvoted 2 times

guirax 2 years, 12 months ago
C is the correct

ES Analyst
ess_analyst
Owns notable events
and performs notable
event status changes

Administering Splunk Enterprise Security page 20
upvoted 2 times

CurryMuncher 3 years, 5 months ago
SORRY C is the correct answer
I made a mistake earlier. Answer is C
upvoted 2 times

CurryMuncher 3 years, 5 months ago

B is the correct answer -

upvoted 2 times

BMO 3 years, 6 months ago

C is correct

Admin ES - Slide 20

upvoted 2 times

Imcool 3 years, 9 months ago

ess_analyst is also true, and from a best practices perspective it is better to assign this one instead of admin no ?

upvoted 2 times

Question #8 *Topic 1*

Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?

A. VIP

B. Priority

C. Importance

D. Criticality

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

andy73 2 years, 12 months ago
B is correct
upvoted 3 times

ectomorph 3 years, 1 month ago
B is correct but the question is worded incorrectly. Urgency is defined by priority of the asset or identity and the severity of the event (not the security)
upvoted 4 times

_adem 3 years, 1 month ago
B
upvoted 1 times

Question #9 *Topic 1*

What does the risk framework add to an object (user, server or other type) to indicate increased risk?

A. An urgency.

B. A risk profile.

C. An aggregation.

D. A numeric score.

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskScoring

Community vote distribution
D (100%)

jaemon22 6 months ago

Selected Answer: D

The risk framework in Splunk Enterprise Security adds a numeric score to an object (user, server, or other type) to indicate increased risk. This score quantifies the level of risk associated with the object, allowing security teams to prioritize their responses based on the severity of the risk.

upvoted 1 times

kkrises 1 year, 10 months ago

Correct answer is D

upvoted 1 times

huu_nguyen 2 years, 1 month ago

D is correct

upvoted 1 times

niuksas 2 years, 1 month ago

Selected Answer: D

The correct answer is D

upvoted 2 times

andy73 2 years, 12 months ago

D is correct

upvoted 2 times

_adem 3 years, 1 month ago

Ans: A numeric score.
Ref: https://docs.splunk.com/Documentation/ES/latest/User/RiskScoring

upvoted 2 times

1qaz2wsx 3 years, 1 month ago

D is answer

upvoted 4 times

Hudda 3 years, 4 months ago

It should be C, do you have any source for saying D? pls provide

upvoted 1 times

oksey 4 years, 2 months ago

I think D is the Ans

upvoted 3 times

ames 4 years, 2 months ago

I would say D

upvoted 3 times

Question #10 *Topic 1*

Which indexes are searched by default for CIM data models?

A. notable and default

B. summary and notable

C. _internal and summary

D. All indexes

Suggested Answer: *D*
Reference:
https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

andy73 2 years, 12 months ago
D is correct
upvoted 3 times

BMO 3 years, 6 months ago
D is correct
Admin ES - Slide 217
upvoted 4 times

SandMan 3 years, 9 months ago
Answer is D
"By default a datamodel will search across all indexes."
upvoted 1 times

Question #11 *Topic 1*

Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath

B. tstatsHomePath

C. summaryHomePath

D. warmToColdScript

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

sylax 2 years, 4 months ago
Correct Answer: B
Pg. 327 on the Administering Splunk Enterprise Security 7.0
upvoted 2 times

asashima 2 years, 11 months ago
Correct Answer: B
Pg. 331 on the Administering Splunk Enterprise Security 6.6
upvoted 1 times

andy73 2 years, 12 months ago
B is correct
upvoted 1 times

_adem 3 years, 1 month ago
Ans: tstatsHomePath
Ref: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels
upvoted 3 times

BhanuAyikam 3 years, 2 months ago
B is correct
upvoted 1 times

Question #12 *Topic 1*

Which of the following is a way to test for a property normalized data model?

A. Use Audit -> Normalization Audit and check the Errors panel.

B. Run a | datamodel search, compare results to the CIM documentation for the datamodel.

C. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.

D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizedataatsearchtime

andy73 2 years, 12 months ago
B is correct
upvoted 2 times

BhanuAyikam 3 years, 2 months ago
B is the answer
upvoted 4 times

Question #13 *Topic 1*

Which argument to the | tstats command restricts the search to summarized data only?

A. summaries=t

B. summaries=all

C. summariesonly=t

D. summariesonly=all

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

SandMan Highly Voted 3 years, 9 months ago

Answer is C
https://docs.splunk.com/Documentation/Splunk/8.1.2/SearchReference/Tstats
- Uses the summariesonly argument to get the time range of the summary for an accelerated data model named mydm.
- | tstats summariesonly=t min(_time) AS min, max(_time) AS max FROM datamodel=mydm

upvoted 7 times

andy73 Most Recent 2 years, 12 months ago

C is correct

upvoted 2 times

Question #14 *Topic 1*

When investigating, what is the best way to store a newly-found IOC?

A. Paste it into Notepad.

B. Click the ג€Add IOCג€ button.

C. Click the ג€Add Artifactג€ button.

D. Add it in a text note to the investigation.

Suggested Answer: *B*

Community vote distribution

C (100%)

BhanuAyikam Highly Voted 3 years, 2 months ago

C is the correct answers

There is no button called Add IOC so B is not correct

upvoted 9 times

esdee3 Most Recent 1 year, 1 month ago

Selected Answer: C

C is the answer. I have not seen any button called ADD IOC

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: C

C. Click the "Add Artifact" button.

upvoted 1 times

kkrises 1 year, 10 months ago

D is the answer - Text note option

upvoted 1 times

andy73 2 years, 12 months ago

C is correct

upvoted 1 times

Question #15 *Topic 1*

How is it possible to navigate to the list of currently-enabled ES correlation searches?

A. Configure -> Correlation Searches -> Select Status ɹ€Enabledɹ€

B. Settings -> Searches, Reports, and Alerts -> Filter by Name of ɹ€Correlationɹ€

C. Configure -> Content Management -> Select Type ɹ€Correlationɹ€ and Status ɹ€Enabledɹ€

D. Settings -> Searches, Reports, and Alerts -> Select App of ɹ€SplunkEnterpriseSecuritySuiteɹ€ and filter by ɹ€-Ruleɹ€

Suggested Answer: *A*

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Listcorrelationsearches

Community vote distribution

C (100%)

Glat Highly Voted 3 years, 2 months ago

C is the answer.

Configure > Content > Content management in Enterprise Security

upvoted 12 times

adamsca Most Recent 6 months ago

Selected Answer: C

C is Correct

Configure > Content > Content management

upvoted 1 times

dohatelo 7 months, 2 weeks ago

C is the correct one

upvoted 1 times

spl_consumer 1 year, 11 months ago

Selected Answer: C

Answer C

upvoted 3 times

huu_nguyen 2 years, 1 month ago

Vote for C

upvoted 2 times

andy73 2 years, 12 months ago

C is correct

upvoted 4 times

Question #16 *Topic 1*

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?

A. Indexers might crash.

B. Indexers might be processing.

C. Indexers might not be reachable.

D. Indexers have different settings.

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf

Community vote distribution
D (67%) C (33%)

jaemon22 5 months, 4 weeks ago

Selected Answer: C

A risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf is that indexers might not be reachable. If an indexer is not reachable during the deployment, it may not receive the updated configurations, leading to inconsistencies in the environment.

upvoted 1 times

huu_nguyen 2 years, 1 month ago

Selected Answer: D

Vote for D

upvoted 2 times

andy73 2 years, 12 months ago

D is correct

upvoted 2 times

Hudda 3 years, 4 months ago

Friends, could you please confirm this answer?

upvoted 1 times

learner321 3 years, 4 months ago

I think D is the right answer
https://community.splunk.com/t5/Splunk-Enterprise-Security/Splunk-Enterprise-Security-requires-a-deployment-client-but/m-p/279749

upvoted 4 times

kerb 4 years, 1 month ago

I believe D is the right answer

upvoted 4 times

TASOOMRO 4 years ago

Hi Kerb,
Could you please explain briefly how D is correct NOT A. I also have doubts A is no way correct.

upvoted 1 times

Question #17 *Topic 1*

Which of the following are data models used by ES? (Choose all that apply.)

A. Web

B. Anomalies

C. Authentication

D. Network Traffic

Suggested Answer: *B*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/datamodelsusedbyes/

Glat Highly Voted 3 years, 2 months ago
Answer is A, C and D
upvoted 14 times

dohatelo Most Recent 7 months, 2 weeks ago
correct is A, C, D
upvoted 1 times

Oldergranite 2 years, 6 months ago
Answer is A, C and D.
upvoted 1 times

SriAkula 2 years, 11 months ago
Answer: A,C and D
upvoted 1 times

dinesh_splunk 3 years, 2 months ago
https://docs.splunk.com/Documentation/CIM/4.20.2/User/CIMfields
upvoted 2 times

Question #18 *Topic 1*

At what point in the ES installation process should Splunk_TA_ForIndexers.spl be deployed to the indexers?

A. When adding apps to the deployment server.

B. Splunk_TA_ForIndexers.spl is installed first.

C. After installing ES on the search head(s) and running the distributed configuration management tool.

D. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and the splunk apply cluster-bundle command.

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

Community vote distribution
D (67%) C (33%)

BMO Highly Voted 3 years, 6 months ago
C is correct
Admin ES - Slide 161
upvoted 8 times

kiragi Most Recent 1 month ago
Selected Answer: C
answer is C, ES must be installed on the search head to collect the TA for indexers
upvoted 1 times

jaemon22 5 months, 4 weeks ago
Selected Answer: C
After installing Splunk Enterprise Security (ES) on the search head(s) and running the distributed configuration management tool, you should deploy Splunk_TA_ForIndexers.spl to the indexers. This ensures that the necessary configurations and knowledge objects are properly distributed and applied to the indexers.
upvoted 1 times

dohatelo 7 months, 2 weeks ago
Correct answer D ! See instructions from Admin ES: • Install ES on the Deployer
1. On the Splunk toolbar, select Apps > Manage Apps and click
Install app from file
2. Click Choose File and select the Splunk Enterprise Security file
3. Click Upload to begin the installation
4. Click Continue to app setup page
5. Click Start Configuration Process, and wait for it to complete
6. Use the Deployer to deploy ES to the cluster members. From the Deployer
run: splunk apply shcluster-bundle
upvoted 2 times

vasudvn 11 months, 1 week ago
Selected Answer: D
Splunk_TA_ForIndexers.spl is created only for clustered indexer environment
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons#Create_the_Splunk_TA_ForIndexers_and_manage_deployment_manually
upvoted 2 times

andy73 2 years, 12 months ago
C is correct
upvoted 3 times

oksey 4 years, 2 months ago
C is the Ans

upvoted 4 times

Question #19 *Topic 1*

Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.

B. Window interval.

C. Window duration.

D. Schedule window.

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

Community vote distribution
C (100%)

andy73 Highly Voted 2 years, 12 months ago
C is correct
upvoted 6 times

kkrises Most Recent 1 year, 10 months ago
Windows duration - C is the correct answer
upvoted 3 times

spl_consumer 1 year, 11 months ago
Selected Answer: C
Throttling
Window duration
second(s)
How much time to ignore other events that match the field values specified in Fields to group by.
Fields to group by
>>>> Copy from web UI <<<<<
upvoted 4 times

QueenNile 3 years, 5 months ago
Correct, the answer is C.
upvoted 4 times

Question #20 *Topic 1*

Both `Recommended Actions` and `Adaptive Response Actions` use adaptive response. How do they differ?

A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.

B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.

C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.

D. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

Community vote distribution
B (100%)

mybox1 Highly Voted 3 years, 3 months ago
Confirm, B is correct
upvoted 6 times

andy73 Highly Voted 2 years, 12 months ago
B is correct
upvoted 5 times

c2mp2 Most Recent 9 months, 2 weeks ago
Selected Answer: B
B is correct.
upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago
B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.
upvoted 1 times

_adem 3 years, 1 month ago
Ans: B
"Identifying Recommended Adaptive Responses will highlight those actions for the analyst when looking at the list of response actions available, making it easier to find them among the longer list of available actions."
upvoted 5 times

Hudda 3 years, 4 months ago
I think it is D
upvoted 1 times

Hudda 3 years, 4 months ago
Friends, any other thoughts?
upvoted 1 times

lmcool 3 years, 9 months ago
Answer Is B
upvoted 4 times

Question #21 *Topic 1*

What does the Security Posture dashboard display?

A. Active investigations and their status.

B. A high-level overview of notable events.

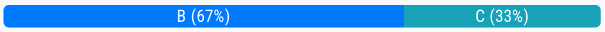
C. Current threats being tracked by the SOC.

D. A display of the status of security tools.

Suggested Answer: *B*

The Security Posture dashboard is designed to provide high-level insight into the notable events across all domains of your deployment, suitable for display in a
Security Operations Center (SOC). This dashboard shows all events from the past 24 hours, along with the trends over the past 24 hours, and provides real-time event information and updates.
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/SecurityPosturedashboard

Community vote distribution



jaemon22 6 months ago

Selected Answer: C

In Splunk Enterprise Security, an asset typically refers to IP addresses, hostnames, and MAC addresses, which are used to identify and categorize different devices and systems within the network.

upvoted 1 times

dohatelo 7 months, 2 weeks ago

B is correct

upvoted 1 times

andy73 2 years, 12 months ago

B is correct

upvoted 3 times

mi5 3 years ago

Selected Answer: B

B is correct

upvoted 2 times

Question #22 *Topic 1*

`10.22.63.159`, `websvr4`, and `00:26:08:18: CF:1D` would be matched against what in ES?

A. A user.

B. A device.

C. An asset.

D. An identity.

Suggested Answer: *B*

Community vote distribution

C (67%) B (33%)

prich1111 Highly Voted 3 years, 3 months ago

Answer is C

upvoted 9 times

8e3ad88 Most Recent 4 months ago

Selected Answer: C

Definitely asset.

upvoted 1 times

jaemon22 6 months ago

It's C an asset, In Splunk Enterprise Security, an asset typically refers to IP addresses, hostnames, and MAC addresses, which are used to identify and categorize different devices and systems within the network.

upvoted 1 times

dohatelo 7 months, 2 weeks ago

Answer is C:

Explanation:
"10.22.63.159", "websvr4", and "00:26:08:18: CF:1D" would be matched against an asset in ES. An asset is a device on a network that can be identified by an IP address, MAC address, DNS name, or other attributes. ES uses an asset and identity system to correlate asset and identity information with events to enrich and provide context to the data1. The asset fields that ES can match include ip, mac, nt_host, dns, and others2. An identity is a user account that can be identified by a username, email address, phone number, or other attributes. An identity is not the same as an asset, although an identity can be associated with an asset1. References =

Add asset and identity data to Splunk Enterprise Security
Asset and identity fields in Splunk Enterprise Security

upvoted 2 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: C

C. An asset.

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: B

Suggested Answer

upvoted 1 times

huu_nguyen 2 years, 1 month ago

C for sure

upvoted 1 times

guirax 2 years, 12 months ago

Answers is C

Asset field matching settings

– Name - which headers/fields in a lookup table to match during the merge process
– Key - like ip (key), field is used in merge process
– Tag - field can be used as an asset tag
– Multivalue - field can output multiple values
– Multivalue Limit - number of values in a multivalue field merge

Administering Splunk Enterprise Security page 276
upvoted 1 times

andy73 2 years, 12 months ago
C is correct
upvoted 1 times

Question #23 *Topic 1*

How should an administrator add a new lookup through the ES app?

A. Upload the lookup file in Settings -> Lookups -> Lookup Definitions

B. Upload the lookup file in Settings -> Lookups -> Lookup table files

C. Add the lookup file to /etc/apps/SplunkEnterpriseSecuritySuite/lookups

D. Upload the lookup file using Configure -> Content Management -> Create New Content -> Managed Lookup

Suggested Answer: *D*

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

Community vote distribution

D (100%)

jaemon22 6 months ago

answer should be B

This allows you to upload the lookup file so it can be managed and used within Splunk Enterprise Security.

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: D

Suggested Answer: D

upvoted 2 times

sylax 2 years, 4 months ago

Selected Answer: D

pg 242 Administering Splunk Enterprise Security 7.0

upvoted 4 times

andy73 2 years, 12 months ago

D is correct

upvoted 3 times

mi5 3 years ago

Selected Answer: D

D is right

upvoted 3 times

Question #24 *Topic 1*

Glass tables can display static images and text, the results of ad-hoc searches, and which of the following objects?

A. Lookup searches.

B. Summarized data.

C. Security metrics.

D. Metrics store searches.

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

QueenNile Highly Voted 3 years, 5 months ago
C is correct. https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable
upvoted 7 times

tmmt Most Recent 1 year, 8 months ago
In ES 7 dashboard replace glass tables.
upvoted 2 times

andy73 2 years, 12 months ago
C is correct
upvoted 2 times

Question #25 *Topic 1*

Which of the following is a key feature of a glass table?

A. Rigidity.

B. Customization.

C. Interactive investigations.

D. Strong data for later retrieval.

Suggested Answer: *B*

1M4hqQ9G 1 year, 11 months ago

yup, its B

upvoted 1 times

huu_nguyen 2 years, 1 month ago

B for sure

upvoted 1 times

andy73 2 years, 12 months ago

B is correct

upvoted 3 times

Question #26 *Topic 1*

An administrator is asked to configure an `Nslookup` adaptive response action, so that it appears as a selectable option in the notable event's action menu when an analyst is working in the Incident Review dashboard.
What steps would the administrator take to configure this option?

A. Configure -> Content Management -> Type: Correlation Search -> Notable -> Nslookup

B. Configure -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

C. Configure -> Content Management -> Type: Correlation Search -> Notable -> Next Steps -> Nslookup

D. Configure -> Content Management -> Type: Correlation Search -> Notable -> Recommended Actions -> Nslookup

Suggested Answer: *D*

Community vote distribution

andy73 Highly Voted 2 years, 12 months ago

D is correct

upvoted 7 times

qtygbapjpesdayazko Most Recent 1 year, 7 months ago

Selected Answer: D

Suggested Answer: D

upvoted 1 times

huu_nguyen 2 years, 1 month ago

Selected Answer: D

D is the one

upvoted 3 times

mi5 3 years ago

D is correct

upvoted 4 times

Question #27 *Topic 1*

What are the steps to add a new column to the Notable Event table in the Incident Review dashboard?

A. Configure -> Incident Management -> Notable Event Statuses

B. Configure -> Content Management -> Type: Correlation Search

C. Configure -> Incident Management -> Incident Review Settings -> Event Management

D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Customizenotables

Community vote distribution

D (100%)

oksey Highly Voted 4 years, 2 months ago

The Ans is D not C

upvoted 10 times

meeha Highly Voted 3 years, 11 months ago

Answer is D

upvoted 8 times

leezanelatto Most Recent 1 year, 4 months ago

Answer is D

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: D

D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: D

D. Configure -> Incident Management -> Incident Review Settings -> Table Attributes

upvoted 1 times

spl_consumer 1 year, 11 months ago

Selected Answer: D

Incident Review - Table Attributes

An ordered list of attributes displayed as columns on the Incident Review dashboard.

Press arrow up or arrow down to re-order items.... copied from WEB UI

upvoted 2 times

Adam98870 1 year, 11 months ago

D is right

upvoted 1 times

asashima 2 years, 11 months ago

Correct Answer: D

Pg. 40 on the Administering Splunk Enterprise Security 6.6

upvoted 2 times

andy73 2 years, 12 months ago

D is correct

upvoted 1 times

ectomorph 3 years, 1 month ago

Answer is D:

https://docs.splunk.com/Documentation/ES/6.1.0/Admin/CustomizeIR

Change Incident Review columns
You can change the columns displayed on the Incident Review dashboard.

Review the existing columns in Incident Review - Table Attributes.
Use the action column to edit, remove, or change the order of the available columns.
Add custom columns by selecting Insert below or selecting More..., then Insert above.
upvoted 2 times

Hudda 3 years, 4 months ago
Do you have any prof links?
upvoted 1 times

Question #28 *Topic 1*

To observe what network services are in use in a network's activity overall, which of the following dashboards in Enterprise Security will contain the most relevant data?

A. Intrusion Center

B. Protocol Analysis

C. User Intelligence

D. Threat Intelligence

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/NetworkProtectionDomaindashboards

Community vote distribution
B (100%)

oksey Highly Voted 4 years, 2 months ago
The Ans Is Protocol Analysis, B
upvoted 14 times

b5white Most Recent 3 months ago
Selected Answer: B
There isn't a Protocol Analysis dashboard, but there is a Protocol Center where you can do analysis, and some of the other dashboards in that group *are* called Analysis. Clearly none of the other 3 are correct. So I think it has to be B.
upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago
Selected Answer: B
B. Protocol Analysis
upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago
Selected Answer: B
B. Protocol Analysis
upvoted 1 times

kkrises 1 year, 10 months ago
Potentially A would be the correct answer as we have only Protocol Intelligence dashboard which is not in the option.
upvoted 1 times

andy73 2 years, 12 months ago
B is correct
upvoted 3 times

ectomorph 3 years, 1 month ago
Answer is B (kinda) Protocol Center:

https://docs.splunk.com/Documentation/ES/6.6.2/User/ProtocolIntelligence
upvoted 1 times

1qaz2wsx 3 years, 2 months ago
where is Protocol Analysis dashboard in ES?
I think correct answer is A
upvoted 1 times

Hudda 3 years, 4 months ago
i think it should be D. any comments friends.
upvoted 1 times

dinesh_splunk 3 years, 2 months ago

no, B is the correct answer

upvoted 1 times

1qaz2wsx 3 years, 2 months ago

where find in document any Protocol Analysis dashboard? why is B answer is correct? there is protocol center dashboard only

upvoted 1 times

Question #29 *Topic 1*

Adaptive response action history is stored in which index?

A. cim_modactions

B. modular_history

C. cim_adaptiveactions

D. modular_action_history

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

Community vote distribution
A (100%)

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: A

cim_modactions

upvoted 1 times

jassthefab 2 years, 5 months ago

Selected Answer: A

A is correct.
Reference: https://docs.splunk.com/Documentation/CIM/5.0.1/User/Install

upvoted 3 times

andy73 2 years, 12 months ago

A is correct

upvoted 1 times

mybox1 3 years, 3 months ago

A is correct

upvoted 1 times

Hudda 3 years, 4 months ago

any comments on this Q friends?

upvoted 1 times

Question #30 *Topic 1*

Which of the following actions would not reduce the number of false positives from a correlation search?

A. Reducing the severity.

B. Removing throttling fields.

C. Increasing the throttling window.

D. Increasing threshold sensitivity.

Suggested Answer: *A*

Community vote distribution

oksey Highly Voted 4 years, 2 months ago

A is correct not B

upvoted 7 times

c2mp2 Most Recent 9 months, 3 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

RIchardMatos 1 year, 5 months ago

Selected Answer: C

Increasing the throttling window: Throttling window defines the time period during which events are considered for correlation. Increasing the throttling window allows for a broader time range of events to be considered, which can help in better identifying true correlations and reducing false positives.

upvoted 1 times

RIchardMatos 1 year, 5 months ago

Sorry, correcting here option A is correct :

A. Reducing the severity.

Reducing the severity would not directly impact the number of false positives in a correlation search. Severity is typically used to assign a level of importance or priority to events or alerts, but it doesn't affect the accuracy or false positive rate of the correlation search itself.

upvoted 2 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: C

C. Increasing the throttling window: This option may help reduce false positives. The throttling window determines how long related events are grouped together. If the window is too short, unrelated events may be grouped together, generating false positives. If the window is too long, legitimate events may be excluded from the group. Increasing the window may allow more legitimate events to be grouped together, reducing the number of false positives.

upvoted 1 times

Ntani 1 year, 9 months ago

A is correct

upvoted 2 times

noysherer 2 years, 11 months ago

Can someone please explain this?

upvoted 1 times

andy73 2 years, 12 months ago

A is correct

upvoted 2 times

_adem 3 years, 1 month ago

A is correct

upvoted 1 times

oksey 4 years, 2 months ago

I am not sure but I think B will do the job

upvoted 1 times

1qaz2wsx 3 years, 2 months ago

"not reduce"

upvoted 1 times

Question #31 *Topic 1*

Where is the Add-On Builder available from?

A. GitHub

B. SplunkBase

C. www.splunk.com

D. The ES installation package

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

Ntani 1 year, 9 months ago
B is correct
upvoted 1 times

huu_nguyen 2 years, 1 month ago
B. It's from Splunkbase
upvoted 2 times

andy73 2 years, 12 months ago
B is correct
upvoted 4 times

Question #32 *Topic 1*

Which of the following would allow an add-on to be automatically imported into Splunk Enterprise Security?

A. A prefix of CIM_

B. A suffix of .spl

C. A prefix of TECH_

D. A prefix of Splunk_TA_

Suggested Answer: *D*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

inwigboji 1 month, 4 weeks ago
D is the right answer
upvoted 1 times

andy73 2 years, 12 months ago
D is correct
upvoted 2 times

Question #33 *Topic 1*

ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?

A. $SPLUNK_HOME/etc/master-apps/

B. $SPLUNK_HOME/etc/system/local/

C. $SPLUNK_HOME/etc/shcluster/apps

D. $SPLUNK_HOME/var/run/searchpeers/

Suggested Answer: *C*
The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in
$SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into $SPLUNK_HOME/etc/disabled-apps on staging

Ntani 1 year, 9 months ago
Yes C is correct
upvoted 2 times

andy73 2 years, 12 months ago
C is correct
upvoted 4 times

Question #34 *Topic 1*

How is notable event urgency calculated?

A. Asset priority and threat weight.

B. Alert severity found by the correlation search.

C. Asset or identity risk and severity found by the correlation search.

D. Severity set by the correlation search and priority assigned to the associated asset or identity.

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

inwigboji 1 month, 4 weeks ago
D is correct
upvoted 1 times

huu_nguyen 2 years, 1 month ago
It's D. Asset priority + Event severity = Urgency
upvoted 2 times

andy73 2 years, 12 months ago
D is correct
upvoted 4 times

Question #35 *Topic 1*

What kind of value is in the red box in this picture?

Additional Fields	Value
HTTP Method	GET
Source	10.98.27.195 500
Source Expected	false
Source PCI Domain	untrust
Source Requires Antivirus	false
Source Should Time Synchronize	false
Source Should Update	false
Tag	modaction_result

A. A risk score.

B. A source ranking.

C. An event priority.

D. An IP address rating.

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/8.0.2/Data/FormateventsforHTTPEventCollector

Community vote distribution

A (100%)

Glat Highly Voted 3 years, 2 months ago

Answer is A

upvoted 12 times

leezanelatto Most Recent 1 year, 4 months ago

Selected Answer: A

A risk score

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: A

A. A risk score.

upvoted 1 times

Adam98870 1 year, 11 months ago

A : Risk Score is calculated

upvoted 2 times

SriAkula 2 years, 11 months ago

Answer: A (Clearly specified in Splunk ES Documentation Training)

upvoted 1 times

Question #36 *Topic 1*

Where is it possible to export content, such as correlation searches, from ES?

A. Content exporter

B. Configure -> Content Management

C. Export content dashboard

D. Settings Menu -> ES -> Export

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

Community vote distribution
B (100%)

noysherer Highly Voted 2 years, 11 months ago

Selected Answer: B

B is the correct answer - slide 262 on the admin ES slides

upvoted 6 times

Question #37 *Topic 1*

Which of the following threat intelligence types can ES download? (Choose all that apply.)

A. Text

B. STIX/TAXII

C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Downloadthreatfeed

Community vote distribution
B (100%)

mi5 Highly Voted 3 years ago
Ans is "B" because ES can download the following threat intelligence types-
- Threat List (IP)
- STIX/TAXII
- Open IOC
upvoted 6 times

anonon Highly Voted 3 years, 1 month ago
A & B are the answers.
upvoted 5 times

leezanelatto Most Recent 1 year, 4 months ago
Selected Answer: B
Ans is "B" because ES can download the following threat intelligence types-
- Threat List (IP)
- STIX/TAXII
- Open IOC
upvoted 1 times

andy73 2 years, 12 months ago
A, B are correct
upvoted 5 times

Question #38 *Topic 1*

A site has a single existing search head which hosts a mix of both CIM and non-CIM compliant applications. All of the applications are mission-critical. The customer wants to carefully control cost, but wants good ES performance.
What is the best practice for installing ES?

A. Install ES on the existing search head.

B. Add a new search head and install ES on it.

C. Increase the number of CPUs and amount of memory on the search head, then install ES.

D. Delete the non-CIM-compliant apps from the search head, then install ES.

Suggested Answer: *B*
Reference:
https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

asashima Highly Voted 2 years, 11 months ago
B is correct
Administering Splunk Enterprise Security 6.6.pdf 324P
upvoted 8 times

Soccerfan Most Recent 1 year, 4 months ago
B. Read page 12 of the SVA.

https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf
upvoted 1 times

b5white 3 months ago
Thanks for trying but the PDF now redirects to a single page with only high level content. ¯_(□)_/¯
upvoted 1 times

andy73 2 years, 12 months ago
C is correct
upvoted 1 times

Question #39 *Topic 1*

Enterprise Security's dashboards primarily pull data from what type of knowledge object?

A. Tstats

B. KV Store

C. Data models

D. Dynamic lookups

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Splexicon:Knowledgeobject

Community vote distribution

C (100%)

andy73 Highly Voted 2 years, 12 months ago

C is correct

upvoted 7 times

kkrises Most Recent 1 year, 10 months ago

C is right

upvoted 2 times

huu_nguyen 2 years, 1 month ago

Selected Answer: C

Vote for C

upvoted 1 times

Question #40 *Topic 1*

To which of the following should the ES application be uploaded?

A. The indexer.

B. The KV Store.

C. The search head.

D. The dedicated forwarder.

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

andy73 Highly Voted 2 years, 12 months ago
C is correct
upvoted 5 times

Question #41 *Topic 1*

If a username does not match the `˜identity' column in the identities list, which column is checked next?

A. Email.

B. Nickname

C. IP address.

D. Combination of Last Name, First Name.

Suggested Answer: *C*

Community vote distribution

A (100%)

Glat Highly Voted 3 years, 3 months ago

Correct answer is A . See Identity Matching p.301

upvoted 8 times

kirtak Most Recent 8 months ago

Order Column Description

1 identity Exact match on any one of a list of usernames in identity column

2 Email Exact match

3 Email First part of email, i.e. “htrapper” of “htrapper@acmetech.com”

4 Any Disabled by default—see “conventions” in identityLookup.conf.spec

upvoted 1 times

leezanelatto 1 year, 4 months ago

Selected Answer: A

Correct is A

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: A

A. Email.

upvoted 1 times

Ntani 1 year, 9 months ago

Correct Answer is A

upvoted 2 times

sylax 2 years, 4 months ago

Selected Answer: A

pg 250 Administering Splunk Enterprise Security

upvoted 2 times

andy73 2 years, 12 months ago

A is correct

upvoted 4 times

Question #42 *Topic 1*

Which of the following features can the Add-on Builder configure in a new add-on?

A. Expire data.

B. Normalize data.

C. Summarize data.

D. Translate data.

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Overview

andy73 Highly Voted 2 years, 12 months ago

B is correct

upvoted 5 times

Question #43 *Topic 1*

What is the maximum recommended volume of indexing per day, per indexer, for a non-cloud (on-prem) ES deployment?

A. 50 GB

B. 100 GB

C. 300 GB

D. 500 MB

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

andy73 2 years, 12 months ago
B is correct
upvoted 4 times

learner321 3 years, 4 months ago
B is correct
https://docs.splunk.com/Documentation/ES/4.7.4/Install/DeploymentPlanning#Splunk_Enterprise_system_requirement
upvoted 2 times

Question #44 *Topic 1*

ES needs to be installed on a search head with which of the following options?

A. No other apps.

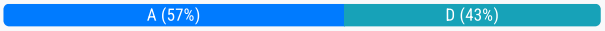
B. Any other apps installed.

C. All apps removed except for TA-*.

D. Only default built-in and CIM-compliant apps.

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity

Community vote distribution



oksey Highly Voted 4 years ago
D is the ans
upvoted 18 times

adamsca Most Recent 5 months, 2 weeks ago
Selected Answer: D
D is Correct
upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago
Selected Answer: D
D. Only default built-in and CIM-compliant apps.
upvoted 2 times

brettw 2 years, 9 months ago
Selected Answer: A
ES recommended installation is on a dedicated search head with only the default installation, due to the number of resources required for ES to run efficiently.
upvoted 4 times

SriAkula 2 years, 11 months ago
Answer: D (Clearly specified in Splunk ES documentation that Splunk Uses by default CIM also default apps should not be deleted)
upvoted 4 times

guirax 2 years, 12 months ago
D is correct

ES generally requires a new, dedicated search head or search head
cluster
– ES is only compatible with other CIM-compatible apps
– ES adds a large number of searches and search results

Administering Splunk Enterprise Security page 113
upvoted 2 times

andy73 2 years, 12 months ago
D is correct
upvoted 1 times

Question #45 *Topic 1*

Which settings indicates that the correlation search will be executed as new events are indexed?

A. Always-On

B. Real-Time

C. Scheduled

D. Continuous

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

Community vote distribution
B (67%) D (33%)

mybox1 Highly Voted 3 years, 3 months ago
B is correct from my perspective.
upvoted 11 times

wasssss Most Recent 3 months, 3 weeks ago
Real Time
upvoted 1 times

SnakeTech 4 months ago
Selected Answer: B
B is correct
upvoted 1 times

llll228736 8 months ago
by chatGPT,

In Splunk, the setting that indicates that the correlation search will be executed as new events are indexed is:

B. Real-Time

This setting allows the correlation search to be triggered instantly upon data ingestion, providing the ability to identify and respond to potential security incidents or other important events as they occur. Real-time searches in Splunk are used to monitor data continuously and trigger alerts or actions immediately when certain conditions are met.
upvoted 1 times

KellyPumphrey 10 months, 3 weeks ago
Selected Answer: D
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

Correlation searches can run with a real-time or continuous schedule. Use a real-time schedule to prioritize current data and performance. Searches with a real-time schedule are skipped if the search cannot be run at the scheduled time. Searches with a real-time schedule do not backfill gaps in data that occur if the search is skipped. Use a continuous schedule to prioritize data completion, as searches with a continuous schedule are never skipped.
upvoted 1 times

vasudvn 11 months, 1 week ago
D is correct
Real-time searches only consider events that are in progress or have recently occurred and have not yet been indexed. They do not include historical data.
the question clearly states that events are indexed
upvoted 1 times

b5white 3 months ago

I'm going to disagree. The way the question is worded, "Real-time" indicates they will be run as the data is indexed. Whereas "Continuous" can run against other data as well, if it got skipped when it was indexed.

upvoted 1 times

qtygbapjpesdayazko 1 year, 7 months ago

Selected Answer: B

B. Real-Time

upvoted 1 times

Ntani 1 year, 9 months ago

B is the correct answer

upvoted 1 times

niuksas 2 years, 1 month ago

B is the correct answer

upvoted 2 times

andy73 2 years, 12 months ago

B is correct.

Scheduling: real-time or continuous.

upvoted 2 times

learner321 3 years, 4 months ago

D is correct answer

upvoted 1 times