SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

QUESTION 1

After installing Enterprise Security, the distributed configuration management tool can be used to create which app to configure indexers?

A. Splunk_DS_ForIndexers.spl

B. Splunk_ES_ForIndexers.spl

C. Splunk_SA_ForIndexers.spl

D. Splunk_TA_ForIndexers.spl

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallTechnologyAdd-ons

QUESTION 2

What are adaptive responses triggered by?

A. By correlation searches and users on the incident review dashboard.

B. By correlation searches and custom tech add-ons.

C. By correlation searches and users on the threat analysis dashboard.

D. By custom tech add-ons and users on the risk analysis dashboard.

Correct Answer: D

QUESTION 3

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.

Correct Answer: C

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

QUESTION 4

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

Correct Answer: D

QUESTION 5

What should be used to map a non-standard field name to a CIM field name?

A. Field alias.

B. Search time extraction.

C. Tag.

D. Eventtype.

Correct Answer: A

QUESTION 6

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

A. Text

B. STIX/TAXII

C. VulnScanSPL

D. SplunkEnterpriseThreatGenerator

Correct Answer: AB

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Downloadthreatfeed

QUESTION 7

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.

Correct Answer: D

Reference: https://docs.splunk.com/Documentation/ES/latest/Admin/Configureadaptiveresponse

QUESTION 8

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. "fieldname"

C. %fieldname%

D. _fieldname_

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

QUESTION 9

When ES content is exported, an app with a .spl extension is automatically created. What is the best practice when exporting and importing updates to ES content?

A. Use new app names each time content is exported.

B. Do not use the .spl extension when naming an export.

C. Always include existing and new content for each export.

D. Either use new app names or always include both existing and new content.

Correct Answer: D

Either use new app names each time (which could be difficult to manage) or make sure you always include all content (old and new) each time you export.

QUESTION 10

What is the main purpose of the Dashboard Requirements Matrix document?

A. Identifies on which data model(s) each dashboard depends.

B. Provides instructions for customizing each dashboard for local data models.

C. Identifies the searches used by the dashboards.

D. Identifies which data model(s) depend on each dashboard.

Correct Answer: D

QUESTION 11

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.

Correct Answer: B

Reference: https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

QUESTION 12

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

A. Always-On

B. Real-Time

C. Scheduled

D. Continuous

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Configurecorrelationsearches

QUESTION 13

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

A. Indexes might crash.

B. Indexes might be processing.

C. Indexes might not be reachable.

D. Indexes have different settings.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf

QUESTION 14

What is the bar across the bottom of any ES window?

A. The Investigator Workbench.

B. The Investigation Bar.

C. The Analyst Bar.

D. The Compliance Bar.

Correct Answer: B

Reference: https://docs.splunk.com/Documentation/ES/6.4.1/User/Startaninvestigation

QUESTION 15

Which of the following ES features would a security analyst use while investigating a network anomaly notable?

A. Correlation editor.

B. Key indicator search.

C. Threat download dashboard.

D. Protocol intelligence dashboard.

Correct Answer: D

Reference: https://www.splunk.com/en_us/products/premium-solutions/splunk-enterprise-security/ features.html