Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

NEW QUESTION 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.

Answer: D

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

NEW QUESTION 2
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_

Answer: C

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

NEW QUESTION 3
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. Therat Intelligence Enforcement

Answer: B

NEW QUESTION 4
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

Answer: D

Explanation:
Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html

NEW QUESTION 5
Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath
B. tstatsHomePath
C. summaryHomePath
D. warmToColdScript

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

NEW QUESTION 6
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.

Answer: B

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

NEW QUESTION 7
When investigating, what is the best way to store a newly-found IOC?

A. Paste it into Notepad.
B. Click the “Add IOC” button.
C. Click the “Add Artifact” button.
D. Add it in a text note to the investigation.

Answer: B

NEW QUESTION 8
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.

Answer: A

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

NEW QUESTION 9
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.

Answer: D

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

NEW QUESTION 10
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.

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

NEW QUESTION 10
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

Answer: D

NEW QUESTION 12
Where is the Add-On Builder available from?

A. GitHub
B. SplunkBase
C. www.splunk.com
D. The ES installation package

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/AddonBuilder/3.0.1/UserGuide/Installation

NEW QUESTION 16
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_

Answer: D

Explanation:
Reference: https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/planintegrationes/

NEW QUESTION 19
Which of the following threat intelligence types can ES download? (Choose all that apply)

A. Text
B. STIX/TAXII
C. VulnScanSPL
D. SplunkEnterpriseThreatGenerator

Answer: B

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

NEW QUESTION 22
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.

Answer: B

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

NEW QUESTION 23
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.

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

NEW QUESTION 24
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.

Answer: C

NEW QUESTION 28
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.

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecurity

NEW QUESTION 33
Which data model populated the panels on the Risk Analysis dashboard?

A. Risk
B. Audit
C. Domain analysis
D. Threat intelligence

Answer: A

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

NEW QUESTION 37
What tools does the Risk Analysis dashboard provide?

A. High risk threats.
B. Notable event domains displayed by risk score.
C. A display of the highest risk assets and identities.
D. Key indicators showing the highest probability correlation searches in the environment.

Answer: C

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis

NEW QUESTION 38
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.

Answer: A

NEW QUESTION 42
Who can delete an investigation?

A. ess_admin users only.
B. The investigation owner only.
C. The investigation owner and ess-admin.
D. The investigation owner and collaborators.

Answer: A

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

NEW QUESTION 47
The Brute Force Access Behavior Detected correlation search is enabled, and is generating many false positives. Assuming the input data has already been validated. How can the correlation search be made less sensitive?

A. Edit the search and modify the notable event status field to make the notable events less urgent.
B. Edit the search, look for where or xswhere statements, and after the threshold value being compared to make it less common match.
C. Edit the search, look for where or xswhere statements, and alter the threshold value being compared to make it a more common match.
D. Modify the urgency table for this correlation search and add a new severity level to make notable events from this search less urgent.

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

NEW QUESTION 51
Which component normalizes events?

A. SA-CIM.
B. SA-Notable.
C. ES application.
D. Technology add-on.

Answer: A

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

NEW QUESTION 54
What is the first step when preparing to install ES?

A. Install ES.
B. Determine the data sources used.
C. Determine the hardware required.
D. Determine the size and scope of installation.

Answer: D

NEW QUESTION 56
What is the default schedule for accelerating ES Datamodels?

A. 1 minute
B. 5 minutes
C. 15 minutes
D. 1 hour

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Knowledge/Acceleratedatamodels

NEW QUESTION 61
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SPLK-3001 Practice Exam Features:

* SPLK-3001 Questions and Answers Updated Frequently

* SPLK-3001 Practice Questions Verified by Expert Senior Certified Staff

* SPLK-3001 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* SPLK-3001 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The SPLK-3001 Practice Test Here