Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

NEW QUESTION 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

Answer: A

Explanation:
Reference: https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduled-searches.html

NEW QUESTION 2
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.

Answer: C

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

NEW QUESTION 3
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

Answer: B

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

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

A. Web
B. Anomalies
C. Authentication
D. Network Traffic

Answer: B

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

NEW QUESTION 6
At what point in the ES installation process should Splunk_TA_ForIndexes.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.

Answer: B

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

NEW 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.

Answer: D

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

NEW QUESTION 8
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.

Answer: B

Explanation:
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

NEW QUESTION 9
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

Answer: D

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

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 10
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

Answer: C

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

NEW QUESTION 15
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

Answer: A

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

NEW QUESTION 16
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 19
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

Answer: B

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

NEW QUESTION 24
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 29
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 31
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

Answer: B

Explanation:
Reference: https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan

NEW QUESTION 34
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

Answer: C

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

NEW QUESTION 39
Where are attachments to investigations stored?

A. KV Store
B. notable index
C. attachments.csv lookup
D. <splunk_home>/etc/apps/SA-Investigations/default/ui/views/attachments

Answer: A

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

NEW QUESTION 40
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 44
Which of the following actions can improve overall search performance?

A. Disable indexed real-time search.
B. Increase priority of all correlation searches.
C. Reduce the frequency (schedule) of lower-priority correlation searches.
D. Add notable event suppressions for correlation searches with high numbers of false positives.

Answer: A

NEW QUESTION 45
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.

Answer: D

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

NEW QUESTION 46
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 50
An administrator wants to ensure that none of the ES indexed data could be compromised through tampering. What feature would satisfy this requirement?

A. Index consistency.
B. Data integrity control.
C. Indexer acknowledgement.
D. Index access permissions.

Answer: B

Explanation:
Reference: https://answers.splunk.com/answers/790783/anti-tampering-features-to-protect-splunk-logs-the.html

NEW QUESTION 52
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 53
......