Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam

https://www.2passeasy.com/dumps/SPLK-3001/

NEW QUESTION 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.

Answer: C

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

NEW QUESTION 2
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 3
Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.
B. Window interval.
C. Window duration.
D. Schedule windows.

Answer: C

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

NEW QUESTION 4
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 5
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 6
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.

Answer: B

NEW QUESTION 7
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 8
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

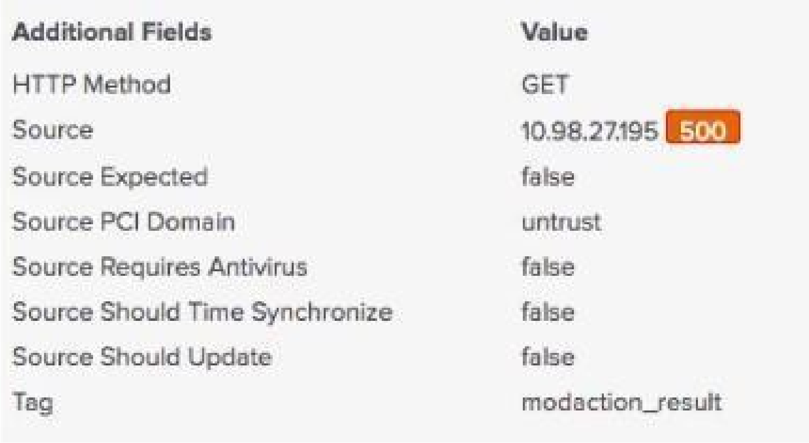
NEW QUESTION 9
How is notable event urgency calculated?

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.

Answer: D

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

NEW QUESTION 10
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.

Answer: C

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

NEW QUESTION 10
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 14
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 17
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.

Answer: B

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

NEW QUESTION 21
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 22
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 27
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 32
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 35
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 36
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

Answer: D

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

NEW QUESTION 37
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 42
......