

Splunk

Exam Questions SPLK-3001

Splunk Enterprise Security Certified Admin Exam



NEW QUESTION 1

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

- A. DA-
- B. SA-
- C. TA-
- D. App-

Answer: C

Explanation:

Reference: <https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/>

NEW QUESTION 2

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 3

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

- A. Configure -> Correlation Searches -> Select Status “Enabled”
- B. Settings -> Searches, Reports, and Alerts -> Filter by Name of “Correlation”
- C. Configure -> Content Management -> Select Type “Correlation” and Status “Enabled”
- D. Settings -> Searches, Reports, and Alerts -> Select App of “SplunkEnterpriseSecuritySuite” and filter by “-Rule”

Answer: A

Explanation:

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

NEW QUESTION 4

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 Responses 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 5

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 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

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 8

Adaptive response action history is stored in which index?

- A. cim_modactions
- B. modular_history
- C. cim_adaptiveactions
- D. modular_action_history

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes>

NEW QUESTION 9

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 10

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 10

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 14

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 15

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 17

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 22

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 27

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)