Vendor: Splunk

Exam Code: SPLK-3001

Exam Name: Splunk Enterprise Security Certified Admin

Version: DEMO

QUESTION 1
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:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Createlookups

QUESTION 2
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:
https://docs.splunk.com/Documentation/ES/6.1.0/User/CreateGlassTable

QUESTION 3
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

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

Answer: D

QUESTION 5
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: D
Explanation:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/CustomizeIR
Change Incident Review columns
You can change the columns displayed on the Incident Review dashboard.
Review the existing columns in Incident Review - Table Attributes.
Use the action column to edit, remove, or change the order of the available columns.
Add custom columns by selecting Insert below or selecting More..., then Insert above.

QUESTION 6
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: B
Explanation:
https://docs.splunk.com/Documentation/ES/6.6.2/User/ProtocolIntelligence

QUESTION 7
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:
https://docs.splunk.com/Documentation/ES/6.1.0/Install/Indexes

QUESTION 8
Which of the following actions would not reduce the number of false positives from a correlation search?

A. Reducing the severity.
B. Removing throttling fields.

C. Increasing the throttling window.
D. Increasing threshold sensitivity.

Answer: A
Explanation:
Reducing the severity of a correlation search does not impact the actual number of false positives generated. Instead, it changes how critical those alerts appear but does not affect the underlying logic or frequency of the alerts.

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

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

QUESTION 11
ES apps and add-ons from $SPLUNK_HOME/etc/apps should be copied from the staging instance to what location on the cluster deployer instance?

A. $SPLUNK_HOME/etc/master-apps/
B. $SPLUNK_HOME/etc/system/local/
C. $SPLUNK_HOME/etc/shcluster/apps
D. $SPLUNK_HOME/var/run/searchpeers/

Answer: C
Explanation:
The upgraded contents of the staging instance will be migrated back to the deployer and deployed to the search head cluster members. On the staging instance, copy $SPLUNK_HOME/etc/apps to $SPLUNK_HOME/etc/shcluster/apps on the deployer. 1. On the deployer, remove any deprecated apps or add-ons in $SPLUNK_HOME/etc/shcluster/apps that were removed during the upgrade on staging. Confirm by reviewing the ES upgrade report generated on staging, or by examining the apps moved into

$SPLUNK_HOME/etc/disabled-apps on staging.

QUESTION 12
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:
https://docs.splunk.com/Documentation/ES/6.1.0/User/Howurgencyisassigned

QUESTION 13
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: A

QUESTION 14
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:
https://docs.splunk.com/Documentation/ES/6.1.0/Admin/Export

QUESTION 15
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:
ES can download the following threat intelligence types-
- Threat List (IP)
- STIX/TAXII
- Open IOC

QUESTION 16
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:
https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

QUESTION 17
Enterprise Security's dashboards primarily pull data from what type of knowledge object?

A. Tstats
B. KV Store
C. Data models
D. Dynamic lookups

Answer: C
Explanation:
https://docs.splunk.com/Splexicon:Knowledgeobject

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**