PassQueen
a.k.a dumpsqueen.com

Splunk Enterprise Security Certified Admin Exam

Splunk SPLK-3001

Version Demo

Total Demo Questions: 13

Total Premium Questions: 132

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Deploying Splunk Enterprise Security	32
Topic 2, Configuring Splunk Enterprise Security	56
Topic 3, Managing Splunk Enterprise Security Content	24
Topic 4, Investigating with Splunk Enterprise Security	20
Total	132

QUESTION NO: 1

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:

Splunk_TA_ForIndexers.spl is the app package generated by the Enterprise Security distributed configuration management tool for deployment to indexers. Enterprise Security requires supporting configurations on indexers so that the data used by ES is indexed and handled consistently across a distributed Splunk deployment. The configuration-management workflow packages the required indexer-side knowledge and settings into the Splunk_TA_ForIndexers app, which can then be distributed through the deployment mechanism appropriate to the environment, such as an indexer-cluster manager or deployment server.

This generated technical add-on is intended specifically for the indexer tier; it helps ensure that the ES deployment's index-related configuration is applied consistently rather than requiring manual replication of settings to every indexer. Creating and deploying this package is therefore an important post-installation step when Enterprise Security is deployed in a distributed topology. Splunk's Enterprise Security installation documentation describes configuring indexers as part of the distributed deployment process, and the Enterprise Security documentation landing page provides version-specific installation guidance: Configure indexers for Enterprise Security and Splunk Enterprise Security installation documentation.

QUESTION NO: 2

Which statements describe risk-based alerting in Enterprise Security? (Choose all that apply)

A. Risk events can accumulate for a risk object over time.

B. A risk-based alert can create a notable event when a threshold is met.

C. Detections can use the Risk Analysis adaptive response action to generate risk events.

D. Risk events automatically change the urgency of existing notable events.

ANSWER: A B C

Explanation:

Risk-based alerting accumulates risk events for risk objects over a defined time period. Risk events can be generated by detections that use the Risk Analysis adaptive response action, and a risk-based alert can create a notable event when configured risk thresholds are met. This workflow helps analysts prioritize entities associated with multiple related behaviors instead of responding independently to every low-confidence detection.

Risk events do not automatically change the urgency of existing notable events. Notable-event urgency is calculated separately using the event severity and the priority of the associated asset or identity. See the Risk-based alerting overview.

QUESTION NO: 3

Which knowledge objects are commonly included in a CIM-compliant technology add-on to normalize source data? (Choose all that apply)

A. Field extractions

B. Field aliases

C. Event types and tags

D. Data model acceleration summaries

ANSWER: A B C

Explanation:

Field extractions, field aliases, event types, and tags are commonly used by technology add-ons to normalize source data for the Common Information Model. Field extractions expose source values, field aliases map source-specific field names to CIM field names, and event types and tags classify events so they match the applicable CIM data model datasets.

Data model acceleration is configured for a data model and is not a source-data normalization object supplied by a technology add-on. See the CIM normalization documentation and the Common Information Model overview.

QUESTION NO: 4

Which of the following knowledge objects can be used to support CIM normalization? (Choose all that apply)

A. Field aliases

B. Event types

C. Tags

D. Indexes

ANSWER: A B C

Explanation:

Field aliases, **event types**, and **tags** can support CIM normalization. A field alias maps a source-specific field to a CIM field name at search time. Event types classify events that match defined search criteria, and tags apply CIM-recognized classifications to event types or fields. CIM data model datasets commonly use tags and event types in their constraints to identify relevant events.

Indexes determine where data is stored, but do not normalize fields or classify events for CIM. See the Splunk documentation for field aliases and the Splunk Common Information Model.

QUESTION NO: 5

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:

Adaptive response action history is stored in the `cim_modactions` index. In Splunk Enterprise Security, adaptive response actions are the automated or semi-automated actions initiated from findings, such as creating tickets, sending notifications, or executing an action through an integration. Enterprise Security records the action lifecycle and associated metadata as

modular-action events so administrators and analysts can investigate what action was requested, its execution state, timing, result, and relevant contextual details. The `cim_modactions` index is the designated location for those records and is therefore the appropriate index to search when auditing adaptive-response activity or troubleshooting action execution. For example, an administrator can search this index to correlate action records with notable events and determine whether a response action completed successfully. This storage design supports the Enterprise Security adaptive response framework and its reporting and audit workflows. Splunk's Enterprise Security documentation is available at Splunk Enterprise Security Documentation, and Splunk's index-management documentation provides background on how indexed event data is stored and searched at Set up multiple indexes.

QUESTION NO: 6

Which actions can an analyst perform from Incident Review when working with a notable event? (Choose all that apply)

A. Assign an owner

B. Change the event status

C. Add a comment

D. Create a new correlation search

ANSWER: A B C

Explanation:

Analysts can assign an owner, change a notable event status, and add comments from Incident Review. These actions support the operational incident-response workflow by allowing analysts to document investigation findings, establish accountability, and move a notable event through the organization's configured status process.

Creating a new correlation search is an administrative content-development task, not an action performed from an individual notable event in Incident Review. See Use Incident Review in Splunk Enterprise Security.

QUESTION NO: 7

What is an example of an ES asset?

A. MAC address

B. User name

C. Server

D. People

ANSWER: C

Explanation:

Server is an example of an Enterprise Security asset. In Splunk Enterprise Security, an asset represents a system, device, or other managed entity in the organization's environment that can generate, receive, or be associated with security-relevant activity. Typical assets include servers, workstations, network devices, and domain controllers. Asset information is maintained in ES asset and identity lookups and can include identifying and contextual fields such as hostname, IP address, MAC address, operating system, owner, priority, category, and business unit.

Classifying a server as an asset gives ES the context needed to correlate raw events with the actual system involved. For example, an alert or notable event containing a host or IP value can be enriched with the server's criticality, ownership, and network details. This enrichment supports risk-based prioritization, incident investigation, and correlation searches that distinguish high-value infrastructure from less critical systems. A MAC address can be an attribute recorded for an asset, but the server itself is the asset entity. Splunk's documentation describes assets as devices or systems and explains how asset

lookup data provides this contextual enrichment in ES. See Configure asset and identity lists and Enterprise Security use case overview.

QUESTION NO: 8

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

A. Web

B. Anomalies

C. Authentication

D. Network Traffic

ANSWER: A C D

Explanation:

Web, **Authentication**, and **Network Traffic** are Common Information Model (CIM) data models used by Splunk Enterprise Security. Enterprise Security relies on CIM-normalized data to populate its security views, enable consistent correlation searches, and support accelerated searches across data from different security products. The Authentication data model standardizes identity and login-related events, providing the normalized fields and datasets needed for authentication monitoring and detection content. The Network Traffic data model represents network communication activity and is used to analyze connections, bytes transferred, protocols, and related traffic attributes. The Web data model normalizes web-server and web-proxy activity, enabling web-focused visibility and security analytics. Proper CIM mapping is therefore an essential ES administration task: data should be assigned to the appropriate tags and field conventions so that the relevant data-model datasets are populated. Splunk documents the CIM data models, their purposes, and their datasets in the CIM manual; the Enterprise Security documentation also describes how ES uses CIM compliance as a foundation for its content and dashboards. See the Splunk Common Information Model overview and CIM data models documentation.

QUESTION NO: 9

Which CIM data model is most relevant when onboarding firewall connection logs containing source IP address, destination IP address, destination port, and bytes transferred?

A. Network Traffic

B. Authentication

C. Web

D. Change

ANSWER: A

Explanation:

Network Traffic is correct. The Network Traffic data model represents network communications and includes normalized fields used to describe source and destination systems, ports, protocols, actions, and byte counts. Firewall connection logs commonly provide this type of telemetry and should be mapped to the appropriate Network Traffic dataset when they meet the CIM requirements.

The Authentication data model is intended for login and authentication activity, while Web is intended for HTTP-related activity. See the Network Traffic data model.

QUESTION NO: 10

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:

`tstatsHomePath` is the `indexes.conf` setting that specifies the filesystem location used for accelerated data stored as TSIDX files. Splunk Enterprise uses this path for data-model acceleration and other `tstats`-related accelerated storage associated with an index. Configuring it lets an administrator place this high-performance, potentially storage-intensive data on a location separate from the index's normal hot/warm, cold, and thawed bucket paths. This can be useful when accelerated searches require fast storage, when disk capacity must be managed independently, or when the deployment's storage layout separates raw indexed data from acceleration artifacts. The value is configured on the relevant index stanza in `indexes.conf`, and the selected path must be accessible to the Splunk Enterprise instance and managed consistently across the deployment where applicable. Splunk documents `tstatsHomePath` as the path for storing TSIDX files generated by data-model acceleration. See the indexes.conf specification and the data model acceleration documentation for configuration and storage details.

QUESTION NO: 11

Which of the following lookup types in Enterprise Security contains information about known hostile IP addresses?

A. Security domains.

B. Threat intel.

C. Assets.

D. Domains.

ANSWER: B

Explanation:

Threat intel is correct because Splunk Enterprise Security uses threat-intelligence lookups to store and match indicators of compromise, including known malicious or hostile IP addresses. Threat intelligence frameworks and feeds supply these indicators, which can also include domains, URLs, file hashes, and other observable values associated with suspicious or malicious activity. Enterprise Security correlates incoming event data with these indicators to enrich investigations and generate notable events when activity matches a known threat indicator. In particular, IP-based threat indicators allow analysts to identify communications involving addresses associated with malicious infrastructure, such as command-and-control servers, scanners, botnets, or other hostile sources. The lookup-based structure makes threat data available to correlation searches and investigation workflows, helping security teams prioritize activity that has an established threat context. Splunk documents that threat intelligence in Enterprise Security supports indicators from sources including threat feeds and enables matching against events through its threat-intelligence framework. See Splunk Enterprise Security threat intelligence documentation and Splunk guidance for configuring threat intelligence.

QUESTION NO: 12

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 correct answer is **A high-level overview of notable events.** In Splunk Enterprise Security, the Security Posture dashboard is intended to give security teams an at-a-glance view of the organization's current security state. It aggregates notable-event information across the Enterprise Security deployment and presents it in a concise, visual format that is appropriate for ongoing monitoring, including use on a SOC display. The dashboard helps analysts and operational teams quickly understand the volume, distribution, and overall posture represented by notable events without requiring them to begin in a detailed investigation workflow.

Notable events are central to Enterprise Security's incident-detection process: correlation searches identify potentially important activity and generate notable events for analyst review and investigation. By surfacing these events at a high level, the Security Posture dashboard supports situational awareness and prioritization of security operations. Splunk's Enterprise Security documentation describes dashboards as views for monitoring and investigating security data, while the notable-events documentation explains their role in representing findings created by correlation searches. See the Splunk Enterprise Security overview and correlation search and notable-event documentation.

QUESTION NO: 13

Which of the following can be configured as adaptive response actions for a correlation search in Enterprise Security? (Choose all that apply)

A. Create notable event

B. Add risk

C. Send email

D. Change index retention policy

ANSWER: A B C

Explanation:

Create notable event, **Add risk**, and **Send email** can be configured as adaptive response actions, depending on the installed Enterprise Security content and integrations. Create notable event sends qualifying results to Incident Review. Add risk creates risk events that can contribute to risk-based alerting. Send email can notify designated recipients when a detection meets its trigger criteria.

Changing an index retention policy is an index administration task and is not an adaptive response action. See Configure adaptive response actions.