SPLK-3001 Q&As

Splunk Enterprise Security Certified Admin

Pass Splunk SPLK-3001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/splk-3001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Splunk Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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.

Correct Answer: C

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/Install/InstallEnterpriseSecuritySHC

QUESTION 2

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.

Correct Answer: B

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

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

QUESTION 3

Which of the following is a risk of using the Auto Deployment feature of Distributed Configuration Management to distribute indexes.conf?

A. Indexes might crash.

B. Indexes might be processing.

C. Indexes might not be reachable.

D. Indexes have different settings.

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/Splunk/8.0.2/Admin/Indexesconf

QUESTION 4

Which data model populated the panels on the Risk Analysis dashboard?

A. Risk

B. Audit

C. Domain analysis

D. Threat intelligence

Correct Answer: A

Reference: https://docs.splunk.com/Documentation/ES/6.1.0/User/RiskAnalysis#Dashboard_panels

QUESTION 5

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

Correct Answer: D

Reference: https://answers.splunk.com/answers/600354/indexes-searched-by-cim-data-models.html