



# SPLK-3001<sup>Q&As</sup>

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.passapply.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

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 2

Which column in the Asset or Identity list is combined with event security to make a notable event's urgency?

- A. VIP
- B. Priority
- C. Importance
- D. Criticality

Correct Answer: B

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

---

### QUESTION 3

After managing source types and extracting fields, which key step comes next In the Add-On Builder?

- A. Validate and package
- B. Configure data collection.
- C. Create alert actions.
- D. Map to data models.

Correct Answer: D



#### QUESTION 4

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

Correct Answer: B

Reference: <https://docs.splunk.com/Documentation/ITSI/4.4.2/Install/Plan>

---

#### QUESTION 5

Which of the following threat intelligence types can ES download? (Choose all that apply)

- A. Text
- B. STIX/TAXII
- C. VulnScanSPL
- D. SplunkEnterpriseThreatGenerator

Correct Answer: AB

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

[Latest SPLK-3001 Dumps](#)

[SPLK-3001 PDF Dumps](#)

[SPLK-3001 VCE Dumps](#)