

Splunk SPLK-3001

Splunk Enterprise Security Certified Admin Exam

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/splk-3001>

Latest Version: 9.0

Question: 1

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

- A. DAB.
- SAC.
- TAD.
- App-

Answer: C

Explanation:

Reference:

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

Question: 2

Which of the following are examples of sources for events in the endpoint security domain dashboards?

- A. REST API invocations.
- B. Investigation final results status.
- C. Workstations, notebooks, and point-of-sale systems.
- D. Lifecycle auditing of incidents, from assignment to resolution.

Answer: C

Explanation:

Reference:

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

Question: 3

When creating custom correlation searches, what format is used to embed field values in the title, description, and drill-down fields of a notable event?

- A. \$fieldname\$
- B. "fieldname"
- C. %fieldname%

D. _fieldname_

Answer: A

Explanation:

Reference: <https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch>

Question: 4

What feature of Enterprise Security downloads threat intelligence data from a web server?

- A. Threat Service Manager
- B. Threat Download Manager
- C. Threat Intelligence Parser
- D. Therat Intelligence Enforcement

Answer: B

Explanation:

"The Threat Intelligence Framework provides a modular input (Threat Intelligence Downloads) that handles the majority of configurations typically needed for downloading intelligence files & data. To access this modular input, you simply need to create a stanza in your Inputs.conf file called "threatlist"."

Question: 5

The Remote Access panel within the User Activity dashboard is not populating with the most recent hour of data. What data model should be checked for potential errors such as skipped searches?

- A. Web
- B. Risk
- C. Performance
- D. Authentication

Answer: D

Explanation:

Reference: <https://answers.splunk.com/answers/565482/how-to-resolve-skipped-scheduledsearches.html>

Thank You for Trying Our Product
Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>