Demo Questions

SPLUNK SPLK-3001 Exam

Splunk Enterprise Security Certified Admin

Thank you for downloading **SPLK-3001** Exam PDF

Question #1*Topic 1*

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

- A. DA-
- B. SA-
- C. TA-
- D. App-

Correct Answer: *C*
Reference:
https://dev.splunk.com/enterprise/docs/developapps/enterprisesecurity/abouttheessolution/

Question #2*Topic 1*

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.

Correct Answer: *D*
Reference:
https://docs.splunk.com/Documentation/ES/6.1.0/User/EndpointProtectionDomaindashboards

Question #3*Topic 1*

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_

Correct Answer: *C*
Reference:
https://docs.splunk.com/Documentation/ITSI/4.4.2/Configure/Createcorrelationsearch

Question #4*Topic 1*

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

Correct Answer: *B*

Question #5*Topic 1*

In order to include an eventtype in a data model node, what is the next step after extracting the correct fields?

- A. Save the settings.
- B. Apply the correct tags.

- C. Run the correct search.
- D. Visit the CIM dashboard.

Correct Answer: *C*
Reference:
https://docs.splunk.com/Documentation/CIM/4.15.0/User/UsetheCIMtonormalizeOSSECdata