Splunk Enterprise Security Certified Admin

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

A. DA-

B. SA-

C. TA-

D. App-

Answer(s): C

---

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(s): D

---

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(s): C

---

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. Threat Intelligence Enforcement

Answer(s): B

---

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(s): A

---

6. 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.

Answer(s): C

---

7. What role should be assigned to a security team member who will be taking ownership of notable events in the incident review dashboard?

A. ess_user

B. ess_admin

C. ess_analyst

D. ess_reviewer

Answer(s): B

---

8. 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

Answer(s): B

---

9. What does the risk framework add to an object (user, server or other type) to indicate increased risk?

A. An urgency.

B. A risk profile.

C. An aggregation.

D. A numeric score.

Answer(s): C

---

10. 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

Answer(s): D

---

11. Which setting is used in indexes.conf to specify alternate locations for accelerated storage?

A. thawedPath

B. tstatsHomePath

C. summaryHomePath

D. warmToColdScript

Answer(s): B

---

12. Which of the following is a way to test for a property normalized data model?

A. Use Audit -> Normalization Audit and check the Errors panel.

B. Run a | datamodel search, compare results to the CIM documentation for the datamodel.

C. Run a | loadjob search, look at tag values and compare them to known tags based on the encoding.

D. Run a | datamodel search and compare the results to the list of data models in the ES normalization guide.

Answer(s): B

---

13. Which argument to the | tstats command restricts the search to summarized data only?

A. summaries=t

B. summaries=all

C. summariesonly=t

D. summariesonly=all

Answer(s): C

---

14. When investigating, what is the best way to store a newly-found IOC?

A. Paste it into Notepad.

B. Click the “Add IOC” button.

C. Click the “Add Artifact” button.

D. Add it in a text note to the investigation.

Answer(s): B

---

15. How is it possible to navigate to the list of currently-enabled ES correlation searches?

A. Configure -> Correlation Searches -> Select Status “Enabled”

B. Settings -> Searches, Reports, and Alerts -> Filter by Name of “Correlation”

C. Configure -> Content Management -> Select Type “Correlation” and Status “Enabled”

D. Settings -> Searches, Reports, and Alerts -> Select App of “SplunkEnterpriseSecuritySuite” and filter by “- Rule”

Answer(s): A

---

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

A. Indexers might crash.

B. Indexers might be processing.

C. Indexers might not be reachable.

D. Indexers have different settings.

Answer(s): A

---

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

A. Web

B. Anomalies

C. Authentication

D. Network Traffic

Answer(s): B

18. At what point in the ES installation process should Splunk_TA_ForIndexers.spl be deployed to the indexers?

A. When adding apps to the deployment server.

B. Splunk_TA_ForIndexers.spl is installed first.

C. After installing ES on the search head(s) and running the distributed configuration management tool.

D. Splunk_TA_ForIndexers.spl is only installed on indexer cluster sites using the cluster master and thesplunk apply cluster-bundle command.

Answer(s): B

---

19. Which correlation search feature is used to throttle the creation of notable events?

A. Schedule priority.

B. Window interval.

C. Window duration.

D. Schedule window.

Answer(s): C

---

20. Both “Recommended Actions” and “Adaptive Response Actions” use adaptive response. How do they differ?

A. Recommended Actions show a textual description to an analyst, Adaptive Response Actions show them encoded.

B. Recommended Actions show a list of Adaptive Responses to an analyst, Adaptive Response Actions run them automatically.

C. Recommended Actions show a list of Adaptive Responses that have already been run, Adaptive Response Actions run them automatically.

D. Recommended Actions show a list of Adaptive Resposes to an analyst, Adaptive Response Actions run manually with analyst intervention.

Answer(s): D
