PASS QUESTION

QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Provide One Year Free Update!

https://www.passquestion.com

Exam : **SPLK-5003**

Title : Splunk Certified Cybersecurity Defense Architect

Version : DEMO

1.Sophia manages data ingestion for her organization's SIEM. The data science team wants to perform real-time analytics on security data and asks Sophia for a copy of all new endpoint telemetry from the current point forward. The SIEM currently collects 15TB of endpoint telemetry every day.
Which of the following solutions can Sophia use to best help the data science team?
A. Export the last 12 months of telemetry data from the SIEM in OCSF.
B. Use a message bus to send data to both the SIEM and data science team.
C. Export the last 12 months of telemetry data from the SIEM in JSON format.
D. Configure the SIEM to export a CSV report of all new telemetry data every night.
Answer: B

2.To ensure leadership is aware of the security team's performance, which measurements should be presented on a regular basis? (Choose all that apply.)
A. Patch compliance percentage
B. Mean time to contain
C. Number of emergency change requests
D. Mean time to respond
Answer: ABD

3.Justin has just finished successfully importing data from the CMDB platform into the SIEM. While validating data, he discovers a host with a MAC address (35:33:33:20:76) that does not have the same OUI (03:83:71) as the rest of the deployed devices.
Which of the following is the most likely explanation for this discrepancy?
A. CMDB contains data from personal devices managed under MDM
B. CMDB data was normalized during the SIEM import process
C. CMDB data was corrupted during the export process
D. CMDB contains data related to dynamic VPN pool addresses
Answer: A

4.Which of the following are common criteria used for the evaluation of threat intelligence feeds? (Choose all that apply.)
A. TLP
B. Industry
C. Source
D. Severity
Answer: ABCD

5.Which MLTK command can be combined with tstats in an ES detection to apply a machine learning model to search results?
A. Summary
B. Fit
C. Cluster
D. Sample
Answer: B