CrowdStrike

CCSA-205

CrowdStrike Certified SIEM Analyst

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.**

Latest Version: 6.0

Question: 1

A detection includes a suspicious URL, user, host, and file hash. What should the analyst use these values as?

A. Investigation pivots
B. Dashboard themes
C. Case templates
D. Report headers

Answer: A

Question: 2

A query returns thousands of events across several days. The analyst only needs events that occurred during the suspected intrusion window. What should be adjusted first?

A. Case notes
B. Time parameters
C. Alert severity labels
D. User permissions

Answer: B

Question: 3

A file hash is seen on one endpoint and later appears on two file servers. What should the analyst do?

A. Search hash activity
B. Close the first case
C. Disable host logging
D. Delete server events

Answer: A

Question: 4

An analyst wants to find process events where either cmd.exe or powershell.exe launched a network tool. Which CQL design is most appropriate?

A. Use case notes as filters
B. Search all process events
C. Review only endpoint alerts
D. Group process names with OR

Answer: D

Question: 5

A Falcon Fusion SOAR workflow is available for confirmed malware detections. When should the analyst use it?

A. To replace all hunting
B. Before reviewing alerts
C. After confirming evidence
D. To delete raw events

Answer: C

Question: 6

A chart shows a sudden rise in encoded PowerShell commands. What should the analyst do before escalating?

A. Delete the visualization
B. Review supporting raw events
C. Disable PowerShell logging
D. Escalate without context

Answer: B

Question: 7

A host connects to a known malicious IP, then downloads an unknown executable. What should the analyst identify first?

A. Related IOC activity
B. Dashboard owner name
C. Query display format

D. Case folder color

Answer: A

Question: 8

An investigation summary must support handoff to another analyst. What should it contain?

A. Report font family
B. Dashboard color choices
C. Query window shape
D. Findings and next steps

Answer: D

Question: 9

A confirmed malicious process is active on a workstation. What should guide remediation?

A. Dashboard owner
B. Case color theme
C. Evidence and impact
D. Query row height

Answer: C

Question: 10

An analyst confirms that suspicious activity affected only one test host with no outbound traffic. What should this support?

A. Sensor shutdown
B. Confirmed data theft
C. Global rule removal
D. Limited incident scope

Answer: D

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/