CrowdStrike
CCSA-205
CrowdStrike Certified SIEM Analyst

Latest Version: 6.0

Question: 1

A suspicious domain appears in email, proxy, and endpoint events for the same user. What should the analyst build?
Response:

A. Event timeline
B. Dashboard color
C. Case template
D. Role mapping

Answer: A

Question: 2

A detection shows high severity but low confidence. Which analyst response best reflects proper alert review?
Response:

A. Review evidence before action
B. Close it due to confidence
C. Escalate without validation
D. Remove the detection type

Answer: A

Question: 3

An alert has medium severity but high confidence and involves unusual administrator activity. What should the analyst do?
Response:

A. Review context before closure
B. Close it due to medium severity
C. Delete matching admin events
D. Disable related detections

Answer: A

Question: 4

A SOC analyst compares a suspicious login alert with HR travel records and VPN history. What is the analyst trying to determine?
Response:

A. False positive or threat
B. Dashboard display order
C. Query storage capacity
D. Sensor install status

Answer: A

Question: 5

A low-severity alert has low confidence and occurs on a test host during approved maintenance. What is the most reasonable analyst action?
Response:

A. Validate and document context
B. Escalate without review
C. Disable all test host alerts
D. Delete the alert metadata

Answer: A

Question: 6

An analyst sees repeated failed logins, one successful login, and privilege changes for the same account. What should this sequence suggest?
Response:

A. Possible account takeover
B. Normal dashboard usage
C. Routine case creation
D. Expected log rotation

Answer: A

Question: 7

A malicious hash appears on several hosts in different departments. What should the analyst determine?
Response:

A. Spread and impact
B. Chart label order
C. Case owner theme
D. Query row height

Answer: A

Question: 8

A detection shows suspicious script execution followed by registry changes under a startup location. Which behavior is indicated?
Response:

A. Persistence activity
B. Dashboard filtering
C. Case assignment
D. Report creation

Answer: A

Question: 9

A host runs a suspicious script and then attempts credential access. What should the analyst review next?
Response:

A. Related login events
B. Dashboard chart size
C. Case folder color
D. Report export type

Answer: A

Question: 10

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

Response:

A. Related IOC activity
B. Dashboard owner name
C. Query display format
D. Case folder color

Answer: A

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer