

Exam : CCSA-205

Title : CrowdStrike SIEM Analyst

Version : DEMO

1.A suspicious domain appears in email, proxy, and endpoint events for the same user.

What should the analyst build?

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

Answer: A

2.A detection shows high severity but low confidence.

Which analyst response best reflects proper alert review?

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

Answer: A

3.An alert has medium severity but high confidence and involves unusual administrator activity.

What should the analyst do?

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

Answer: A

4.A SOC analyst compares a suspicious login alert with HR travel records and VPN history.

What is the analyst trying to determine?

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

Answer: A

5.A low-severity alert has low confidence and occurs on a test host during approved maintenance.

What is the most reasonable analyst action?

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

Answer: A