
Exam : 250-624

Title : Symantec CBX R1
Technical Specialist

Version : DEMO

1.A senior analyst is transferring an active case containing regulated data to a contractor who will assist for one week.

Which sequence best preserves least-privilege RBAC guardrails?

- A. Share access broadly now and tighten the scope afterward
- B. Hand off the case first, then decide on the access later
- C. Give the contractor the senior analyst's own role fully
- D. Grant a scoped time-limited role, then hand off the case

Answer: D

2.A SOC lead separates two modes of team work: responding to alerts the platform raises, and actively searching the environment for threats that have not triggered any alert.

Which statement best describes proactive threat hunting rather than reactive alert response?

- A. Working through alerts the console raised
- B. Hunting for threats no alert has flagged
- C. Waiting for detections to escalate first
- D. Closing tickets after remediation ends

Answer: B

3.A CBX deployment already collects endpoint and network telemetry. The security team is deciding whether Microsoft Entra ID synchronization adds meaningful detection value.

What is the strongest reason to include directory synchronization as a detection input?

- A. It blocks unsanctioned applications on its own
- B. It encrypts all synchronized user credentials
- C. It surfaces unmanaged app and identity usage
- D. It replaces the need for endpoint telemetry

Answer: C

4.An analyst notes that CBX can relate activity seen on a laptop to network events involving the same host.

Conceptually, how does the Endpoint Security Agent make this possible?

- A. By blocking suspicious network traffic
- B. By hosting the unified CBX dashboard
- C. By forwarding endpoint signals to CBX
- D. By encrypting locally stored records

Answer: C

5.A CBX analyst has confirmed, via directory synchronization, that a team is using an unsanctioned project-management app to store client data.

Which follow-up actions are reasonable and proportionate first responses? Select the two correct answers.

- A. Purge all Entra ID synchronization history
- B. Immediately blocklist the entire cloud provider
- C. Disable directory sync to stop the alerts
- D. Assess the data-handling risk the app poses

E. Engage the team about the business need

Answer: DE