Broadcom

250-624

Broadcom Symantec CBX R1 Technical Specialist

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 lead responder explains to a junior analyst why the team visualizes an incident's blast radius early in a response.
Which two benefits does visualizing the blast radius provide when scoping the response?
Select the two correct answers.

A. It reveals the full set of affected entities
B. It updates endpoint protection definitions automatically
C. It writes the final compliance report
D. It authenticates analysts into the console
E. It prevents over-containing unaffected systems

Answer: A,E

Question: 2

An analyst must hand off an investigation that includes sensitive data-loss telemetry to a peer who only needs the network findings.
How do RBAC guardrails best support this handover?

A. Grant the peer the analyst's complete case access
B. Export all telemetry so the peer has full context
C. Scope the peer's role to the network telemetry only
D. Copy the sensitive data into a shared open workspace

Answer: C

Question: 3

A SOC lead is deciding how to fit AI-generated incident summaries into the team's triage process.
At which point does such a summary add the most value?

A. Only after remediation, when writing the closing report
B. Early, to grasp incident scope before prioritizing
C. Only once the incident has already been escalated
D. Only when a compliance audit later requests it

Answer: B

Question: 4

A security lead is explaining why CBX's Microsoft Entra ID synchronization matters to the organization's security posture.
Which outcomes does surfacing shadow IT through directory synchronization support?
Select the two correct answers.

A. Guaranteeing no unsanctioned app is ever installed
B. Automatically patching every unmanaged endpoint
C. Expanding visibility into unmanaged usage
D. Replacing the need for network telemetry entirely
E. Revealing unsanctioned apps that bypass IT review

Answer: C,E

Question: 5

An incident review shows that a phishing site repeatedly lured managed users over several days before it was flagged. Endpoint cleanup is complete, but leadership wants assurance the same site cannot be reached again by anyone in the organization.
What is the most durable hardening step?

A. Revoke the sessions of all the users who clicked
B. Re-image only the endpoints that were hit
C. Generate a compliance report on the case
D. Add the phishing site to the global deny list

Answer: D

Question: 6

An analyst begins a shift in the CBX Alerts workspace and is presented with a very large volume of open alerts.
What is the primary purpose of applying the workspace's multi-dimensional filters?

A. Permanently delete low-priority alerts from storage
B. Narrow the alert set by combining several attributes
C. Assign every open alert to a separate analyst
D. Group related alerts into a formal investigation case

Answer: B

Question: 7

Which statement best describes the relationship between a detection and a global deny list update in CBX hardening?

A. The deny list update removes the need to detect threats
B. The deny list update affects only the analyst's session
C. The detection automatically encrypts all of the flagged traffic
D. The detection justifies a policy change enforced org-wide

Answer: D

Question: 8

A team is deciding when a coordinated cross-domain containment response is warranted rather than a narrower single-domain action.
Which two situations call for cross-domain containment?
Select the two correct answers.

A. A threat is active on the host, network, and in data
B. A dashboard needs a posture summary for a report card
C. A closed incident is being documented for compliance
D. A single quarantined file needs analyst review soon
E. A fast-spreading incident is pivoting between vectors

Answer: A,E

Question: 9

During an active investigation, an analyst sees several alerts that appear to stem from one intrusion and wants to track them together as a single, managed unit of work.
Which CBX capability is designed for grouping related activity in this way?

A. Definition updates delivered by LiveUpdate
B. Multi-dimensional filters in the Alerts workspace
C. Incident summaries from the AI Assistant
D. Case management in the Investigations layer

Answer: D

Question: 10

On their own, a single endpoint alert and a single network alert each look low-severity and are easy to dismiss.
Why can correlating them across sources change that assessment?

A. Correlation discards the weaker alert
B. Together the signals reveal a threat
C. Each source raises its own severity
D. Network signals always take precedence

Answer: B

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/