Boost up Your Certification Score

Broadcom

250-624

Broadcom Symantec CBX R1 Technical Specialist

Exams Boost

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/250-624

Latest Version: 6.2

Question: 1

At the end of a shift, an analyst hands an active Investigation to an incoming colleague, who will now be responsible for it.
Which action records that handover in the Investigations layer?
Response:

A. Export the alert list and email it to the team
B. Reassign the Investigation's owner to the colleague
C. Change the Investigation's state to Closed
D. Open a new Investigation for the colleague

Answer: B

Explanation:
Investigations carry an Assigned To owner; reassigning it transfers ownership while the case keeps tracking the same response.

Question: 2

A hunter hypothesizes that a specific abused utility is running on several endpoints, yet only one alert exists. Leadership is pushing for containment, but the true scope is still unknown.
What should the hunter do first so the response stays proportionate?
Response:

A. Ban the utility's hash everywhere at once
B. Query endpoints to establish true scope
C. Revoke sessions on the alerted host
D. Open a compliance report on the case

Answer: B

Explanation:
Querying endpoints first establishes how widespread the activity really is, so any containment that follows is sized to the actual scope rather than a guess.

Question: 3

A mid-size SecOps team has just adopted CBX after years of juggling separate endpoint, network, and data tools. Leadership asks the team to justify the shift in one sentence during a review.
Which justification most accurately reflects what the unified CBX Console provides?

Response:

A. One console removes the need to define any analyst roles
B. One dashboard guarantees that every incident is stopped instantly
C. One cohesive view replaces pivoting across disconnected tools
D. One console makes the endpoint agent unnecessary

Answer: C

Explanation:
The Console's value is exactly this: a single cohesive view that ends the pivoting across siloed endpoint, network, and data tools.

Question: 4

While reviewing a detection, an analyst finds a long, obfuscated command line and wants a plain explanation of what it does before deciding how to respond.
Which CBX capability can provide that explanation?
Response:

A. Ask the SymantecAI Assistant to explain it
B. Run a Device Query across the whole fleet
C. Add the command to the Cloud SWG global deny list
D. Set the alert's workflow state to Closed

Answer: A

Explanation:
The SymantecAI Assistant answers investigation questions, including command-line explanations, drawing on curated threat intelligence data.

Question: 5

The same malicious executable has been discovered on many endpoints across the estate. No identity or session has been implicated.
Which remediation blocks that exact file everywhere?
Response:

A. Revoke the affected user sessions
B. Run a Device Query on each host
C. Open a Live Response shell per host
D. Deploy a hash ban for the binary

Answer: D

Explanation:
Because the threat is a file and no identity is compromised, banning its hash blocks that exact binary on every managed endpoint.

Question: 6

A compromised host has been network-isolated, yet the responder still needs hands-on, command-line access to that device to investigate and remediate it.
Which CBX capability is designed to interact with such an isolated device?
Response:

A. A fleet-wide Device Query across all hosts
B. A Live Response shell opened on that host
C. An AI Assistant summary of the host's activity
D. An alerts view filtered by several attributes

Answer: B

Explanation:
A Live Response shell is built to interact with isolated devices; Live Response can be used on quarantined devices to investigate, contain and remediate from a command line.

Question: 7

In the CBX remediation model, what does cross-domain containment coordinate?
Response:

A. A single endpoint isolation applied on its own
B. A network block scheduled for a later maintenance window
C. One coordinated action across every domain an incident touches
D. A summary report of actions taken across domains

Answer: C

Explanation:
The Entities and Remediation workspace executes frictionless, cross-domain containment with a single click, so one incident is contained across the domains it touches.

Question: 8

An incident is being handed from the day shift to an on-call responder who must only triage the monitoring queues, not remediate. Two options are proposed. Option 1: grant a role that also permits remediation. Option 2: grant a role limited to triage.
Under least-privilege RBAC guardrails, which choice is correct and why?
Response:

A. Option 1, because responders always need full rights
B. Option 1, because triage roles slow the response down
C. Option 2, but only after disabling audit logging
D. Option 2, because access should fit the role's task

Answer: D

Explanation:
A role limited to triage matches access to the actual task, satisfying least privilege.

Question: 9

An analyst has picked up an alert in the Alerts workspace and started triaging it, but has not finished.
Which alert workflow state reflects this?
Response:

A. Open
B. Closed
C. Archived
D. In Progress

Answer: D

Explanation:
Alerts move through the workflow states Open, In Progress and Closed; an alert that is being worked but not finished is In Progress.

Question: 10

Using the Threat Tracer canvas, an analyst sees that a malicious file has spread from one endpoint to three connected hosts and one service account.
How does this blast-radius view most directly help the response?
Response:

A. It automatically revokes the affected user sessions
B. It shows which entities the containment must cover
C. It rewrites the global web deny lists in Cloud SWG
D. It generates the post-incident compliance report

Answer: B

Explanation:
Seeing the affected hosts and account tells the responder which entities the containment action needs to reach.

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

