DUMPSBOSS.

Palo Alto Networks Security Operations Professional

Palo Alto Networks SecOps-Pro

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

What are the primary functions of the Causality Analysis Engine in Cortex XDR?

A. To identify the root cause of alerts and provide a complete forensic timeline of events

B. To prioritize critical alerts and reduce the overall number of alerts generated

C. To perform regular system backups and restore operations in case of failure

D. To determine only the root cause of an attack and automatically remediate threats

ANSWER: A

Explanation:

To identify the root cause of alerts and provide a complete forensic timeline of events is correct because Cortex XDR's Causality Analysis Engine correlates related endpoint activity into a causality chain. Rather than leaving an analyst with isolated detections, it traces relationships among processes, files, network activity, registry operations, and other observed events. This analysis helps identify the causality group owner: the initiating process or action associated with the chain of activity that led to the alert.

The resulting causality view supplies the investigative context needed to understand the sequence and scope of an incident. Analysts can follow the chain from the originating activity through subsequent child processes and actions, allowing them to reconstruct what occurred and assess the affected assets. This root-cause-oriented timeline is central to efficient incident investigation because it presents correlated evidence in context instead of requiring manual review of large volumes of raw telemetry. Palo Alto Networks describes Cortex XDR as correlating endpoint, network, and cloud data to support detection and investigation, and its documentation describes using causality views during alert investigation. See the Cortex XDR alert details documentation and the Cortex XDR product overview.

QUESTION NO: 2

A Cortex XDR incident confirms that a malicious process is actively encrypting files on a finance workstation. The SOC must immediately stop the process and prevent the endpoint from communicating with other internal systems while the investigation continues. Which two Cortex XDR response actions should the analyst perform? (Choose two answers)

A. Isolate the endpoint

B. Retrieve the malicious file

C. Terminate the malicious process

D. Add the file hash to the Global Block List

E. Open a Live Terminal session

ANSWER: A C

Explanation:

Isolate the endpoint and **terminate the malicious process** are correct. Endpoint isolation restricts the compromised device from communicating with the network while maintaining its connection to Cortex XDR for continued investigation and response. Terminating the active malicious process stops the observed encryption activity.

Adding a hash to the Global Block List helps prevent future execution of a known malicious file, but it does not stop the currently running process. Live Terminal supports hands-on collection and remediation, but it is not the fastest direct containment action for the stated requirements. Retrieving a file collects evidence but does not contain the active threat.

QUESTION NO: 3

Which dashboard or module in Cortex XSIAM provides visibility into unmanaged devices, unauthorized shadow IT, and cloud assets that do not currently have a Cortex agent installed?

A. Host Insights

B. Asset Inventory

C. Cloud Discovery & Exposure

D. Identity Analytics

ANSWER: C

Explanation:

Cloud Discovery & Exposure is the Cortex XSIAM capability intended to identify assets that sit outside normal endpoint-agent coverage and therefore represent security visibility gaps. It helps security teams discover cloud-hosted resources, externally exposed services, unmanaged devices, and potential shadow IT that may not be represented by the organization's managed Cortex endpoint inventory. By correlating discovered assets with exposure and risk context, analysts can prioritize investigation of resources that are internet-facing, unknown to the security team, or insufficiently protected.

This visibility is important because an agent-based endpoint inventory can only report on devices where an agent is already deployed. Cloud Discovery & Exposure extends the organization's understanding beyond that managed population, supporting attack-surface management workflows and helping teams locate assets that require onboarding, remediation, ownership validation, or additional controls. Palo Alto Networks describes Cortex XSIAM as a platform that centralizes security operations data and workflows, including exposure-management capabilities. See the Cortex XSIAM product page and Palo Alto Networks' Attack Surface Management overview for additional context on discovering and assessing exposed and unknown assets.

QUESTION NO: 4

Which two statements are relevant to reports in Cortex XDR? (Choose two.)

A. They can be sent in a password protected PDF version.

B. They can be automatically pushed to the corporate intranet.

C. They can use mock data for visualization.

D. They can have an attached screenshot of an XQL query widget.

ANSWER: A D

Explanation:

Cortex XDR reporting supports securely distributing report output by email. When configuring a scheduled report, administrators can select PDF output and protect the PDF with a password. This enables recipients to access report content while providing an additional safeguard for potentially sensitive operational information, such as endpoint, user, alert, and incident data. The report-delivery workflow also supports defining recipients and a schedule, making it suitable for recurring stakeholder reporting.

Reports can also include an attached screenshot of an XQL query widget. Cortex XDR widgets visualize query results, and reports use the configured widgets to present the relevant data visually in generated output. Including widget screenshots preserves the chart, table, or other visualization that was configured for the report, allowing readers to review the report's findings without needing to manually run the underlying XQL query. These capabilities align with Cortex XDR's report configuration and scheduling features. For details, see the Palo Alto Networks documentation for Cortex XDR Reports and the XQL Query Language.

QUESTION NO: 5

A Cortex XSOAR tenant must automate investigations against two internal services in a restricted network segment. The Cortex XSOAR tenant cannot directly reach either service. Which two actions are required to execute the integrations from that segment? (Choose two answers)

A. Deploy an XSOAR Engine in the restricted network segment.

B. Assign the internal-service integration instances to the XSOAR Engine.

C. Deploy a Broker VM in place of the XSOAR Engine.

D. Allow inbound connections from the Cortex XSOAR tenant to both internal services.

ANSWER: A B

Explanation:

Deploy an XSOAR Engine in the restricted segment and **assign the relevant integration instances to that Engine** are correct. The Engine executes integration commands where network access to the internal services is available, then returns results to the Cortex XSOAR tenant. Assigning the integration instance ensures that commands for that instance are routed through the correct Engine.

A Broker VM is used for collection and forwarding of supported data sources into Cortex products; it does not provide remote execution for XSOAR integrations. The design does not require opening inbound connectivity from the tenant to the restricted segment, because the Engine uses outbound communication to connect with Cortex XSOAR.

QUESTION NO: 6

Which two functions are allowed when stitching logs in Cortex XDR? (Choose two.)

A. Providing real-time threat prevention or remediation of threats

B. Creating granular BIOC and correlation rules

C. Enabling creation of custom scripts for remediation of security incidents

D. Running investigation queries based on combined network and endpoint events

ANSWER: B D

Explanation:

Creating granular BIOC and correlation rules is supported by the enriched context produced through log stitching. Cortex XDR associates related network and endpoint telemetry so detections can evaluate meaningful relationships rather than isolated events. For example, detection logic can account for an endpoint process and its related network activity, improving the specificity and investigative value of behavioral analytics. This supports the development of more focused BIOC and correlation-based detections using the available enriched data.

Running investigation queries based on combined network and endpoint events is also a core use of stitched data. By associating observations from these telemetry sources, Cortex XDR enables analysts to investigate activity in context, pivot between related evidence, and construct a more complete sequence of events during triage and root-cause analysis. XQL investigations can use the normalized and correlated telemetry available in Cortex XDR to identify the affected host, process, user, and associated network communications. Palo Alto Networks describes the investigation capabilities and telemetry context in the Cortex XDR investigation documentation and documents BIOC-based behavioral detection in the BIOCs documentation.

QUESTION NO: 7

Where can an administrator begin to grant a new non-SSO user access to a Cortex XDR tenant? (Choose one answer)

A. Customer Support Portal

B. Cortex Gateway

C. Cortex XDR tenant settings under Access Management

D. IT Service Portal

ANSWER: B

Explanation:

Cortex Gateway is the correct starting point for granting a new non-SSO user access to a Cortex XDR tenant. Cortex Gateway is the centralized identity and application-access interface for Cortex products. An administrator first accesses the Cortex Gateway user-management workflow to add or invite the non-SSO user and associate that user with the applicable Cortex XDR tenant. This establishes the user's entitlement to enter the tenant through the Palo Alto Networks Cortex platform.

After the user has been granted tenant access, the administrator can configure the user's Cortex XDR role and the permissions required for their operational responsibilities. Separating platform-level user provisioning from tenant-level role assignment helps ensure that access is granted deliberately and that the user receives only the permissions appropriate to their job function. For non-SSO accounts, this workflow also supports the account invitation and credential-setup process needed before the user can sign in.

Palo Alto Networks documents Cortex platform and tenant administration in the Cortex documentation portal. Additional official guidance and product resources are available through the Cortex XDR product page.

QUESTION NO: 8

What is a primary responsibility of an incident responder in a SOC?

A. Mitigating incidents that have been escalated

B. Supervising vulnerability assessments and penetration tests

C. Determining or adjusting criticality of alerts

D. Developing incident recovery crises communications plans

ANSWER: A

Explanation:

Mitigating incidents that have been escalated is a primary responsibility of an incident responder because this role takes ownership once an alert has been validated and requires active investigation and response. The responder determines the incident's scope and impact, gathers and correlates relevant endpoint, network, identity, and log evidence, and carries out containment and remediation actions. Depending on the situation, those actions can include isolating an affected endpoint, terminating a malicious process, disabling or resetting a compromised account, blocking malicious indicators, and removing persistence mechanisms. The aim is to limit further harm while preserving sufficient evidence to support investigation and recovery.

In a Palo Alto Networks environment, Cortex XDR and Cortex XSIAM support this workflow by providing incident context, investigation views, and response capabilities that let security teams contain threats directly from the operational console. Escalated incident mitigation therefore reflects the hands-on operational purpose of incident response: reducing adversary dwell time, stopping malicious activity, and restoring affected assets safely. Palo Alto Networks describes endpoint response actions and investigation workflows in its Cortex XDR response documentation. This also aligns with the containment, eradication, and recovery activities defined in the NIST Computer Security Incident Handling Guide.