DUMPSBOSS.

Palo Alto Networks Systems Engineer ProfessionalCortex

Palo Alto Networks PSE-Cortex-Pro-24

Version Demo

Total Demo Questions: 17

Total Premium Questions: 172

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cortex XDR	69
Topic 2, Cortex XSOAR	62
Topic 3, Cortex XSIAM	21
Topic 4, Cortex Xpanse	11
Topic 5, Mix Questions	9
Total	172

QUESTION NO: 1

What are two manual actions allowed on War Room entries? (Choose two.)

A. Mark as artifact

B. Mark as scheduled entry

C. Mark as note

D. Mark as evidence

ANSWER: C D

Explanation:

Mark as note and **Mark as evidence** are the supported manual classifications for War Room entries. Marking an entry as a note lets an analyst preserve important investigation context, observations, or analyst-entered information in a form that is clearly distinguished from automated task output. This helps keep the incident record understandable for other analysts and for later review.

Marking an entry as evidence identifies the entry as material that supports the investigation or its conclusions. Evidence can be retained and reviewed as part of the incident's documented investigative record, helping teams maintain traceability for items that informed triage, containment, remediation, or closure decisions. These actions are performed from the War Room entry controls and apply to the selected entry without requiring a playbook step. Palo Alto Networks documents the War Room as the central incident workspace for reviewing entries and managing investigation context, while evidence handling is part of maintaining an auditable incident record. See the Cortex XSOAR War Room documentation and the Cortex XSOAR incidents documentation.

QUESTION NO: 2

A customer has no complete inventory of externally exposed assets and wants to identify unknown internet-facing services that may belong to the organization. The customer does not want to install agents or provide network credentials before discovery begins.

Which Cortex Xpanse capability addresses this requirement?

A. Public-internet discovery and asset attribution

B. Agent-based scanning of customer endpoints

C. Credentialed vulnerability scanning of internal networks

D. VPN-based discovery of remote user devices

ANSWER: A

Explanation:

Cortex Xpanse uses **public-internet discovery and attribution** to identify externally visible assets and associate relevant assets with the customer. This approach does not depend on an endpoint agent, internal-network credentials, or a customer-provided inventory. Internal vulnerability scanning and VPN-based discovery would only provide visibility into assets reachable through those internal methods.

QUESTION NO: 3

The certificate used for decryption was installed as a trusted toot CA certificate to ensure communication between the Cortex XDR Agent and Cortex XDR Management Console. What action needs to be taken if the administrator determines the Cortex XDR Agents are not communicating with the Cortex XDR Management Console?

A. add paloaltonetworks.com to the SSL Decryption Exclusion list

B. enable SSL decryption

C. disable SSL decryption

D. reinstall the root CA certificate

ANSWER: A

Explanation:

Adding *paloaltonetworks.com* to the SSL Decryption Exclusion list is the appropriate action. Cortex XDR agents must establish secure outbound HTTPS sessions with Palo Alto Networks cloud services, including the Cortex XDR management infrastructure. Even when an enterprise decryption certificate has been distributed to endpoints as a trusted root CA, SSL forward-proxy inspection can still interfere with agent connectivity because the agent's service communications, certificate validation, or cloud-service endpoints may not operate correctly through the decryption workflow. Excluding the Palo Alto Networks service domain from decryption allows the agent to establish its original end-to-end TLS connection to the Cortex XDR Management Console without SSL interception.

The exclusion should be implemented in the security device or proxy performing SSL decryption and should cover the required Palo Alto Networks/Cortex XDR service hostnames used by the tenant. This approach preserves encrypted agent-to-console communications while avoiding inspection-related registration, heartbeat, and telemetry-delivery failures. Palo Alto Networks documents the network connectivity requirements for Cortex XDR agents and the need to permit required cloud-service communications over HTTPS. See the Cortex XDR agent network-access documentation and the PAN-OS Decryption documentation.

QUESTION NO: 4 - (SIMULATION)

Rearrange the steps into the correct order for modifying an incident layout.

ANSWER: See the explanation for the answer

Explanation:

Correct order for modifying an incident layout:

1. Navigate to `Settings → Objects Setup → Incidents → Layouts`.
2. Locate and select the incident layout to change.
3. Click `Edit` (or open the layout in the layout editor).
4. Modify the layout as needed, such as adding, removing, or rearranging tabs, sections, and incident fields.
5. Click `Save` to apply the layout changes.

If the layout must be used by a particular incident type, ensure that incident type is configured to use the updated layout after saving.

QUESTION NO: 5

A security operations team creates a Cortex XSOAR incident type for suspected cloud-account compromise. Every incident of this type must start the approved investigation workflow automatically, and analysts must see an incident workspace designed for cloud-account evidence.

Which two incident type settings should be configured? (Choose two.)

A. Configure the approved playbook to run automatically

B. Assign an incident layout tailored to cloud-account evidence

C. Assign the incident type to an engine group

D. Assign the incident type to a dashboard widget

ANSWER: A B

Explanation:

The incident type should be configured to **run the approved playbook automatically** so the intended workflow begins when an incident of that type is created. It should also be associated with an **incident layout** tailored to the fields and investigation context required by cloud-account compromise cases.

An engine group controls distributed execution capacity, not incident presentation or automatic workflow selection. A dashboard widget can display operational information but does not define an incident type's handling behavior.

QUESTION NO: 6

A General Purpose Dynamic Section can be added to which two layouts for incident types? (Choose two)

A. "Close" Incident Form

B. Incident Summary

C. Incident Quick View

D. "New"/Edit" Incident Form

ANSWER: B C

Explanation:

General Purpose Dynamic Sections are supported in the **Incident Summary** and **Incident Quick View** layouts. These sections allow an administrator to present dynamically generated contextual content for an incident, rather than only displaying static incident fields. The Incident Summary is the primary analyst-facing incident workspace, so a dynamic section can expose useful investigation data, results, or contextual information while the incident is being handled. Incident Quick View provides a condensed incident view, and including a dynamic section there enables analysts to access the same type of generated context without opening the full incident workspace.

The section’s content is supplied dynamically, typically by automation or scripts configured for the section, making it useful for displaying information that depends on the current incident and its data. This layout capability helps tailor the analyst experience to the incident type and investigation workflow. Palo Alto Networks documents incident-layout customization and the use of dynamic sections in the Cortex XSOAR Administrator Guide: Customize an Incident Layout and Define a Dynamic Section.

QUESTION NO: 7

Which playbook feature allows concurrent execution of tasks?

A. parallel tasks

B. automation tasks

C. manual tasks

D. conditional tasks

ANSWER: A

Explanation:

Parallel tasks allow concurrent execution of multiple tasks in a Cortex XSOAR playbook. A playbook author can place tasks on separate branches that begin from the same point in the workflow. When the playbook reaches that branching point, Cortex XSOAR can run the independent tasks simultaneously rather than requiring one task to complete before the next begins. This is useful when several enrichment, collection, or validation activities do not depend on one another’s results,

helping reduce the overall time required to process an incident. The playbook's flow subsequently continues once the required parallel branches have completed and converge at the next applicable task. Cortex XSOAR documentation describes using parallel task branches to execute multiple playbook paths concurrently, while task configuration determines the specific automation or action performed within each branch. See the Cortex XSOAR playbook task documentation and the Cortex XSOAR Administrator Guide: Playbooks.

QUESTION NO: 8

What are two ways Cortex XSIAM monitors for issues with data ingestion? (Choose two.)

A. The Data Ingestion Health page identifies deviations from normal patterns of log collection

B. The Cortex XSIAM Command Center dashboard will display a red icon if a data source is having issues.

C. The tenant's compute units consumption will change dramatically, indicating a collection issue.

D. It automatically runs a copilot playbook to troubleshoot and resolve ingestion issues.

ANSWER: A B

Explanation:

Cortex XSIAM provides dedicated operational visibility for ingestion health rather than requiring administrators to infer ingestion problems from general resource use. The Data Ingestion Health page identifies deviations from normal patterns of log collection, allowing teams to compare current collection behavior with expected baselines and quickly investigate sources whose volume or delivery pattern has changed. This monitoring is valuable because an unexpected reduction, interruption, or abnormal pattern in telemetry can affect detection coverage and investigation context.

The Cortex XSIAM Command Center dashboard will display a red icon if a data source is having issues. This provides an at-a-glance operational signal that a source requires attention, so analysts and platform administrators can identify affected integrations without first navigating through detailed ingestion metrics. Together, the health page's trend and deviation analysis and the Command Center's visual source-status indicator provide complementary monitoring mechanisms: one supports detailed health assessment, while the other surfaces immediate status awareness.

For Cortex XSIAM administrative guidance and platform-monitoring documentation, see the Cortex XSIAM Administrator Guide and the Cortex XSIAM product overview.

QUESTION NO: 9

What is the primary mechanism for the attribution of attack surface data in Cortex Xpanse?

A. Active scanning with network-installed agents

B. Dark web monitoring

C. Customer-provided asset inventory lists

D. Scanning from public internet data sources

ANSWER: D

Explanation:

Scanning from public internet data sources is correct because Cortex Xpanse is built around continuous, global discovery of the externally visible attack surface. It scans the public-facing internet at scale to collect observable data about assets, services, certificates, domains, and other exposure indicators. Cortex Xpanse then applies its attribution capabilities to correlate those observed signals and identify which internet-connected assets belong to the customer's organization. This internet-first approach enables discovery of unknown, unmanaged, or incorrectly documented assets rather than limiting visibility to assets already known internally. The resulting attribution provides an organization-specific view of external exposure and helps security teams prioritize risks based on the assets that are actually accessible from the public internet. Palo Alto Networks describes Cortex Xpanse as providing attack surface management through continuous discovery and

attribution of internet-connected assets. See the Cortex Xpanse product overview and the Cortex Xpanse documentation for details on its internet-scale discovery and attribution model.

QUESTION NO: 10

Which two troubleshooting steps should be taken when an integration is failing to connect? (Choose two.)

A. Ensure the playbook is set to run in quiet mode to minimize CPU usage and suppress errors

B. Confirm the integration credentials or API keys are valid.

C. Check the integration logs and enable a higher logging level, if needed, view the specific error.

D. Confirm there are no dashboards or reports configured to use that integration instance.

ANSWER: B C

Explanation:

Confirming that the integration credentials or API keys are valid is an essential first step because Cortex XSOAR integrations authenticate to external products and services using the configured instance parameters. Credentials may have expired, been revoked, changed in the target service, or lack the permissions required for the integration's API calls. Revalidating the configured authentication details and permissions helps restore the connection and ensures that subsequent troubleshooting is based on a working authentication configuration.

Checking the integration logs and enabling a higher logging level when needed is equally important because the logs provide the concrete error returned during connection attempts. Detailed logging can expose authentication failures, DNS or network reachability issues, TLS certificate problems, proxy configuration issues, rate-limit responses, and malformed endpoint settings. This evidence enables an administrator to identify the failing part of the connection flow and take a targeted corrective action. Cortex XSOAR documentation describes how integration instances are configured and tested, while the administrator documentation covers using system information and logs for operational troubleshooting. See the Cortex XSOAR documentation and the Cortex XSOAR Administrator Guide.

QUESTION NO: 11

An Administrator is alerted to a Suspicious Process Creation security event from multiple users.

The users believe that these events are false positives Which two steps should the administrator take to confirm the false positives and create an exception? (Choose two)

A. With the Malware Security profile, disable the " Prevent Malicious Child Process Execution " module

B. Within the Malware Security profile add the specific parent process, child process, and command line argument to the child process whitelist

C. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments

D. Contact support and ask for a security exception.

ANSWER: B C

Explanation:

Reviewing the specific parent process, child process, and command-line arguments in the Cortex XDR security event is the appropriate validation step because a Suspicious Process Creation alert is based on the observed process relationship and execution context. The administrator should verify that the parent-child lineage, executable paths, command-line parameters, affected endpoints, and expected business activity match the legitimate application behavior reported by the users. This provides the precise indicators needed to establish that the repeated activity is expected rather than broadly suppressing a protection capability.

After that validation, adding the specific parent process, child process, and command-line argument to the child process whitelist in the Malware Security profile creates a narrowly scoped exception. Cortex XDR evaluates the defined process relationship and command-line context, allowing the approved behavior while retaining malicious-child-process prevention for unrelated processes and commands. This least-privilege exception approach both addresses the confirmed false positive and preserves endpoint protection coverage. Palo Alto Networks documents malware-profile configuration and endpoint protection exceptions in the Malware Security Profile documentation and provides investigation workflow guidance in the Cortex XDR Alerts documentation.

QUESTION NO: 12

Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR? (Choose two)

A. Security Event

B. HIP

C. Correlation

D. Analytics

ANSWER: A B

Explanation:

Security Event and **HIP** should be forwarded to Cortex Data Lake to provide Cortex XDR with the firewall and endpoint-posture context it needs for detection, investigation, and correlation. Security Event logging provides the security-relevant activity generated by the firewall, supplying telemetry that Cortex XDR can use alongside its endpoint and network analytics. This visibility helps connect observed security activity to users, hosts, and network sessions during an investigation.

HIP logging supplies Host Information Profile data from GlobalProtect-connected endpoints. HIP information identifies endpoint characteristics and posture attributes, such as operating-system details, security-software state, and other compliance-relevant information evaluated by policy. Making this context available in Cortex Data Lake allows Cortex XDR to enrich firewall-related investigations with endpoint posture data, improving the analyst's ability to understand the affected device and its security state.

These log types should be included in the firewall log-forwarding configuration targeting Cortex Data Lake so Cortex XDR can consume the relevant network-security and HIP telemetry. Palo Alto Networks Cortex XDR documentation is available at Cortex XDR Documentation, and additional Cortex XDR operational guidance is available through the Cortex XDR article library.

QUESTION NO: 13

A prospect has agreed to do a 30-day POC and asked to integrate with a product that Demisto currently does not have an integration with. How should you respond?

A. Extend the POC window to allow the solution architects to build it

B. Tell them we can build it with Professional Services.

C. Tell them custom integrations are not created as part of the POC

D. Agree to build the integration as part of the POC

ANSWER: D

Explanation:

Agree to build the integration as part of the POC. A proof of concept is intended to validate that the platform can address the prospect's real operational requirements, including connecting to the tools that are central to its security workflow. Demisto, now Cortex XSOAR, is designed to support both prebuilt content and custom integrations. Its integration framework enables

an integration to define commands that communicate with an external product and return normalized results for use in investigations, playbooks, and automation. Building the requested integration during the POC therefore demonstrates the extensibility that the prospect needs to evaluate, while also allowing the POC team to validate the integration against the prospect's environment and intended use cases. This approach should include agreeing on a practical scope, required API access, authentication method, and the specific actions or data to demonstrate within the 30-day period. Palo Alto Networks provides developer guidance for creating integrations and content packs, supporting this type of implementation work: Cortex XSOAR Integration Overview and Cortex XSOAR Integration Code Conventions.

QUESTION NO: 14

What method does the Traps agent use to identify malware during a scheduled scan?

A. Heuristic analysis

B. Local analysis

C. Signature comparison

D. WildFire hash comparison and dynamic analysis

ANSWER: D

Explanation:

WildFire hash comparison and dynamic analysis is correct because scheduled malware scans in the Traps agent use WildFire intelligence to determine whether scanned files are malicious. The agent calculates a file hash and checks it against WildFire's known-file information. This enables rapid identification of files for which WildFire already has a malicious verdict, without requiring the endpoint to independently reproduce the full analysis. When a file requires further inspection, WildFire analysis provides the cloud-based verdicting capability, including dynamic analysis in a controlled environment to observe malicious behavior. The resulting verdict and associated intelligence are then used by Traps to identify and report malicious files found by the scan. This approach combines efficient hash-based recognition of previously analyzed malware with the behavioral visibility supplied by WildFire for files needing deeper analysis. Palo Alto Networks describes WildFire as a cloud-based analysis service that identifies unknown threats and distributes verdicts to enforcement products. See the WildFire concepts documentation and the Traps malware scanning documentation.

QUESTION NO: 15

Which three Demisto incident type features can be customized under Settings > Advanced > Incident Types? (Choose three.)

A. Define whether a playbook runs automatically when an incident type is encountered

B. Set reminders for an incident SLA

C. Add new fields to an incident type

D. Define the way that incidents of a specific type are displayed in the system

E. Drop new incidents of the same type that contain similar information

ANSWER: A B D

Explanation:

Incident types in Demisto, now Cortex XSOAR, provide a way to apply consistent handling and presentation settings to incidents that share a common purpose. Administrators can associate an incident type with a playbook and configure the playbook to run automatically when an incident of that type is created. This ensures that the intended investigation and response workflow begins without requiring an analyst to manually select it.

An incident type can also be associated with an SLA configuration. SLA settings establish timing expectations for the incident lifecycle and can generate reminder notifications as thresholds or deadlines approach, helping teams track and meet

response commitments. Finally, the incident type can be assigned an incident layout, which controls the way incident data is organized and displayed to analysts, including the tabs, sections, and fields shown in the incident workspace. These settings allow a distinct workflow, operational timeline, and analyst-facing view for each incident category. Palo Alto Networks documents incident-type configuration and associated playbook/layout behavior in the Cortex XSOAR Administrator Guide; SLA concepts are also covered in the SLA configuration documentation.

QUESTION NO: 16

Which feature of Cortex XSIAM helps analyst reduce the noise and false positives that often plague traditional SIEM systems?

A. Alert range indicators

B. AI-generated correlation rules

C. Automatic incident scoring

D. Dynamic alarm fields

ANSWER: B

Explanation:

AI-generated correlation rules is correct because Cortex XSIAM applies artificial intelligence and machine learning to analyze large volumes of telemetry, identify related events, and correlate them into meaningful alerts and incidents. Rather than requiring analysts to manually connect isolated logs and alerts, the platform can recognize patterns across endpoint, network, cloud, identity, and other data sources. This context-driven correlation prioritizes activity that represents a credible attack chain, allowing routine or unrelated signals to be filtered from the analyst workflow.

This capability is central to XSIAM's goal of transforming the traditional SIEM model: it combines data management, detection, investigation, and response with analytics that reduce alert fatigue. By automating correlation and producing higher-fidelity detections, security teams can focus their time on incidents with greater operational significance and respond more quickly. Palo Alto Networks describes XSIAM as using AI-driven analytics and automation to reduce the volume of alerts requiring manual investigation. See the Cortex XSIAM product overview and the Cortex XSIAM documentation.

QUESTION NO: 17

How can Cortex XSOAR save time when a phishing incident occurs?

A. It can automatically email staff to warn them about the phishing attack and show them a copy of the email.

B. It can automatically respond to the phishing email to unsubscribe from future emails.

C. It can automatically purge the email from user mailboxes in which it has not yet been opened.

D. It can automatically identify every mailbox that received the phish and create corresponding cases for them.

ANSWER: C

Explanation:

It can automatically purge the email from user mailboxes in which it has not yet been opened. Cortex XSOAR phishing-response playbooks automate the operational steps that otherwise require analysts to manually investigate and remediate a reported message. After an email is identified as malicious, the playbook can use mail-security and email-platform integrations to search for matching messages throughout the organization and remove them from affected recipients' mailboxes. This containment action reduces the period in which users can interact with the phishing message, while also eliminating repetitive mailbox-by-mailbox remediation work for the security operations team. Cortex XSOAR's phishing-response deployment content is specifically designed to accelerate this workflow through prebuilt automation, including investigation enrichment, email search, and remediation actions such as message deletion or purge where supported by the connected email service. Organizations can still incorporate approval gates and incident-specific logic before executing

destructive remediation, but the central time-saving capability is orchestrating the purge at scale from the incident workflow. Palo Alto Networks describes this phishing-response automation in its Cortex XSOAR phishing-response deployment wizard overview. Additional implementation content and integrations are available through the Cortex XSOAR integration documentation.