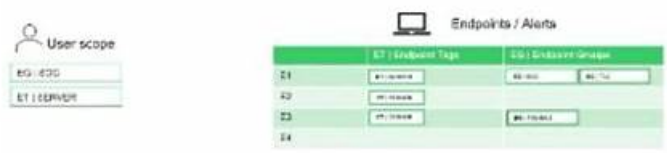
# XDR-Engineer Latest Test Format, XDR-Engineer Online Version




What's more, part of that Itbraindumps XDR-Engineer dumps now are free: https://drive.google.com/open?id=1ReGDOLBPOMxOfzL2mIF4u6bO4JsdOyLU

Itbraindumps Palo Alto Networks XDR-Engineer exam study material has three formats: XDR-Engineer PDF Questions, desktop Palo Alto Networks XDR-Engineer practice test software, and a XDR-Engineer web-based practice exam. You can easily download these formats of Palo Alto Networks XDR Engineer (XDR-Engineer) actual dumps and use them to prepare for the Palo Alto Networks XDR-Engineer Certification test. You don't need to enroll yourself in expensive XDR-Engineer exam training classes. With the Palo Alto Networks XDR-Engineer valid dumps, you can easily prepare well for the actual Palo Alto Networks XDR-Engineer exam at home.

## Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • Detection and Reporting: This section of the exam measures skills of the detection engineer and covers creating detection rules to meet security requirements, including correlation, custom prevention rules, and the use of behavioral indicators of compromise (BIOCs) and indicators of compromise (IOCs). It also assesses configuring exceptions and exclusions, as well as building custom dashboards and reporting templates for effective threat detection and reporting. |
| Topic 2 | • Planning and Installation: This section of the exam measures skills of the security engineer and covers the deployment process, objectives, and required resources such as hardware, software, data sources, and integrations for Cortex XDR. It also includes understanding and explaining the deployment and functionality of components like the XDR agent, Broker VM, XDR Collector, and Cloud Identity Engine. Additionally, it assesses the ability to configure user roles, permissions, and access controls, as well as knowledge of data retention and compute unit considerations. |
| Topic 3 | • Maintenance and Troubleshooting: This section of the exam measures skills of the XDR engineer and covers managing software component updates for Cortex XDR, such as content, agents, Collectors, and Broker VM. It also includes troubleshooting data management issues like data ingestion and parsing, as well as resolving issues with Cortex XDR components to ensure ongoing system reliability and performance. |
| Topic 4 | • Cortex XDR Agent Configuration: This section of the exam measures skills of the XDR engineer and covers configuring endpoint prevention profiles and policies, setting up endpoint extension profiles, and managing endpoint groups. The focus is on ensuring endpoints are properly protected and policies are consistently applied across the organization. |
| Topic 5 | • Ingestion and Automation: This section of the exam measures skills of the security engineer and covers onboarding various data sources including NGFW, network, cloud, and identity systems. It also includes managing simple automation rules, configuring Broker VM applets and clusters, setting up XDR Collectors, and creating parsing rules for data normalization and automation within the Cortex XDR environment. |

**>> XDR-Engineer Latest Test Format <<**

## XDR-Engineer Online Version | XDR-Engineer Frequent Updates

The web-based Palo Alto Networks XDR Engineer (XDR-Engineer) practice exam is accessible from any major OS, including Mac OS X, Linux, Android, Windows, or iOS. These Palo Alto Networks XDR-Engineer exam questions are browser-based, so there's no need to install anything on your computer. Chrome, IE, Firefox, and Opera all support this Palo Alto Networks XDR-Engineer web-based practice exam. You can take this Palo Alto Networks XDR Engineer (XDR-Engineer) practice exam without plugins and software installation.

## Palo Alto Networks XDR Engineer Sample Questions (Q23-Q28):

**NEW QUESTION # 23**
What are two possible actions that can be triggered by a dashboard drilldown? (Choose two.)

- A. Link to an XQL query
- B. Initiate automated response actions
- C. Navigate to a different dashboard
- D. Send alerts to console users

**Answer: A,C**

Explanation:
In Cortex XDR,dashboard drilldownsallow users to interact with widgets (e.g., charts or tables) by clicking on elements to access additional details or perform actions. Drilldowns enhance the investigative capabilities of dashboards by linking to related data or views.
* Correct Answer Analysis (A, C):
* A. Navigate to a different dashboard: A drilldown can be configured to navigate to another dashboard, providing a more detailed view or related metrics. For example, clicking on an alert count in a widget might open a dashboard focused on alert details.
* C. Link to an XQL query: Drilldowns often link to anXQL querythat filters data based on the clicked element (e.g., an alert name or source). This allows users to view raw events or detailed records in the Query Builder or Investigation view.
* Why not the other options?
* B. Initiate automated response actions: Drilldowns are primarily for navigation and data exploration, not for triggering automated response actions. Response actions (e.g., isolating an endpoint) are typically initiated from the Incident or Alert views, not dashboards.
* D. Send alerts to console users: Drilldowns do not send alerts to users. Alerts are generated by correlation rules or BIOCs, and dashboards are used for visualization, not alert distribution.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes drilldown functionality: "Dashboard drilldowns can navigate to another dashboard or link to an XQL query to display detailed data based on the selected widget element" (paraphrased from the Dashboards and Widgets section). TheEDU-262: Cortex XDR Investigation and Responsecourse covers dashboards, stating that "drilldowns enable navigation to other dashboards or XQL queries for deeper analysis" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "dashboards and reporting" as a key exam topic, encompassing drilldown configuration.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-262: Cortex XDR Investigation and Response Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

**NEW QUESTION # 24**
Based on the SBAC scenario image below, when the tenant is switched to permissive mode, which endpoint (s) data will be accessible?

- A. E1 only
- B. E1, E2, and E3
- C. E1, E2, E3, and E4
- D. E2 only

**Answer: B**

Explanation:
In Cortex XDR,Scope-Based Access Control (SBAC)restricts user access to data based on predefined scopes, which can be assigned to endpoints, users, or other resources. Inpermissive mode, SBAC allows users to access data within their assigned scopes but may restrict access to data outside those scopes. The question assumes an SBAC scenario with four endpoints (E1, E2, E3,

E4), where the user likely has access to a specific scope (e.g., Scope A) that includes E1, E2, and E3, while E4 is in a different scope (e.g., Scope B).
* Correct Answer Analysis (C):When the tenant is switched to permissive mode, the user will have access toE1, E2, and E3because these endpoints are within the user's assigned scope (e.g., Scope A).
E4, being in a different scope (e.g., Scope B), will not be accessible unless the user has explicit accessto that scope. Permissive mode enforces scope restrictions, ensuring that only data within the user's scope is visible.
* Why not the other options?
* A. E1 only: This is too restrictive; the user's scope includes E1, E2, and E3, not just E1.
* B. E2 only: Similarly, this is too restrictive; the user's scope includes E1, E2, and E3, not just E2.
* D. E1, E2, E3, and E4: This would only be correct if the user had access to both Scope A and Scope B or if permissive mode ignored scope restrictions entirely, which it does not. Permissive mode still enforces SBAC rules, limiting access to the user's assigned scopes.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains SBAC: "In permissive mode, Scope-Based Access Control restricts user access to endpoints within their assigned scopes, ensuring data visibility aligns with scope permissions" (paraphrased from the Scope-Based Access Control section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers SBAC configuration, stating that "permissive mode allows access to endpoints within a user's scope, such as E1, E2, and E3, while restricting access to endpoints in other scopes" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheet includes "post-deployment management and configuration" as a key exam topic, encompassing SBAC settings.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

**NEW QUESTION # 25**
Based on the image of a validated false positive alert below, which action is recommended for resolution?

- A. Disable an action to the CGO Process DWWIN.EXE
- B. Create an exception for the CGO DWWIN.EXE for ROP Mitigation Module
- C. Create an exception for OUTLOOK.EXE for ROP Mitigation Module
- D. Create an alert exclusion for OUTLOOK.EXE

**Answer: C**

Explanation:
In Cortex XDR, a false positive alert involvingOUTLOOK.EXEtriggering aCGO (Codegen Operation)alert related toDWWIN.EXEsuggests that theROP (Return-Oriented Programming) Mitigation Module(part of Cortex XDR's exploit prevention) has flagged legitimate behavior as suspicious. ROP mitigation detects attempts to manipulate program control flow, often used in exploits, but can generate false positives for trusted applications like OUTLOOK.EXE. To resolve this, the recommended action is to create an exception for the specific process and module causing the false positive, allowing the legitimate behavior to proceed without triggering alerts.
* Correct Answer Analysis (D):Create an exception for OUTLOOK.EXE for ROP Mitigation Moduleis the recommended action. Since OUTLOOK.EXE is the process triggering the alert, creating an exception for OUTLOOK.EXE in the ROP Mitigation Module allows this legitimate behavior to occur without being flagged. This is done by adding OUTLOOK.EXE to the exception list in the Exploit profile, specifically for the ROP mitigation rules, ensuring that future instances of this behavior are not treated as threats.
* Why not the other options?
* A. Create an alert exclusion for OUTLOOK.EXE: While an alert exclusion can suppress alerts for OUTLOOK.EXE, it is a broader action that applies to all alert types, not just those from the ROP Mitigation Module. This could suppress other legitimate alerts for OUTLOOK.EXE, reducing visibility into potential threats. An exception in the ROP Mitigation Module is more targeted.
* B. Disable an action to the CGO Process DWWIN.EXE: Disabling actions for DWWIN.EXE in the context of CGO is not a valid or recommended approach in Cortex XDR. DWWIN.EXE (Dr. Watson, a Windows error reporting tool) may be involved, but the primary process triggering the alert is OUTLOOK.EXE, and there is no "disable action" specifically for CGO processes in this context.
* C. Create an exception for the CGO DWWIN.EXE for ROP Mitigation Module: While DWWIN.EXE is mentioned in the alert, the primary process causing the false positive is OUTLOOK.EXE, as it's the application initiating the behavior. Creating an exception for DWWIN.EXE would not address the root cause, as OUTLOOK.EXE needs the exception to prevent the ROP Mitigation Module from flagging its legitimate operations.
Exact Extract or Reference:

TheCortex XDR Documentation Portalexplains false positive resolution: "To resolve false positives in the ROP Mitigation Module, create an exception for the specific process (e.g., OUTLOOK.EXE) in the Exploit profile to allow legitimate behavior without triggering alerts" (paraphrased from the Exploit Protection section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers exploit prevention tuning, stating that "exceptions for processes like OUTLOOK.EXE in the ROP Mitigation Module prevent false positives while maintaining protection" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing false positive resolution.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer
Note on Image: Since the image was not provided, I assumed a typical scenario where OUTLOOK.EXE triggers a false positive CGO alert related to DWWIN.EXE due to ROP mitigation. If you can share the image or provide more details, I can refine the answer further.

**NEW QUESTION # 26**
Which step is required to configure a proxy for an XDR Collector?

- A. Edit the YAML configuration file with the new proxy information
- B. Configure the proxy settings on the Cortex XDR tenant
- C. Restart the XDR Collector after configuring the proxy settings
- D. Connect the XDR Collector to the Pathfinder

**Answer: A**

Explanation:
TheXDR Collectorin Cortex XDR is a lightweight tool for collecting logs and events from servers and endpoints. When a proxy is required for the XDR Collector to communicate with the Cortex XDR cloud, the proxy settings must be configured in the collector's configuration file. Specifically, theYAML configuration file(e.g., config.yaml) must be edited to include the proxy details, such as the proxy server's address, port, and authentication credentials (if required).
* Correct Answer Analysis (A):To configure a proxy for the XDR Collector, the engineer mustedit the YAML configuration filewith the new proxy information. This involves adding or updating the proxy settings in the file, which the collector uses to route its traffic through the specified proxy server.
* Why not the other options?
* B. Restart the XDR Collector after configuring the proxy settings: While restarting the collector may be necessary to apply changes, it is not the primary step required to configure the proxy. The YAML file must be edited first.
* C. Connect the XDR Collector to the Pathfinder: The Pathfinder is a Cortex XDR feature for discovering endpoints, not for configuring proxy settings for the XDR Collector.
* D. Configure the proxy settings on the Cortex XDR tenant: Proxy settings for the XDR Collector are configured locally on the collector, not in the Cortex XDR tenant's web interface.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains XDR Collector configuration: "To configure a proxy for the XDR Collector, edit the YAML configuration file to include the proxy server details, such as address and port" (paraphrased from the XDR Collector Configuration section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers XDR Collector setup, stating that"proxy settings are configured by editing the collector's YAML file" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing XDR Collector configuration.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

**NEW QUESTION # 27**
When isolating Cortex XDR agent components to troubleshoot for compatibility, which command is used to turn off a component on a Windows machine?

- A. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" runtime stop

- B. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" stop
- C. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" -s stop
- D. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" occp

**Answer: A**

Explanation:
Cortex XDR agents on Windows include multiple components (e.g., for exploit protection, malware scanning, or behavioral analysis) that can be individually enabled or disabled for troubleshooting purposes, such as isolating compatibility issues. Thecytool.exeutility, located in the Cortex XDR installation directory (typically C:\Program Files\Palo Alto Networks\Traps\), is used to manage agent components and settings. The runtime stop command specifically disables a component without uninstalling the agent.
* Correct Answer Analysis (B):The command"C:\Program Files\Palo Alto Networks\Traps\cytool.
exe" runtime stopis used to turn off a specific Cortex XDR agent component on a Windows machine.
For example, cytool.exe runtime stop protection would disable the protection component, allowing troubleshooting for compatibility issues while keeping other components active.
* Why not the other options?
* A. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" stop: The xdr.exe binary is not used for managing components; it is part of the agent's corefunctionality. The correct utility is cytool.exe.
* C. "C:\Program Files\Palo Alto Networks\Traps\xdr.exe" -s stop: Similarly, xdr.exe is not the correct tool, and -s stop is not a valid command syntax for component management.
* D. "C:\Program Files\Palo Alto Networks\Traps\cytool.exe" occp: The occp command is not a valid cytool.exe option. The correct command for stopping a component is runtime stop.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains component management: "To disable a Cortex XDR agent component on Windows, use the command cytool.exe runtime stop <component> from the installation directory" (paraphrased from the Troubleshooting section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers agent troubleshooting, stating that "cytool.exe runtime stop is used to turn off specific components for compatibility testing" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "maintenance and troubleshooting" as a key exam topic, encompassing agent component management.
References:
Palo Alto Networks Cortex XDR Documentation Portal:https://docs-cortex.paloaltonetworks.com/ EDU-260: Cortex XDR Prevention and Deployment Course Objectives Palo Alto Networks Certified XDR Engineer Datasheet:https://www.paloaltonetworks.com/services/education/certification#xdr-engineer

**NEW QUESTION # 28**
.....

You may find that on our website, we have free renewal policy for customers who have bought our XDR-Engineer practice quiz. You can enjoy one year free updated service. This policy greatly increase the pass percentage of the candidates if they can't pass in one time or in the limited date. And they can enjoy 50% off if they buy them again one year later. All in all, our service is completely considerate. Come to experience our XDR-Engineer Training Materials.

XDR-Engineer ◁ and easily obtain a free download on ⇛ www.dumpsquestion.com ⇚ □Test XDR-Engineer Engine

- Quiz Palo Alto Networks - XDR-Engineer - Palo Alto Networks XDR Engineer –High Pass-Rate Latest Test Format □ Search for □ XDR-Engineer □ and download it for free immediately on ▷ www.pdfvce.com ◁ □XDR-Engineer PDF Dumps Files
- Valid XDR-Engineer Exam Notes □ Valid Dumps XDR-Engineer Ppt □ Valid XDR-Engineer Exam Guide □ Enter 【 www.examcollectionpass.com 】 and search for ⇛ XDR-Engineer ⇚ to download for free □XDR-Engineer PDF Dumps Files
- Quiz Palo Alto Networks - XDR-Engineer - Palo Alto Networks XDR Engineer –High Pass-Rate Latest Test Format □ Copy URL □ www.pdfvce.com □ open and search for [ XDR-Engineer ] to download for free □XDR-Engineer Latest Questions
- Valid Braindumps XDR-Engineer Pdf □ Reliable XDR-Engineer Exam Blueprint □ Cheap XDR-Engineer Dumps □ Search for ⇛ XDR-Engineer ⇚ and easily obtain a free download on ➡ www.prepawaypdf.com □□□ □Reliable XDR-Engineer Exam Bootcamp
- www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, k12.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

BONUS!!! Download part of Itbraindumps XDR-Engineer dumps for free: https://drive.google.com/open?id=1ReGDOLBPOMxOfzL2mIF4u6bO4JsdOyLU