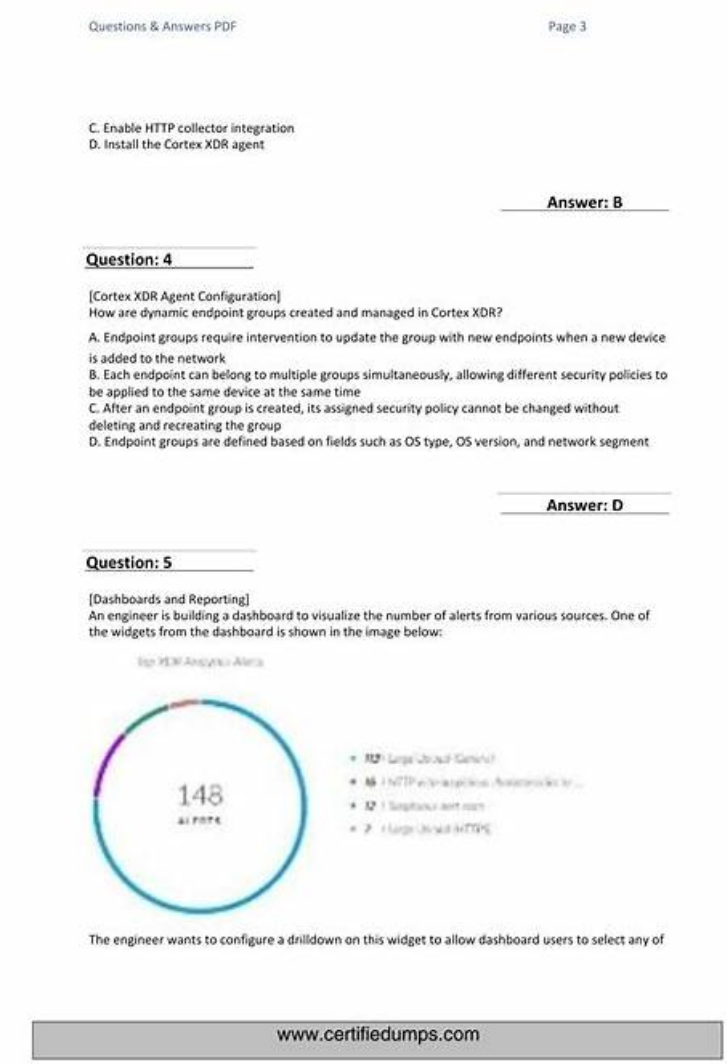
Free Download Reliable XDR-Engineer Learning Materials - How to Download for XDR-Engineer Valid Study Questions Free of Charge


Questions & Answers PDF Page 3

C. Enable HTTP collector integration
D. Install the Cortex XDR agent

Answer: B

Question: 4

[Cortex XDR Agent Configuration]
How are dynamic endpoint groups created and managed in Cortex XDR?

A. Endpoint groups require intervention to update the group with new endpoints when a new device is added to the network
B. Each endpoint can belong to multiple groups simultaneously, allowing different security policies to be applied to the same device at the same time
C. After an endpoint group is created, its assigned security policy cannot be changed without deleting and recreating the group
D. Endpoint groups are defined based on fields such as OS type, OS version, and network segment

Answer: D

Question: 5

[Dashboards and Reporting]
An engineer is building a dashboard to visualize the number of alerts from various sources. One of the widgets from the dashboard is shown in the image below:

148

The engineer wants to configure a drilldown on this widget to allow dashboard users to select any of

www.certifiedumps.com

P.S. Free & New XDR-Engineer dumps are available on Google Drive shared by Prep4sureExam: https://drive.google.com/open?id=1jevi-BW_7Nqux4TWQSfVcvb92Q0VwPfz

All contents of XDR-Engineer training guide are being explicit to make you have explicit understanding of this exam. Their contribution is praised for their purview is unlimited. None cryptic contents in XDR-Engineer learning materials you may encounter. And our XDR-Engineer Exam Questions are easy to understand and they are popular to be sold to all over the world. Just look at the comments on the website, then you will know that we have a lot of loyal customers.

By practicing under the real exam scenario of this Palo Alto Networks XDR-Engineer web-based practice test, you can cope with exam anxiety and appear in the final test with maximum confidence. You can change the time limit and number of questions of this Palo Alto Networks XDR-Engineer web-based practice test. This customization feature of our Palo Alto Networks XDR Engineer (XDR-Engineer) web-based practice exam aids in practicing as per your requirements. You can assess and improve your knowledge with our Palo Alto Networks XDR-Engineer practice exam.

>> Reliable XDR-Engineer Learning Materials <<

XDR-Engineer Valid Study Questions & New XDR-Engineer Exam Notes

It is well known that the best way to improve your competitive advantages in this modern world is to increase your soft power, such as graduation from a first-tier university, fruitful experience in a well-known international company, or even possession of some globally recognized XDR-Engineer certifications, which can totally help you highlight your resume and get a promotion in your workplace to a large extend. As a result, our XDR-Engineer Study Materials raise in response to the proper time and conditions while an increasing number of people are desperate to achieve success and become the elite.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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.
Topic 3	• 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 4	• 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 5	• 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.

Palo Alto Networks XDR Engineer Sample Questions (Q22-Q27):

NEW QUESTION # 22
A security audit determines that the Windows Cortex XDR host-based firewall is not blocking outbound RDP connections for certain remote workers. The audit report confirms the following:
* All devices are running healthy Cortex XDR agents.
* A single host-based firewall rule to block all outbound RDP is implemented.
* The policy hosting the profile containing the rule applies to all Windows endpoints.
* The logic within the firewall rule is adequate.
* Further testing concludes RDP is successfully being blocked on all devices tested at company HQ.
* Network location configuration in Agent Settings is enabled on all Windows endpoints.What is the likely reason the RDP connections are not being blocked?

- A. The profile's default action for outbound traffic is set to Allow
- B. Report mode is set to Enabled in the report settings under the profile configuration
- C. The pertinent host-based firewall rule group is only applied to internal rule groups
- D. The pertinent host-based firewall rule group is only applied to external rule groups

Answer: C

Explanation:
Cortex XDR'shost-based firewallfeature allows administrators to define rules to control network traffic on endpoints, such as blocking outbound Remote Desktop Protocol (RDP) connections (typically on TCP port
3389). The firewall rules are organized intorule groups, which can be applied based on the endpoint's network location(e.g., internal or external). Thenetwork location configurationin Agent Settings determines whether an endpoint is considered internal (e.g., on the company network at HQ) or external (e.g., remote workers on a public network). The audit confirms that a rule to block outbound RDP exists, the rule logic is correct, and it works at HQ but not for remote workers.
* Correct Answer Analysis (D):The likely reason RDP connections are not being blocked for remote workers is thatthe pertinent host-based firewall rule group is only applied to internal rule groups.
Since network location configuration is enabled, Cortex XDR distinguishes between internal (e.g., HQ) and external (e.g., remote workers) networks. If the firewall rule group containing the RDP block rule is applied only tointernal rule groups, it will only take effect for endpoints at HQ (internal network), as confirmed by the audit. Remote workers, on an external network, would not be subject to this rule group, allowing their outbound RDP connections to proceed.
* Why not the other options?
* A. The profile's default action for outbound traffic is set to Allow: While a default action of Allow could permit traffic not matched by a rule, the audit confirms the RDP block rule's logic is adequate and works at HQ. This suggests the rule is being applied correctly for internal endpoints, but not for external ones, pointing to a rule group scoping issue rather than the default action.
* B. The pertinent host-based firewall rule group is only applied to external rule groups: If the rule group were applied only to external rule groups, remote workers (on external networks) would have RDP blocked, but the audit shows the opposite-RDP is blocked at HQ (internal) but not for remote workers.
* C. Report mode is set to Enabled in the report settings under the profile configuration: If report mode were enabled, the firewall rule would only log RDP traffic without blocking it, but this would affect all endpoints (both HQ and remote workers). The audit shows RDP is blocked at HQ, so report mode is not enabled.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains host-based firewall configuration: "Firewall rule groups can be applied to internal or external network locations, as determined by the network location configuration in Agent Settings. Rules applied to internal rule groups will not affect endpoints on external networks" (paraphrased from the Host-Based Firewall section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers firewall rules, stating that "network location settings determine whether a rule group applies to internal or external endpoints, impacting rule enforcement" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing host-based firewall 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 # 23
A Custom Prevention rule that was determined to be a false positive alert needs to be tuned. The behavior was determined to be authorized and expected on the affected endpoint. Based on the image below, which two steps could be taken? (Choose two.)
[Image description: A Custom Prevention rule configuration, assumed to trigger a Behavioral Indicator of Compromise (BIOC) alert for authorized behavior]

- A. Apply an alert exception
- B. Apply an alert exclusion to the XDR behavioral indicator of compromise (BIOC) alert
- C. Apply an alert exclusion to the XDR agent alert
- D. Modify the behavioral indicator of compromise (BIOC) logic

Answer: A,B

Explanation:
In Cortex XDR, aCustom Prevention ruleoften leveragesBehavioral Indicators of Compromise (BIOCs)to detect specific patterns or behaviors on endpoints. When a rule generates a false positive alert for authorized and expected behavior, tuning is required to prevent future false alerts. The question assumes the alert is related to a BIOC triggered by the Custom Prevention rule, and the goal is to suppress or refine the alert without disrupting security.
* Correct Answer Analysis (A, B):
* A. Apply an alert exception: Analert exceptioncan be created in Cortex XDR to suppress alerts for specific conditions, such as a particular endpoint, user, or behavior. This is a quick way to prevent false positive alerts for authorized behavior without modifying the underlying rule, ensuring the behavior is ignored in future detections.
* B. Apply an alert exclusion to the XDR behavioral indicator of compromise (BIOC) alert:

Analert exclusionspecifically targets BIOC alerts, allowing administrators to exclude certain BIOCs from triggering alerts on specific endpoints or under specific conditions. This is an effective way to tune the Custom Prevention rule by suppressing the BIOC alert for the authorized behavior.
* Why not the other options?
* C. Apply an alert exclusion to the XDR agent alert: This option is incorrect because alert exclusions are applied to BIOCs or specific alert types, not to generic"XDR agent alerts." The term "XDR agent alert" is not a standard concept in Cortex XDR for exclusions, making this option invalid.
* D. Modify the behavioral indicator of compromise (BIOC) logic: While modifying the BIOC logic could prevent false positives, it risks altering the rule's effectiveness for other endpoints or scenarios. Since the behavior is authorized only on the affected endpoint, modifying the BIOC logic is less targeted than applying an exception or exclusion and is not one of the best steps in this context.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains alert tuning: "Alert exceptions suppress alerts for specific conditions, such as authorized behaviors, without modifying rules. Alert exclusions can be applied to BIOC alerts to prevent false positives on specific endpoints" (paraphrased from the Alert Management section). The EDU-262: Cortex XDR Investigation and Responsecourse covers alert tuning, stating that "exceptions and BIOC exclusions are used to handle false positives for authorized behaviors" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing alert tuning and BIOC management.
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
How can a Malware profile be configured to prevent a specific executable from being uploaded to the cloud?

- A. Add the executable to the allow list for executions
- B. Disable on-demand file examination for the executable
- C. Set PE and DLL examination for the executable to report action mode
- D. Create an exclusion rule for the executable

Answer: D

Explanation:
In Cortex XDR,Malware profilesdefine how the agent handles files for analysis, including whether they are uploaded to the cloud forWildFireanalysis or other cloud-based inspections. To prevent a specific executable from being uploaded to the cloud, the administrator can configure anexclusion rulein the Malware profile.
Exclusion rules allow specific files, directories, or patterns to be excluded from cloud analysis, ensuring they are not sent to the cloud while still allowing local analysis or other policy enforcement.
* Correct Answer Analysis (D):Creating anexclusion rulefor the executable in the Malware profile ensures that the specified file is not uploaded to the cloud for analysis. This can be done by specifying the file's name, hash, or path in the exclusion settings, preventing unnecessary cloud uploads while maintaining agent functionality for other files.
* Why not the other options?
* A. Disable on-demand file examination for the executable: Disabling on-demand file examination prevents the agent from analyzing the file at all, which could compromise security by bypassing local and cloud analysis entirely. This is not the intended solution.
* B. Set PE and DLL examination for the executable to report action mode: Setting examination to "report action mode" configures the agent to log actions without blocking or uploading, but it does not specifically prevent cloud uploads. This option is unrelated to controlling cloud analysis.
* C. Add the executable to the allow list for executions: Adding an executable to the allow list permits it to run without triggering prevention actions, but it does not prevent the file from being uploaded to the cloud for analysis.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Malware profile configuration: "Exclusion rules in Malware profiles allow administrators to specify files or directories that are excluded from cloud analysis, preventing uploads to WildFire or other cloud services" (paraphrased from the Malware Profile Configuration section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers agent configuration, stating that "exclusion rules can be used to prevent specific files from being sent to the cloud for analysis" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing Malware profile 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
When onboarding a Palo Alto Networks NGFW to Cortex XDR, what must be done to confirm that logs are being ingested successfully after a device is selected and verified?

- A. Confirm that the selected device has a valid certificate
- B. Wait for an incident that involves the NGFW to populate
- C. Conduct an XQL query for NGFW log data
- D. Retrieve device certificate from NGFW dashboard

Answer: C

Explanation:
When onboarding aPalo Alto Networks Next-Generation Firewall (NGFW)to Cortex XDR, the process involves selecting and verifying the device to ensure it can send logs to Cortex XDR. After this step, confirming successful log ingestion is critical to validate the integration. The most direct and reliable method to confirm ingestion is to query the ingested logs usingXQL (XDR Query Language), which allows the engineer to search for NGFW log data in Cortex XDR.
* Correct Answer Analysis (A):Conduct an XQL query for NGFW log datais the correct action.
After onboarding, the engineer can run an XQL query such as dataset = panw_ngfw_logs | limit 10 to check if NGFW logs are present in Cortex XDR. This confirms that logs are being successfully ingested and stored in the appropriate dataset, ensuring the integration is working as expected.
* Why not the other options?
* B. Wait for an incident that involves the NGFW to populate: Waiting for an incident is not a reliable or proactive method to confirm log ingestion. Incidents depend on detection rules and may not occur immediately, even if logs are beingingested.
* C. Confirm that the selected device has a valid certificate: While a valid certificate is necessary during the onboarding process (e.g., for secure communication), this step is part of the verification process, not a method to confirm log ingestion after verification.
* D. Retrieve device certificate from NGFW dashboard: Retrieving the device certificate from the NGFW dashboard is unrelated to confirming log ingestion in Cortex XDR. Certificates are managed during setup, not for post-onboarding validation.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains NGFW log ingestion validation: "To confirm successful ingestion of Palo Alto Networks NGFW logs, run an XQL query (e.g., dataset = panw_ngfw_logs) to verify that log data is present in Cortex XDR" (paraphrased from the Data Ingestion section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers NGFW integration, stating that "XQL queries are used to validate that NGFW logs are being ingested after onboarding" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "data ingestion and integration" as a key exam topic, encompassing log ingestion validation.
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 # 26
How can a customer ingest additional events from a Windows DHCP server into Cortex XDR with minimal configuration?

- A. Install the Cortex XDR agent
- B. Enable HTTP collector integration
- C. Activate Windows Event Collector (WEC)
- D. Install the XDR Collector

Answer: D

Explanation:
To ingest additional events from a Windows DHCP server into Cortex XDR with minimal configuration, the recommended approach is to use theCortex XDR Collector. TheXDR Collectoris a lightweight component designed to collect and forward logs and events from various sources, including Windows servers, to Cortex XDR for analysis and correlation. It is specifically optimized for scenarios where full Cortex XDR agent deployment is not required, and it minimizes configuration overhead by automating much of the data collection process.

For a Windows DHCP server, the XDR Collector can be installed on the server to collect DHCP logs (e.g., lease assignments, renewals, or errors) from the Windows Event Log or other relevant sources. Once installed, the collector forwards these events to the Cortex XDR tenant with minimal setup, requiring only basic configuration such as specifying the target data types and ensuring network connectivity to the Cortex XDR cloud. This approach is more straightforward than alternatives like setting up a full agent or configuring external integrations like Windows Event Collector (WEC) or HTTP collectors, which require additional infrastructure or manual configuration.
* Why not the other options?
* A. Activate Windows Event Collector (WEC): While WEC can collect events from Windows servers, it requires significant configuration, including setting up a WEC server, configuring subscriptions, and integrating with Cortex XDR via a separate ingestion mechanism. This is not minimal configuration.
* C. Enable HTTP collector integration: HTTP collector integration is used for ingesting data via HTTP/HTTPS APIs, which is not applicable for Windows DHCP server events, as DHCP logs are typically stored in the Windows Event Log, not exposed via HTTP.
* D. Install the Cortex XDR agent: The Cortex XDR agent is a full-featured endpoint protection and detection solution that includes prevention, detection, and responsecapabilities. While it can collect some event data, it is overkill for the specific task of ingesting DHCP server events and requires more configuration than the XDR Collector.
Exact Extract or Reference:
TheCortex XDR Documentation Portaldescribes theXDR Collectoras a tool for "collecting logs and events from servers and endpoints with minimal setup" (paraphrased from the Data Ingestion section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse emphasizes that "XDR Collectors are ideal for ingesting server logs, such as those from Windows DHCP servers, with streamlined configuration" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetlists "data source onboarding and integration configuration" as a key skill, which includes configuring XDR Collectors for log ingestion.
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
.....

I believe that you must know Prep4sureExam, because it is the website with currently the highest passing rate of XDR-Engineer certification exam in the market. You can download a part of XDR-Engineer free demo and answers on probation before purchase. After using it, you will find the accuracy rate of our XDR-Engineer test training materials is very high. What's more, after buying our XDR-Engineer exam dumps, we will provide renewal services freely as long as one year.

XDR-Engineer Valid Study Questions: https://www.prep4sureexam.com/XDR-Engineer-dumps-torrent.html

- Certification XDR-Engineer Exam Infor □ Latest XDR-Engineer Real Test □ XDR-Engineer Test Questions Fee □ Search for □ XDR-Engineer □ and download it for free on □ www.vceengine.com □ website □New XDR-Engineer Test Bootcamp
- 100% Pass Quiz XDR-Engineer - Professional Reliable Palo Alto Networks XDR Engineer Learning Materials □ Go to website { www.pdfvce.com } open and search for { XDR-Engineer } to download for free □XDR-Engineer Test Questions Fee
- XDR-Engineer Valid Braindumps Questions □ New XDR-Engineer Test Bootcamp □ Preparation XDR-Engineer Store □ Easily obtain free download of ☀ XDR-Engineer □☀□ by searching on ☀ www.torrentvce.com □☀□ □New XDR-Engineer Exam Objectives
- Reliable XDR-Engineer Learning Materials - Realistic 2026 Palo Alto Networks Palo Alto Networks XDR Engineer Valid Study Questions Pass Guaranteed □ Search for ✔ XDR-Engineer □✔□ and download it for free immediately on ▹ www.pdfvce.com ◃ □Reliable XDR-Engineer Exam Price
- XDR-Engineer Reliable Study Plan □ New XDR-Engineer Exam Objectives □ New XDR-Engineer Test Bootcamp □ Copy URL ➠ www.vceengine.com □ open and search for □ XDR-Engineer □ to download for free ⤴XDR-Engineer Pass Guaranteed
- Palo Alto Networks - XDR-Engineer –High Pass-Rate Reliable Learning Materials □ Search for （ XDR-Engineer ） and easily obtain a free download on ➡ www.pdfvce.com □□□ □XDR-Engineer Pass Guaranteed
- Valid XDR-Engineer Exam Dumps □ XDR-Engineer Test Questions Fee □ XDR-Engineer Latest Dump □ Open website □ www.prepawayexam.com □ and search for ➽ XDR-Engineer □ for free download □Certification XDR-Engineer Exam Dumps
- Certification XDR-Engineer Exam Infor □ XDR-Engineer Pass Guaranteed □ Latest XDR-Engineer Practice Questions

□ Search for ☀ XDR-Engineer □☀□ on 【 www.pdfvce.com 】 immediately to obtain a free download □Certification XDR-Engineer Exam Infor

- 2026 Reliable XDR-Engineer Learning Materials | Perfect 100% Free Palo Alto Networks XDR Engineer Valid Study Questions □ Search for ➤ XDR-Engineer □ and download exam materials for free through { www.prepawaypdf.com } □ □Reliable XDR-Engineer Exam Price
- Palo Alto Networks XDR Engineer Actual Test Guide Boosts the Function to Simulate the Exam - Pdfvce □ Search for 「 XDR-Engineer 」 and download it for free immediately on " www.pdfvce.com " □XDR-Engineer 100% Accuracy
- Top Reliable XDR-Engineer Learning Materials - Perfect XDR-Engineer Valid Study Questions - Fantastic New XDR-Engineer Exam Notes 🈸 Open □ www.pdfdumps.com □ enter □ XDR-Engineer □ and obtain a free download □XDR-Engineer Test Questions Fee
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, dionkrivenko.hathorpro.com, www.stes.tyc.edu.tw, disqus.com, www.hocnhanh.online, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BONUS!!! Download part of Prep4sureExam XDR-Engineer dumps for free: https://drive.google.com/open?id=1jevi-BW_7Nqux4TWQSfVcvb92Q0VwPfz