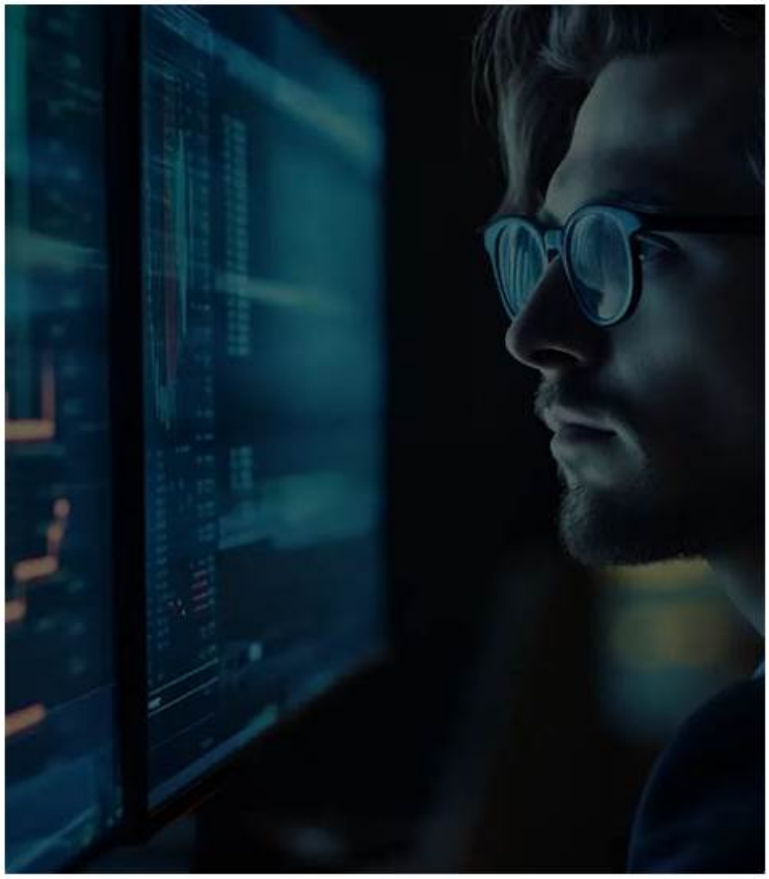
Test XDR-Engineer Practice | Official XDR-Engineer Practice Test



More and more people look forward to getting the XDR-Engineer certification by taking an exam. However, the exam is very difficult for a lot of people. Especially if you do not choose the correct study materials and find a suitable way, it will be more difficult for you to pass the exam and get the Palo Alto Networks related certification. If you want to get the related certification in an efficient method, please choose the XDR-Engineer learning dumps from our company. We can guarantee that the study materials from our company will help you pass the exam and get the certification in a relaxed and efficient method.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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.

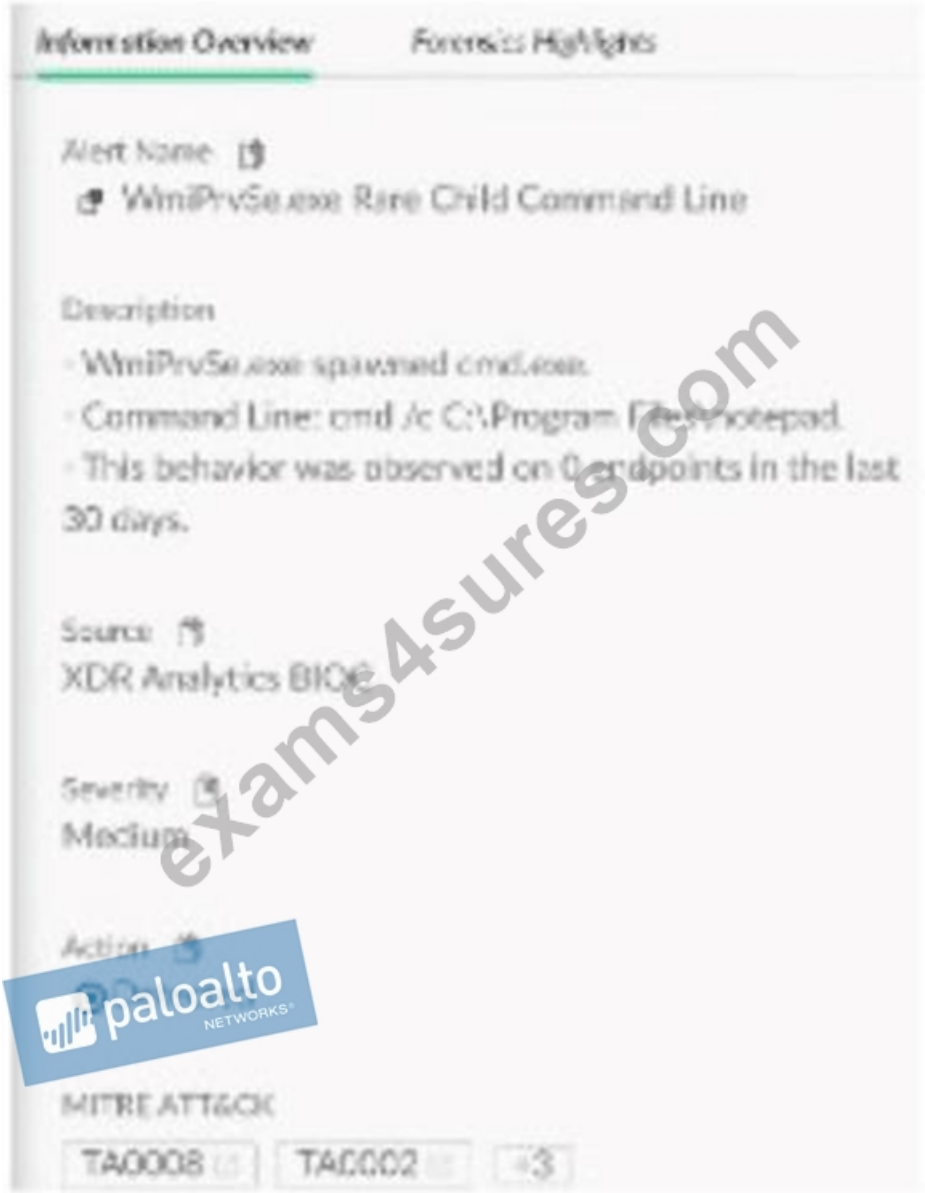
Topic 3	• Maintenance and Troubleshooting: This section of the exam measures skills of the XDR engineer and covers managing software component updates for Cortex XDR, such as content, agents, Collectors, and Broker VM. It also includes troubleshooting data management issues like data ingestion and parsing, 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	• 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.

Official XDR-Engineer Practice Test - Dump XDR-Engineer Check

We try our best to renovate and update our Palo Alto Networks XDR-Engineer study materials in order to help you fill the knowledge gap during your learning process, thus increasing your confidence and success rate. At the same time, Palo Alto Networks XDR-Engineer Preparation baindumps can keep pace with the digitized world by providing timely application. You will never fell disappointed with our XDR-Engineer exam quiz.

Palo Alto Networks XDR Engineer Sample Questions (Q32-Q37):

NEW QUESTION # 32
An analyst considers an alert with the category of lateral movement to be allowed and not needing to be checked in the future. Based on the image below, which action can an engineer take to address the requirement?



- A. Create an exception rule for the parent process and the exact command indicated in the alert
- B. Create a behavioral indicator of compromise (BIOC) suppression rule for the parent process and the specific BIOC: Lateral movement
- C. Create a disable injection and prevention rule for the parent process indicated in the alert
- D. Create an alert exclusion rule by using the alert source and alert name

Answer: D

Explanation:
In Cortex XDR, alateral movementalert (mapped to MITRE ATT&CK T1021, e.g., Remote Services) indicates potential unauthorized network activity, often involving processes like cmd.exe. If the analyst determines this behavior is allowed (e.g., a legitimate use of cmd /c dir for administrative purposes) and should not be flagged in the future, the engineer needs to suppress future alerts for this specific behavior. The most effective way to achieve this is by creating analert exclusion rule, which suppresses alerts based on specific criteria such as the alert source (e.g., Cortex XDR analytics) and alert name (e.g., "Lateral Movement Detected").
* Correct Answer Analysis (B):Create an alert exclusion rule by using the alert source and alert nameis the recommended action. This approach directly addresses the requirement by suppressing future alerts of the same type (lateral movement) from the specified source, ensuring that this legitimate activity (e.g., cmd /c dir by cmd.exe) does not generate alerts. Alert exclusions can be fine-tuned to apply to specific endpoints, users, or other attributes, making this a targeted solution.
* Why not the other options?
* A. Create a behavioral indicator of compromise (BIOC) suppression rule for the parent process and the specific BIOC: Lateral movement: While BIOC suppression rules can suppress specific BIOCs, the alert in question appears to be generated by Cortex XDR analytics (not a custom BIOC), as indicated by the MITRE ATT&CK mapping and alert category. BIOC suppression is more relevant for custom BIOC rules, not analytics-driven alerts.

* C. Create a disable injection and prevention rule for the parent process indicated in the alert: There is no "disable injection and prevention rule" in CortexXDR, and this option does not align with the goal of suppressing alerts. Injection prevention is related to exploit protection, not lateral movement alerts.
* D. Create an exception rule for the parent process and the exact command indicated in the alert: While creating an exception for the parent process (cmd.exe) and command (cmd /c dir) might prevent some detections, it is not the most direct method for suppressing analytics-driven lateral movement alerts. Exceptions are typically used for exploit or malware profiles, not for analytics-based alerts.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains alert suppression: "To prevent future checks for allowed alerts, create an alert exclusion rule using the alert source and alert name to suppress specific alert types" (paraphrased from the Alert Management section). TheEDU-262: Cortex XDR Investigation and Response course covers alert tuning, stating that "alert exclusion rules based on source and name are effective for suppressing analytics-driven alerts like lateral movement" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "detection engineering" as a key exam topic, encompassing alert suppression techniques.
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
Note on Image: The image was not provided, but I assumed a typical lateral movement alert involving a parent process (cmd.exe) and a command (cmd /c dir). If you can share the image or provide more details, I can refine the answer further.

NEW QUESTION # 33
During a recent internal purple team exercise, the following recommendation is given to the detection engineering team: Detect and prevent command line invocation of Python on Windows endpoints by non- technical business units. Which rule type should be implemented?

- A. Analytics Behavioral Indicator of Compromise (ABIOC)
- B. Behavioral Indicator of Compromise (BIOC)
- C. Correlation
- D. Indicator of Compromise (IOC)

Answer: B

Explanation:
The recommendation requires detecting and preventing the command line invocation of Python (e.g., python.
exe or py.exe) on Windows endpoints, specifically for non-technical business units. This involves identifying a specific behavior (command line execution of Python) and enforcing a preventive action (e.g., blocking the process). In Cortex XDR,Behavioral Indicators of Compromise (BIOCs)are used to define and detect specific patterns of behavior on endpoints, such as command line activities, and can be paired with a Restriction profileto block the behavior.
* Correct Answer Analysis (B):ABehavioral Indicator of Compromise (BIOC)rule should be implemented. The BIOC can be configured to detect the command line invocation of Python by defining conditions such as the process name (python.exe or py.exe) and the command line arguments.
For example, a BIOC rule might look for process = python.exe with a command line pattern like cmd.
exe /c python*. This BIOC can then be added to a Restriction profile to prevent the execution of Python by non-technical business units, which can be targeted by applying the profile to specific endpoint groups (e.g., those assigned to non-technical units).
* Why not the other options?
* A. Analytics Behavioral Indicator of Compromise (ABIOC): ABIOCs are analytics-driven rules generated by Cortex XDR's machine learning and behavioralanalytics, not user-defined rules. They are not suitable for creating custom detection and prevention rules like the one needed here.
* C. Correlation: Correlation rules are used to generate alerts by correlating events across multiple datasets (e.g., network and endpoint data), but they do not directly prevent behaviors like command line execution.
* D. Indicator of Compromise (IOC): IOCs are used to detect specific artifacts (e.g., file hashes, IP addresses) associated with known threats, not to detect and prevent behavioral patterns like command line execution.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains BIOC rules: "Behavioral Indicators of Compromise (BIOCs) can detect specific endpoint behaviors, such as command line invocation of processes like Python, and prevent them when added to a Restriction profile" (paraphrased from the BIOC section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse covers detection engineering, stating that "BIOCs are used to detect and block specific behaviors, such as command line executions, on Windows endpoints" (paraphrased from course materials). ThePalo Alto

Networks Certified XDR Engineer datasheetincludes
"detection engineering" as a key exam topic, encompassing BIOC rule creation.
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 # 34
How can a customer ingest additional events from a Windows DHCP server into Cortex XDR with minimal configuration?

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

Answer: C

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 # 35
Which two steps should be considered when configuring the Cortex XDR agent for a sensitive and highly regulated environment? (Choose two.)

- A. Enable critical environment versions

- B. Create an agent settings profile where the agent upgrade scope is maintenance releases only
- C. Enable minor content version updates
- D. Create an agent settings profile, enable content auto-update, and include a delay of four days

Answer: B,D

Explanation:
In a sensitive and highly regulated environment (e.g., healthcare, finance), Cortex XDR agent configurations must balance security with stability and compliance. This often involves controlling agent upgrades and content updates to minimize disruptions while ensuring timely protection updates. The following steps are recommended to achieve this balance.
* Correct Answer Analysis (B, C):
* B. Create an agent settings profile where the agent upgrade scope is maintenance releases only: In regulated environments, frequent agent upgrades can introduce risks of instability or compatibility issues. Limiting upgrades tomaintenance releases only(e.g., bug fixes and minor updates, not major version changes) ensures stability while addressing critical issues. This is configured in the agent settings profile to control the upgrade scope.
* C. Create an agent settings profile, enable content auto-update, and include a delay of four days: Content updates (e.g., Behavioral Threat Protection rules, localanalysis logic) are critical for maintaining protection but can be delayed in regulated environments to allow for testing.
Enablingcontent auto-updatewith afour-day delayensures that updates are applied automatically but provides a window to validate changes, reducing the risk of unexpected behavior.
* Why not the other options?
* A. Enable critical environment versions: There is no specific "critical environment versions" setting in Cortex XDR. This option appears to be a misnomer and does not align with standard agent configuration practices for regulated environments.
* D. Enable minor content version updates: While enabling minor content updates can be useful, it does not provide the control needed in a regulated environment (e.g., a delay for testing).
Option C (auto-update with a delay) is a more comprehensive and appropriate step.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains agent configurations for regulated environments: "In sensitive environments, configure agent settings profiles to limit upgrades to maintenance releases and enable content auto-updates with a delay (e.g., four days) to ensure stability and compliance" (paraphrased from the Agent Settings section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers agent management, stating that "maintenance-only upgrades and delayed content updates are recommended for regulated environments to balance security and stability" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing settings for regulated environments.
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 # 36
Based on the Malware profile image below, what happens when a new custom-developed application attempts to execute on an endpoint?

- A. It will execute after the second attempt
- B. It will immediately execute
- C. It will not execute
- D. It will execute after one hour

Answer: C

Explanation:
Since no image was provided, I assume the Malware profile is configured with default Cortex XDR settings, which typically enforce strict malware prevention for unknown or untrusted executables. In Cortex XDR, the Malware profilewithin the security policy determines how executables are handled on endpoints. For anew custom-developed application(an unknown executable not previously analyzed or allow-listed), the default behavior is toblock executionuntil the file is analyzed byWildFire(Palo Alto Networks' cloud-based threat analysis service) or explicitly allowed via policy.
* Correct Answer Analysis (B):By default, Cortex XDR's Malware profile is configured toblock unknown executables, including new custom-developed applications, to prevent potential threats. When the application attempts ilustrator execute, the Cortex XDR agent intercepts it, sends it to WildFire for analysis (if not excluded), and blocks execution until a verdict is received. If the application is not on an allow list or excluded, itwill not executeimmediately, aligning with option B.
* Why not the other options?
* A. It will immediately execute: This would only occur if the application is on an allow list or if the Malware profile is configured to allow unknown executables, which is not typical for default settings.
* C. It will execute after one hour: There is no default setting in Cortex XDR that delays execution for one hour. Execution depends on the WildFire verdict or policy configuration, not a fixed time delay.
* D. It will execute after the second attempt: Cortex XDR does not have a mechanism that allows execution after a second attempt. Execution is either blocked or allowed based on policy and analysis results.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Malware profile behavior: "By default, unknown executables are blocked until a WildFire verdict is received, ensuring protection against new or custom- developed applications" (paraphrased from the Malware Profile Configuration section). TheEDU-260:
Cortex XDR Prevention and Deploymentcourse covers Malware profiles, stating that "default settings block unknown executables to prevent potential threats until analyzed" (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
Note on Image: Since the image was not provided, I assumed a default Malware profile configuration. If you can share the image or describe its settings (e.g., specific allow lists, exclusions, or block rules), I can refine the answer to match the exact configuration.

NEW QUESTION # 37

.....

XDR-Engineer also offers free demos, allowing users to test the quality and suitability of the XDR-Engineer exam dumps before purchasing. The demo provides access to a limited portion of the material, providing users with a better understanding of the content. Additionally, XDR-Engineer provides three months of free updates to ensure that candidates have access to the latest questions.

Official XDR-Engineer Practice Test: https://www.exams4sures.com/Palo-Alto-Networks/XDR-Engineer-practice-exam-dumps.html

- New Launch XDR-Engineer PDF Dumps [2025] - Palo Alto Networks XDR-Engineer Exam Question □ Open website [www.prep4pass.com] and search for ➽ XDR-Engineer □ for free download □Reliable XDR-Engineer Test Questions
- XDR-Engineer Exam Duration □ XDR-Engineer Latest Exam Fee □ Reliable XDR-Engineer Test Questions □ Open website [www.pdfvce.com] and search for （ XDR-Engineer ） for free download □XDR-Engineer Test Certification Cost
- Valid XDR-Engineer Exam Labs ▸ XDR-Engineer Dumps Questions □ XDR-Engineer Test Certification Cost □ Open ➠ www.prep4pass.com □ enter 「 XDR-Engineer 」 and obtain a free download □Valid XDR-Engineer Test Pdf
- XDR-Engineer Real Braindumps □ XDR-Engineer Exam Duration □ XDR-Engineer Valid Cram Materials □ Go to website ▸ www.pdfvce.com ◂ open and search for { XDR-Engineer } to download for free □New XDR-Engineer Test Book
- XDR-Engineer Exam Cram Questions □ XDR-Engineer Test Certification Cost ↙ Free XDR-Engineer Study Material 👆 Search for □ XDR-Engineer □ and download it for free immediately on □ www.pass4test.com □ □Reliable XDR-Engineer Test Questions
- New Test XDR-Engineer Practice | Pass-Sure XDR-Engineer: Palo Alto Networks XDR Engineer 100% Pass □ Open ▹ www.pdfvce.com ◃ and search for { XDR-Engineer } to download exam materials for free □XDR-Engineer Valid Cram Materials
- XDR-Engineer Exam Cram Questions □ XDR-Engineer Valid Cram Materials □ XDR-Engineer Exam Duration □ Easily obtain ▸ XDR-Engineer ◂ for free download through [www.testkingpdf.com] □Valid XDR-Engineer Exam Labs
- XDR-Engineer Valid Exam Notes □ New XDR-Engineer Test Book □ New XDR-Engineer Test Book □ Go to website （ www.pdfvce.com ） open and search for ➥ XDR-Engineer □ to download for free □XDR-Engineer Valid Exam Notes
- XDR-Engineer pass-king materials - XDR-Engineer test torrent - XDR-Engineer test-king guide □ “ www.passcollection.com ” is best website to obtain 《 XDR-Engineer 》 for free download □XDR-Engineer Valid Cram Materials
- New Launch XDR-Engineer PDF Dumps [2025] - Palo Alto Networks XDR-Engineer Exam Question □ Search for 《 XDR-Engineer 》 and easily obtain a free download on ➽ www.pdfvce.com □ □Free XDR-Engineer Study Material
- Test XDR-Engineer Practice - Realistic 2025 Palo Alto Networks Official Palo Alto Networks XDR Engineer Practice Test □ Open ☀ www.torrentvalid.com □☀□ enter ➡ XDR-Engineer □□□ and obtain a free download □XDR-Engineer Exam Duration
- www.stes.tyc.edu.tw, vxlxemito123.bluxeblog.com, 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, www.gpzj.net, 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, bbs.xinaiml.com, 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