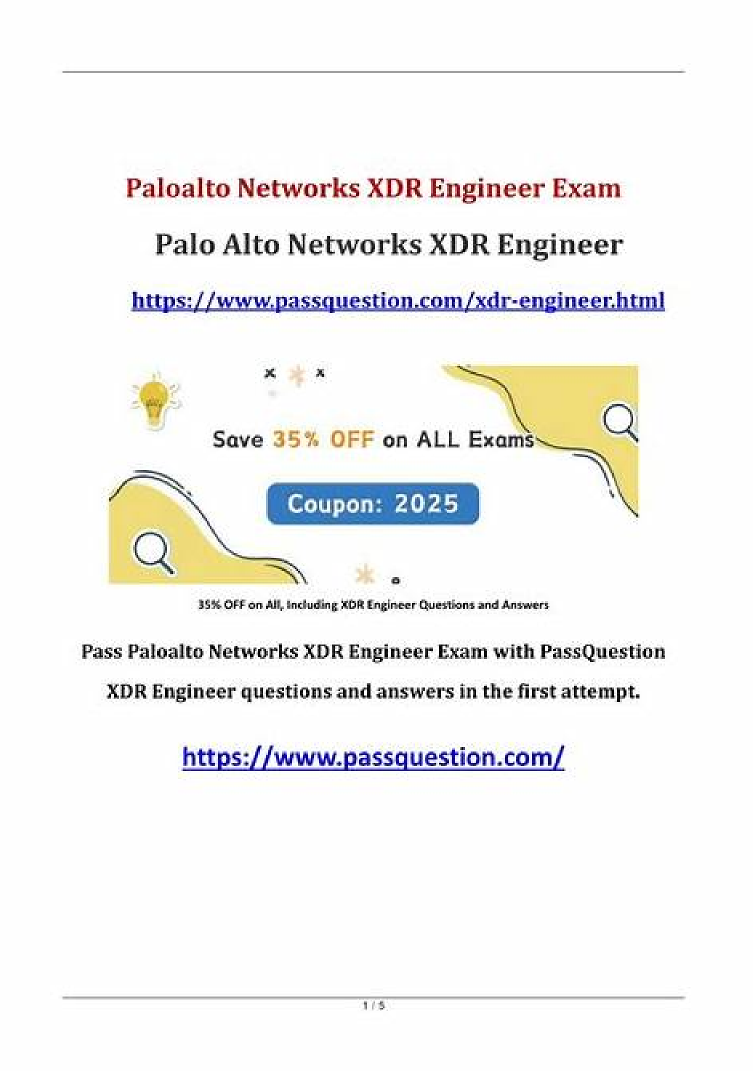
Updated Palo Alto Networks XDR-Engineer Questions To Clear XDR-Engineer Exam



Paloalto Networks XDR Engineer Exam

Palo Alto Networks XDR Engineer

https://www.passquestion.com/xdr-engineer.html

Save 35% OFF on ALL Exams

Coupon: 2025

35% OFF on All, Including XDR Engineer Questions and Answers

Pass Paloalto Networks XDR Engineer Exam with PassQuestion XDR Engineer questions and answers in the first attempt.

https://www.passquestion.com/

1 / 5

BONUS!!! Download part of ITExamSimulator XDR-Engineer dumps for free: https://drive.google.com/open?id=1drg63OIs69SNoPNg-OWkwyOX7a-8zR7m

All of the traits above are available in this web-based XDR-Engineer practice test of ITExamSimulator. The main distinction is that the Palo Alto Networks XDR-Engineer online practice test works with not only Windows but also Mac, Linux, iOS, and Android. Above all, taking the XDR-Engineer web-based practice test while preparing for the examination does not need any software installation. Furthermore, MS Edge, Internet Explorer, Opera, Safari, Chrome, and Firefox support the web-based Palo Alto Networks XDR-Engineer practice test of ITExamSimulator.

Palo Alto Networks XDR-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	- 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 3	- 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 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	- 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.

>> XDR-Engineer New Braindumps Ebook <<

Palo Alto Networks XDR-Engineer New Braindumps Ebook: Palo Alto Networks XDR Engineer - ITExamSimulator High-Efficient Practice Online for your preparing

If you want to get satisfying result in Palo Alto Networks XDR-Engineer practice test, our online training materials will be the best way to success, which apply to any level of candidates. We guarantee the best deal considering the quality and price of XDR-Engineer Braindumps Pdf that you won't find any better available. Our learning materials also contain detailed explanations expert for correct XDR-Engineer test answers.

Palo Alto Networks XDR Engineer Sample Questions (Q28-Q33):

NEW QUESTION # 28
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 one hour
- B. It will immediately execute
- C. It will execute after the second attempt
- D. It will not execute

Answer: D

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 # 29
An XDR engineer is configuring an automation playbook to respond to high-severity malware alerts by automatically isolating the affected endpoint and notifying the security team via email. The playbook should only trigger for alerts generated by the Cortex XDR analytics engine, not custom BIOCs. Which two conditions should the engineer include in the playbook trigger to meet these requirements? (Choose two.)

- A. Alert source is Cortex XDR Analytics
- B. Alert severity is High
- C. Alert category is Malware
- D. Alert status is New

Answer: B,C

Explanation:
In Cortex XDR,automation playbooks(also referred to as response actions or automation rules) allow engineers to define automated responses to specific alerts based on trigger conditions. The playbook in this scenario needs to isolate endpoints and send email notifications for high-severity malware alerts generated by the Cortex XDR analytics engine, excluding custom BIOC alerts. To achieve this, the engineer must configure the playbook trigger with conditions that match the alert's severity, category, and source.
* Correct Answer Analysis (A, C):
* A. Alert severity is High: The playbook should only trigger for high-severity alerts, as specified in the requirement. Setting the conditionAlert severity is Highensures that only alerts with a severity level of "High" activate the playbook, aligning with the engineer's goal.
* C. Alert category is Malware: The playbook targets malware alerts specifically. The condition Alert category is Malwareensures that the playbook only responds to alerts categorized as malware, excluding other types of alerts (e.g., lateral movement, exploit).
* Why not the other options?
* B. Alert source is Cortex XDR Analytics: While this condition would ensure the playbook triggers only for alerts from the Cortex XDR analytics engine (and not custom BIOCs), the requirement to exclude BIOCs is already implicitly met because BIOC alerts are typically categorized differently (e.g., as custom alerts or specific BIOC categories). The alert category (Malware) and severity (High) conditions are sufficient to target analytics-driven malware alerts, and adding the source condition is not strictly necessary for the stated requirements. However, if the engineer wanted to be more explicit, this condition could be considered, but the question asks for the two most critical conditions, which are severity and category.
* D. Alert status is New: The alert status (e.g., New, In Progress, Resolved) determines the investigation stage of the alert, but the requirement does not specify that the playbook should only trigger for new alerts. Alerts with a status of "InProgress" could still be high-severity malware alerts requiring isolation, so this condition is not necessary.
Additional Note on Alert Source: The requirement to exclude custom BIOCs and focus on Cortex XDR analytics alerts is

addressed by theAlert category is Malwarecondition, as analytics-driven malware alerts (e.
g., from WildFire or behavioral analytics) are categorized as "Malware," while BIOC alerts are often tagged differently (e.g., as custom rules). If the question emphasized the need to explicitly filter by source, option B would be relevant, but the primary conditions for the playbook are severity and category.

Exact Extract or Reference:

TheCortex XDR Documentation Portalexplains automation playbook triggers: "Playbook triggers can be configured with conditions such as alert severity (e.g., High) and alert category (e.g., Malware) to automate responses like endpoint isolation and email notifications" (paraphrased from the Automation Rules section).

TheEDU-262: Cortex XDR Investigation and Responsecourse covers playbook creation, stating that "conditions like alert severity and category ensure playbooks target specific alert types, such as high-severity malware alerts from analytics" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "playbook creation and automation" as a key exam topic, encompassing trigger condition 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 # 30

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

Answer: B

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 # 31
A static endpoint group is created by adding 321 endpoints using the Upload From File feature. However, after group creation, the members count field shows 244 endpoints. What are two possible reasons why endpoints were not added to the group? (Choose two.)

- A. Endpoints added to the group were in Disconnected or Connection Lost status when groupmembership was added
- B. Static groups have a limit of 250 endpoints when adding by file
- C. The IP address, hostname, or alias of the endpoints must match an existing agent that has registered with the tenant
- D. Endpoints added to the new group were previously added to an existing group

Answer: A,C

Explanation:
In Cortex XDR,static endpoint groupsare manually defined groups of endpoints, often created by uploading a file containing endpoint identifiers (e.g., IP addresses, hostnames, or aliases) using theUpload From File feature. If fewer endpoints are added to the group than expected (e.g., 244 instead of 321), there are several possible reasons related to endpoint status or registration.
* Correct Answer Analysis (C, D):
* **C. Endpoints added to the group were in Disconnected or Connection Lost status when group status when group membership was added: If endpoints are in aDisconnectedorConnection Loststatus (i.e., not actively communicating with the Cortex XDR tenant), they may not be successfully added to the group, as Cortex XDR requires active registration to validate and process group membership.
* D. The IP address, hostname, or alias of the endpoints must match an existing agent that has registered with the tenant: For endpoints to be added to a static group, their identifiers (IP address, hostname, or alias) in the uploaded file must correspond to agents that are registered with the Cortex XDR tenant. If the identifiers do not match registered agents, those endpoints will not be added to the group.
* Why not the other options?
* A. Static groups have a limit of 250 endpoints when adding by file: There is no documented limit of 250 endpoints for static groups in Cortex XDR when using the Upload From File feature.
The platform supports large numbers of endpoints in groups, and this is not a valid reason.
* B. Endpoints added to the new group were previously added to an existing group: In Cortex XDR, endpoints are assigned to a single group for policy application to avoid conflicts, but this does not prevent endpoints from being added to a new static group during creation. The issue lies in registration or connectivity, not prior group membership.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains endpoint group management: "Endpoints must be registered and actively connected to the tenant to be added to static groups. Unregistered or disconnected endpoints may not be included in the group" (paraphrased from the Endpoint Management section). TheEDU-
260: Cortex XDR Prevention and Deploymentcourse covers group creation, stating that "static groups require valid, registered endpoint identifiers, and disconnected endpoints may not be added" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "Cortex XDR agent configuration" as a key exam topic, encompassing endpoint group 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 # 32
The most recent Cortex XDR agents are being installed at a newly acquired company. A list with endpoint types (i.e., OS, hardware, software) is provided to the engineer. What should be cross-referenced for the Linux systems listed regarding the OS types and OS versions supported?

- A. Content Compatibility Matrix
- B. Agent Installer Certificate
- C. Kernel Module Version Support
- D. End-of-Life Summary

Answer: C

Explanation:
When installing Cortex XDR agents on Linux systems, ensuring compatibility with the operating system (OS) type and version is critical, especially for the most recent agent versions. Linux systems require specific kernel module support because the Cortex XDR agent relies on kernel modules for core functionality, such as process monitoring, file system protection, and network filtering. TheKernel Module Version Support documentation provides detailed information on which Linux distributions (e.g., Ubuntu, CentOS, RHEL) and kernel versions are supported by the Cortex XDR agent, ensuring the agent can operate effectively on the target systems.
* Correct Answer Analysis (B):TheKernel Module Version Supportshould be cross-referenced for Linux systems to verify that the OS types (e.g., Ubuntu, CentOS) and specific kernel versions listed are supported by the Cortex XDR agent. This ensures that the agent's kernel modules, which are essential for protection features, are compatible with the Linux endpoints at the newly acquired company.
* Why not the other options?
* A. Content Compatibility Matrix: A Content Compatibility Matrix typically details compatibility between content updates (e.g., Behavioral Threat Protection rules) and agent versions, not OS or kernel compatibility for Linux systems.
* C. End-of-Life Summary: The End-of-Life Summary provides information on agent versions or OS versions that are no longer supported by Palo Alto Networks, but it is not the primary resource for checking current OS and kernel compatibility.
* D. Agent Installer Certificate: The Agent Installer Certificate relates to the cryptographic verification of the agent installer package, not to OS or kernel compatibility.
Exact Extract or Reference:
TheCortex XDR Documentation Portalexplains Linux agent requirements: "For Linux systems, cross- reference the Kernel Module Version Support to ensure compatibility with supported OS types and kernel versions" (paraphrased from the Linux Agent Deployment section). TheEDU-260: Cortex XDR Prevention and Deploymentcourse covers Linux agent installation, stating that "Kernel Module Version Support lists compatible Linux distributions and kernel versions for Cortex XDR agents" (paraphrased from course materials). ThePalo Alto Networks Certified XDR Engineer datasheetincludes "planning and installation" as a key exam topic, encompassing Linux agent compatibility checks.
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 # 33
......

As you can find that there are three versions of our XDR-Engineer exam questions: the PDF, Software and APP online. Among them, the Software version has the function to stimulate the exam which can help the learners be adjusted to the atmosphere, pace and environment of the Real XDR-Engineer Exam. So our Software version of our XDR-Engineer learning guide can help you learn the study materials and prepare for the test better if you already know all the information about the real exam.

XDR-Engineer Practice Online: https://www.itexamsimulator.com/XDR-Engineer-brain-dumps.html

- Latest XDR-Engineer Test Simulator □ Exam XDR-Engineer Assessment □ XDR-Engineer Valid Test Simulator □ Search for 【 XDR-Engineer 】 and download exam materials for free through [www.dumpsquestion.com] □Exam XDR-Engineer Assessment
- Relevant XDR-Engineer Answers □ Exam XDR-Engineer Assessment □ Valid XDR-Engineer Braindumps □ Search for 「 XDR-Engineer 」 and download exam materials for free through ➥ www.pdfvce.com □ □Reliable XDR-Engineer Test Price
- XDR-Engineer Accurate Test 🏵 Guide XDR-Engineer Torrent □ Valid XDR-Engineer Dumps Demo □ Open □ www.dumpsquestion.com □ and search for ☀ XDR-Engineer □☀□ to download exam materials for free □Hot XDR-Engineer Questions
- XDR-Engineer exam dumps - XDR-Engineer torrent pdf - XDR-Engineer training guide □ Easily obtain ✔ XDR-Engineer □✔□ for free download through □ www.pdfvce.com □ □XDR-Engineer Boot Camp
- Guide XDR-Engineer Torrent □ XDR-Engineer Reliable Exam Topics □ Latest XDR-Engineer Test Labs □ 《

www.testkingpass.com 》 is best website to obtain ➡ XDR-Engineer □□□ for free download □Valid XDR-Engineer Dumps Demo

- XDR-Engineer exam dumps - XDR-Engineer torrent pdf - XDR-Engineer training guide □ ➥ www.pdfvce.com □ is best website to obtain ➡ XDR-Engineer □□□ for free download □XDR-Engineer Reliable Exam Topics
- Hot XDR-Engineer Questions ☯ XDR-Engineer Accurate Test □ Guide XDR-Engineer Torrent □ Open ✔ www.prepawayexam.com □✔□ enter 【 XDR-Engineer 】 and obtain a free download □XDR-Engineer Reliable Exam Topics
- XDR-Engineer Valid Test Simulator □ Latest XDR-Engineer Test Simulator □ Hot XDR-Engineer Questions □ Copy URL ⇛ www.pdfvce.com ⇚ open and search for ✔ XDR-Engineer □✔□ to download for free □Exam XDR-Engineer Book
- Buy Palo Alto Networks XDR-Engineer Valid Dumps Today and Get Free Updates for 1 year □ Search for 「 XDR-Engineer 」 and download it for free on （ www.validtorrent.com ） website □XDR-Engineer Lab Questions
- Guide XDR-Engineer Torrent □ Regualer XDR-Engineer Update □ Exam XDR-Engineer Assessment □ Open ☀ www.pdfvce.com □☀□ and search for [XDR-Engineer] to download exam materials for free □XDR-Engineer Regualer Update
- Exam Dumps XDR-Engineer Pdf □ Exam XDR-Engineer Book □ XDR-Engineer Practice Exam □ （ www.practicevce.com ） is best website to obtain （ XDR-Engineer ） for free download □XDR-Engineer Reliable Exam Topics
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 Palo Alto Networks XDR-Engineer dumps are available on Google Drive shared by ITExamSimulator: https://drive.google.com/open?id=1drg63OIs69SNoPNg-OWkwyOX7a-8zR7m