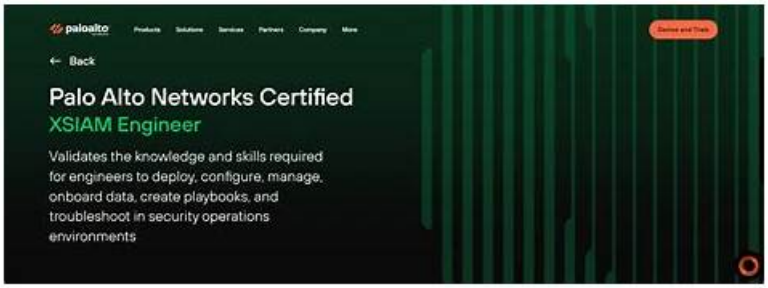
Test Certification XSIAM-Engineer Cost, Reliable XSIAM-Engineer Test Objectives



BONUS!!! Download part of Dumpkiller XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1mjFgI7Nc_DCNoO845bufJ9VVDZxUFPFF

Many people may worry that the XSIAM-Engineer guide torrent is not enough for them to practice and the update is slowly. We guarantee you that our experts check whether the XSIAM-Engineer study materials is updated or not every day and if there is the update the system will send the update to the client automatically. So you have no the necessity to worry that you don't have latest XSIAM-Engineer Exam Torrent to practice. We provide the best service to you and hope you are satisfied with our XSIAM-Engineer exam questions and our service.

Palo Alto Networks XSIAM-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• Content Optimization: This section of the exam measures skills of Detection Engineers and focuses on refining XSIAM content and detection logic. It includes deploying parsing and data modeling rules for normalization, managing detection rules based on correlation, IOCs, BIOCs, and attack surface management, and optimizing incident and alert layouts. Candidates must also demonstrate proficiency in creating custom dashboards and reporting templates to support operational visibility.
Topic 2	• Integration and Automation: This section of the exam measures skills of SIEM Engineers and focuses on data onboarding and automation setup in XSIAM. It covers integrating diverse data sources such as endpoint, network, cloud, and identity, configuring automation feeds like messaging, authentication, and threat intelligence, and implementing Marketplace content packs. It also evaluates the ability to plan, create, customize, and debug playbooks for efficient workflow automation.
Topic 3	• Maintenance and Troubleshooting: This section of the exam measures skills of Security Operations Engineers and covers post-deployment maintenance and troubleshooting of XSIAM components. It includes managing exception configurations, updating software components such as XDR agents and Broker VMs, and diagnosing data ingestion, normalization, and parsing issues. Candidates must also troubleshoot integrations, automation playbooks, and system performance to ensure operational reliability.
Topic 4	• Planning and Installation: This section of the exam measures skills of XSIAM Engineers and covers the planning, evaluation, and installation of Palo Alto Networks Cortex XSIAM components. It focuses on assessing existing IT infrastructure, defining deployment requirements for hardware, software, and integrations, and establishing communication needs for XSIAM architecture. Candidates must also configure agents, Broker VMs, and engines, along with managing user roles, permissions, and access controls.

>> Test Certification XSIAM-Engineer Cost <<

Free PDF 2026 First-grade Palo Alto Networks XSIAM-Engineer: Test Certification Palo Alto Networks XSIAM Engineer Cost

Our XSIAM-Engineer study tools not only provide all candidates with high pass rate study materials, but also provide them with good service. If you have some question or doubt about us or our products, you can contact us to solve it. The thoughtfulness of our XSIAM-Engineer study guide services is insuperable. What we do surly contribute to the success of XSIAM-Engineer practice materials.We all know that it is of great important to pass the XSIAM-Engineer Exam and get the certification for someone who wants to find a good job in internet area. I will recommend our study materials to you. It can be said that our XSIAM-Engineer test prep greatly facilitates users, so that users cannot leave their homes to know the latest information.

Palo Alto Networks XSIAM Engineer Sample Questions (Q175-Q180):

NEW QUESTION # 175
An XSIAM administrator is reviewing the audit logs for user activity and notices suspicious API calls originating from a compromised service account. The API key associated with this service account has 'Security Operations Center - Admin' permissions. The immediate action is to revoke the compromised API key. Which of the following XSIAM commands or API operations would be used to revoke a specific API key, assuming you have the necessary administrative privileges?

- A. Option D
- B. Option B
- C. Option E
- D. Option C
- E. Option A

Answer: B,D

Explanation:
Both the XSIAM UI and the XSIAM API provide mechanisms to revoke API keys. Option B describes the direct IJI approach, which is straightforward for administrators. Option C describes the typical REST API approach for deleting a resource, where DELETE requests are used to revoke or remove API keys. Option A is a pseudocode function call that might be part of an SDK, but not a direct API endpoint. Option D is an extreme measure that would disrupt all API integrations and is not the targeted way to revoke a single key. Option E is an unsupported and dangerous method of configuration management.

NEW QUESTION # 176
A complex XSOAR playbook integrating with multiple external security tools (EDR, Firewall, IAM) is failing intermittently with a generic 'NoneType' object has no attribute 'get'' error in a Python script task. The script processes data returned from a previous EDR query command. You've confirmed the EDR query command sometimes returns valid data and sometimes returns 'null' or an empty list. The script snippet causing the error is as follows:

```
alert_details = demisto.get(demisto.incidents()[0], 'details') # Line X
if alert_details:
    host_name = alert_details.get('host_info', {}).get('hostname') # Line Y
    # Further processing...
else:
    demisto.log('No alert details found.')
```

Which of the following approaches will most effectively debug and resolve this issue while making the playbook more robust?

- A. Implement an explicit 'try-except AttributeError' block around Line Y to catch the 'NoneType' error and log the state of 'alert_details'.
- B. Modify Line Y to 'host_name = alert_details and alert_details.get('host_info', to use short-circuiting for NoneType checks.
- C. Ensure that the 'details' field in the incident context is always populated by an earlier playbook task, potentially using a 'Set' command with a default empty dictionary.
- D. Before Line X, add a check 'if demisto.incidents() and len(demisto.incidents()) > 0:' to ensure an incident object exists, and handle the case where it doesn't.
- E. Analyze the EDR query command's output for cases where it returns 'null' or an empty list, and modify the playbook logic to proactively handle these specific outputs before passing them to the script.

Answer: E

Explanation:
The error 'NoneType' object has no attribute 'get'' at Line Y implies 'alert_details' is 'None'. The current 'if alert_details:' check should handle this if becomes *None' at that point. The problem is likely that 'details')' (Line X) itself is returning 'None' due to the EDR query's intermittent 'null' or empty list output. Option D directly addresses the root cause: the inconsistent output from the EDR query. By proactively handling these 'no data' scenarios before the script, the playbook becomes robust. Options A and B address potential 'NoneType' issues but don't solve the underlying data inconsistency. Option C is a reactive error handling, not a proactive solution. Option E attempts to force a default, but the EDR output itself needs robust handling.

NEW QUESTION # 177
During the planning phase for a Palo Alto Networks XSIAM deployment, a security architect needs to determine the appropriate XSIAM tenant size and scale. The organization anticipates collecting data from 50,000 endpoints, 200 network devices, and 5 major cloud platforms, generating approximately 10 TB of security logs daily. Which two key metrics should the architect prioritize when evaluating the XSIAM tenant's resource requirements?

- A. Required data retention period in Cortex Data Lake (CDL).
- B. Number of active XSIAM users and their roles.
- C. Geographic distribution of the organization's branch offices.
- D. Daily data ingestion rate (DDR) and anticipated data growth over 3 years.
- E. Total number of third-party integrations with XSIAM SOAR.

Answer: A,D

Explanation:
To determine the appropriate XSIAM tenant size and scale, the most critical metrics are the volume of data being ingested (Daily Data Rate - DDR) and the duration for which this data needs to be stored (Data Retention Period). DDR directly impacts the compute and ingestion pipeline capacity, while retention period dictates the required CDL storage. Anticipated data growth is crucial for future-proofing. The number of users (A) influences licensing but not core tenant sizing, geographic distribution (C) might affect CDL region choice but not core capacity, and third- party integrations (E) are more relevant for SOAR complexity than initial tenant sizing.

NEW QUESTION # 178
A critical XSIAM indicator rule detects 'Excessive Failed Login Attempts' on sensitive servers. The rule aggregates events and triggers if a user has more than 10 failed attempts within 5 minutes on a specific Currently, the rule frequently triggers for service accounts due to misconfigurations or temporary network issues, leading to alert fatigue. How can this rule be optimized using XSIAM's capabilities to reduce false positives for service accounts while maintaining efficacy for user accounts?

- A. Create two separate indicator rules: one for user accounts with the current threshold and another for service accounts with a significantly higher threshold (e.g., 50-100 failed attempts).
- B. Configure an automation playbook to automatically dismiss alerts for service accounts and send a daily summary report instead.
- C. Leverage XSIAM's 'Context Tables' or 'Lookup Lists' to maintain a list of known service accounts and their corresponding allowed failed login thresholds, and dynamically apply this within the XQL query using a 'join' or 'lookup' operation.
- D. Modify the rule to exclude service accounts (e.g., contains 'svc_") from the query entirely.
- E. Increase the threshold from 10 to 50 failed attempts for all accounts to reduce the overall alert volume.

Answer: A,C

Explanation:
Both C and D are strong, effective methods for addressing this complex scenario. C: Create Separate Rules: This is a straightforward and effective way to apply different logic based on account type. You create one rule for standard user accounts (with the lower threshold) and another, identical rule but with a higher threshold, specifically targeting identified service accounts. This clearly separates the monitoring logic. D: Leverage Context Tables/Lookup Lists: This is a more elegant and scalable solution, especially if you have many service accounts or different thresholds for various types of service accounts. You maintain a 'Context Table' (also known as a 'Lookup List') in XSIAM that maps service account names to their desired failed login thresholds. The indicator rule's XQL query can then 'join' or "lookup' this table to dynamically apply the correct threshold based on the 'user_name' in the event. This centralizes threshold management and reduces the need for multiple static rules. Option A reduces sensitivity for all

accounts, potentially missing user-based brute-force. Option B completely ignores service account issues, which can still be indicators of compromise. Option E is a post-detection automation, not a rule optimization; it still generates the false positive and consumes alert triage time.

NEW QUESTION # 179
An XSIAM engineer is performing content optimization on indicator rules. They notice that a rule designed to detect 'suspicious process injections' is generating an alarmingly high number of alerts, primarily from legitimate debugging tools and application updates. The current rule uses a broad XQL query:

```
dataset = xdr_data | filter event_type = 'Process Injection' and not process_name in ('svchost.exe', 'lsass.exe')
```

To reduce false positives without compromising the detection of malicious injections, which of the following modifications or considerations would be most effective? (Select all that apply)

- A. Implement a 'risk_score' threshold for the rule, only generating alerts if the aggregated risk score of the host or user exceeds a certain value.
- B. Refine the XQL query to include additional conditions such as 'target_process_integrity_level = 'System'' or 'injection_type = 'remote'' if the data is available, as these are often indicators of malicious activity.
- C. Adjust the rule's 'time window' for correlation to a shorter duration, assuming malicious injections are instantaneous.
- D. Add a filter for to exclude injections originating from known legitimate processes like Visual Studio or trusted update services.
- E. Create a pre-filtering rule with higher precedence to explicitly suppress alerts for processes with valid digital signatures and known clean hashes.

Answer: B,D,E

Explanation:
Options A, C, and D are all effective strategies for reducing false positives in this scenario. A: Filter by parent_process_name: Legitimate debugging or update tools often have predictable parent processes. Excluding injections originating from these known legitimate parents is a highly effective way to reduce noise. C: Refine with additional conditions: Malicious injections often target high-privilege processes or occur remotely. Leveraging fields like or 'injection_type' (if available in XDR data for 'Process Injection' events) makes the rule more precise for malicious intent. D: Pre-filtering with digital signatures/hashes: Legitimate software has valid digital signatures and known hashes. Suppressing alerts for processes matching these criteria is a very strong method to filter out benign events. This often involves creating a separate pre-filtering rule or leveraging XSIAM's trusted signer/hash capabilities. Option B (risk_score threshold) is a reactive measure for alert triage, not a content optimization for the rule itself. It still generates the underlying alert but might not escalate it. Option E (shorter time window) is generally not applicable to instantaneous events like process injection, and might cause detection gaps for multi-stage attacks.

NEW QUESTION # 180
.....

- 100% Pass Reliable XSIAM-Engineer - Test Certification Palo Alto Networks XSIAM Engineer Cost □ Open " www.pdfvce.com " enter [XSIAM-Engineer] and obtain a free download □XSIAM-Engineer Reliable Torrent
- XSIAM-Engineer Reliable Torrent □ XSIAM-Engineer Reliable Torrent □ XSIAM-Engineer Real Exam Answers □ （ www.practicevce.com ） is best website to obtain ➤ XSIAM-Engineer □ for free download □XSIAM-Engineer Real Exam Answers
- XSIAM-Engineer Valid Study Questions □ XSIAM-Engineer Reliable Torrent □ Well XSIAM-Engineer Prep □ Search for " XSIAM-Engineer " and download exam materials for free through 《 www.pdfvce.com 》 □XSIAM-Engineer Exam Material
- Free XSIAM-Engineer Exam □ Exam XSIAM-Engineer Fees ↔ Test XSIAM-Engineer Book ↔ Simply search for ➥ XSIAM-Engineer □ for free download on 「 www.easy4engine.com 」 □XSIAM-Engineer Exam Material
- Exam XSIAM-Engineer Details □ Customizable XSIAM-Engineer Exam Mode □ XSIAM-Engineer Exam Tutorial □ Open ✔ www.pdfvce.com □✔□ enter ✔ XSIAM-Engineer □✔□ and obtain a free download □Customizable XSIAM-Engineer Exam Mode
- XSIAM-Engineer Exam Dumps Get Success With Minimal Effort □ Copy URL （ www.pass4test.com ） open and search for ➤ XSIAM-Engineer □ to download for free □Customizable XSIAM-Engineer Exam Mode
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, witpacourses.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, stackblitz.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, anonup.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, 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, Disposable vapes

BONUS!!! Download part of Dumpkiller XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1mjFgI7Nc_DCNoO845bufJ9VVDZxUFPFF