Free PDF Quiz Pass-Sure XSIAM-Engineer - Reliable Palo Alto Networks XSIAM Engineer Exam Dumps

BONUS!!! Download part of ExamDumpsVCE XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1SJO9vMxWyhoA0BaPWX5qy7krkBJCRCkV

We want to provide our customers with different versions of XSIAM-Engineer test guides to suit their needs in order to learn more efficiently. Our XSIAM-Engineer qualification test can help you make full use of the time and resources to absorb knowledge and information. If you are accustomed to using the printed version of the material, we have a PDF version of the XSIAM-Engineer study tool for you to download and print, so that you can view the learning materials as long as you have free time. If you choose to study online, we have an assessment system that will make an assessment based on your learning of the XSIAM-Engineer qualification test to help you identify weaknesses so that you can understand your own defects of knowledge and develop a dedicated learning plan. Moreover our XSIAM-Engineer test guides provide customers with supplement service-mock test, which can totally inspire them to study hard and check for defects during their learning process. Our commitment is not frank, as long as you choose our XSIAM-Engineer study tool you will truly appreciate the benefits of our products.

XSIAM-Engineer certification exam is a very import component Palo Alto Networks certification exam. But passing Palo Alto Networks certification XSIAM-Engineer exam is not so simple. In order to give to relieve pressure and save time and effort for candidates who take a preparation for the XSIAM-Engineer Certification Exam, ExamDumpsVCE specially produce a variety of training tools. So you can choose an appropriate quick training from ExamDumpsVCE to pass the exam.

>> Reliable XSIAM-Engineer Exam Dumps <<

Dumps XSIAM-Engineer Cost | XSIAM-Engineer Study Reference

With the ExamDumpsVCE exam questions you will get the updated XSIAM-Engineer exam questions all the time and could not miss a single question in the final XSIAM-Engineer exam. As far as the price of XSIAM-Engineer exam questions is concerned, our Palo Alto Networks XSIAM-Engineer Exam prices are affordable for everyone. No one can beat us in terms of Palo Alto Networks XSIAM-Engineer exam question prices. Just download ExamDumpsVCE exam questions after paying affordable charges and start this journey.

Palo Alto Networks XSIAM Engineer Sample Questions (Q408-Q413):

NEW QUESTION # 408
An advanced XSIAM dashboard is required to analyze 'Lateral Movement' attempts, specifically focusing on RDP connections originating from non-standard internal subnets to critical servers. The dashboard should display: 1) Source IP, 2) Destination IP, 3) User, and 4) Connection time, for all such detected attempts. Additionally, it must provide a 'risk score' for each connection based on a custom lookup table of 'known risky internal IPs'. Which combination of XQL, lookup, and visualization would yield the most insightful dashboard?

- A.
```
dataset = network_connection_logs
| filter protocol = 'RDP' and source_ip in (non_standard_internal_subnets_lookup) and destination_ip in (critical_servers_lookup)
| lookup known_risky_internal_ips_lookup on source_ip as risky_ip_score
| select source_ip, destination_ip, user, connection_time, risky_ip_score
```
- B.
```
dataset = security_alerts
| filter alert_type = 'LateralMovement'
| timechart count()
```
- C.
```
dataset = network_connection_logs
| filter protocol = 'RDP'
| group by source_ip, destination_ip
```
- D. Use a pre-built 'Lateral Movement' widget, as custom risk scoring is not feasible.
- E. Manual parsing of RDP logs from endpoints and correlating them in a spreadsheet.

Answer: A

Explanation:
This scenario demands specific filtering, enrichment with a custom lookup, and detailed display. Option A demonstrates the correct approach. It filters `network_connection_logs` for RDP protocol and uses lookups (`non_standard_internal_subnets_lookup` and `critical_servers_lookup`, which would be pre-defined XSIAM lookups) to identify relevant source and destination IPs. The key is the `lookup known_risky_internal_ips_lookup on source_ip as risky_ip_score` command, which enriches the connection data with a custom risk score. Finally, `select` brings out the required fields. A 'Table' widget is perfect for displaying this structured data, and XSIAM tables support conditional formatting for visual emphasis on risk scores. Options B, C, D, and E are either too simplistic, don't meet the requirements for enrichment, or are not XSIAM-native solutions.

NEW QUESTION # 409
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?

- [ ] `XSIAM.API.revoke_key(key_id='')`
- [ ] Access the XSIAM UI -> Settings -> API Keys, locate the key, and click 'Revoke'.
- [ ] `DELETE /public_api/v1/api_keys/`
- [ ] Run `systemctl restart xsiam-api-service` to invalidate all current API keys and force re-issuance.
- [ ] Modify the XSIAM configuration file to comment out the compromised key entry.

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

Answer: A,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 # 410
The CISO requests a custom XSIAM reporting template that provides a weekly 'Executive Summary' of the top 3 critical threats detected, their MITRE ATT&CK techniques, the number of affected assets, and their geographic distribution. This report needs to be distributed as a PDF via email every Monday morning. To automate this, which XSIAM capabilities must be leveraged?

- A. Sending individual alerts via email and expecting the CISO to aggregate them.
- B. Utilizing only the built-in 'Security Operations' report and hoping it covers all executive summary points.
- C. Creating multiple individual dashboard widgets and manually compiling screenshots into a PDF.
- D. Defining a custom report template with XQL queries (using topk and join for MITRE ATT&CK correlation, and potentially geo-enrichment), configuring a 'Map' visualization for geographic distribution, and scheduling the report for email delivery in PDF format.
- E. Exporting raw incident data via API and using an external reporting tool to generate the summary.

Answer: D

Explanation:
Automating a comprehensive executive summary report with specific content and delivery requirements necessitates XSIAM's advanced reporting features. Option B accurately describes the necessary steps. A custom report template allows integrating complex XQL queries to derive the top threats, their MITRE ATT&CK techniques (likely requiring a with MITRE data or pre-enriched incident data), and affected join assets. Geographic distribution necessitates a 'Map' visualization within the report. Crucially, XSIAM's report scheduling feature supports automated email delivery in PDF format, directly addressing the CISO's request. Options A, C, D, and E are either manual, insufficient, or external to XSIAM's integrated reporting capabilities.

NEW QUESTION # 411
An XSIAM tenant has configured a detection rule to identify 'Lateral Movement via PowerShell Remoting'. This rule has a base score of 70. They also have two scoring rules: 1. Scoring Rule A: Condition: = 'DMZ" and 'alert.destination_zone = 'Internal_Servers". Action: Additive Score Change: +20. Order: 10.2. Scoring Rule B: Condition: 'alert.process_name contains 'powershell.exe" and = 'service_account". Action: Multiplicative Score Change: x0.8. Order: 20. If an alert is generated by the 'Lateral Movement via PowerShell Remoting' rule from a source in 'DMZ' to a 'Internal_Servers' destination, where the process is 'powershell.exe' and the user is a 'service_account', what is the final score of this alert? Assume the XSIAM score is capped at 100 and cannot go below 0.

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4

Answer: C

Explanation:
Let's trace the scoring process based on the 'Order' of the rules: 1. Initial Base Score: 70 2. Scoring Rule A (Order: 10) Condition: alert.source_zone = 'DMZ" and 'alert.destination_zone = The alert matches this condition. Action: Additive Score Change: +20. Current Score: 70 + 20 = 90'. 3. Scoring Rule B (Order: 20) Condition: 'alert.process_name contains 'powershell.exe" and 'alert.user_type = 'service_account" The alert matches this condition. Action: Multiplicative Score Change: x0.8. Final Score: '90 0.8 = 72. The final score is 72. This value is within the 0-100 cap.

NEW QUESTION # 412
You are tasked with hardening the security posture of custom integrations within your XSIAM marketplace content packs. Specifically, you need to ensure that API keys and sensitive credentials used by these integrations are stored and accessed securely. Which of the following is the most secure and recommended method for managing these secrets within the XSIAM environment?

- A. Hardcode API keys directly into the Python code of the integration's script. This makes them immediately available.
- B. Prompt the user for API keys every time the integration command is executed within a playbook.

- C. Store API keys as plaintext in the integration's YAML configuration file, as these files are only accessible to administrators.
- D. Encrypt API keys externally and then paste the encrypted string into the integration's configuration. The integration script will then decrypt it at runtime using a hardcoded decryption key.
- E. Utilize XSIAM's built-in credential store (secure parameters) for sensitive information. Integrations should access these parameters at runtime, and their values are encrypted at rest.

Answer: E

Explanation:
Option C is the most secure and recommended method. XSIAM (XSOAR) provides a secure credential store (often referred to as 'secure parameters' or 'instance settings' for integrations) specifically designed for managing sensitive information like API keys. These parameters are encrypted at rest and can be securely referenced by integration instances, ensuring that sensitive data is not exposed in code or configuration files. Options A, B, and D are highly insecure practices. Option E is impractical for automated playbooks.

NEW QUESTION # 413
.....

A free demo of any Palo Alto Networks XSIAM-Engineer exam dumps format will be provided by ExamDumpsVCE to the one who wants to assess before purchasing. The desktop Customer Experience XSIAM-Engineer Practice Exam software is compatible with windows based computers. There is a 24/7 customer support team of ExamDumpsVCE always to fix any problems.

Dumps XSIAM-Engineer Cost: https://www.examdumpsvce.com/XSIAM-Engineer-valid-exam-dumps.html

And for an office worker, the XSIAM-Engineer study engine is desighed to their different learning arrangement as well, such extensive audience greatly improved the core competitiveness of our XSIAM-Engineer practice quiz, which is according to their aptitude, on-demand, maximum to provide users with better suited to their specific circumstances, So it is necessary to select our XSIAM-Engineer exam torrent to get your indispensable Palo Alto Networks XSIAM-Engineer valid certification.

You could win free certification products from TestOut, or a gym bag from the Army National Guard, But Pew s work is rock solid, And for an office worker, the XSIAM-Engineer study engine is desighed to their different learning arrangement as well, such extensive audience greatly improved the core competitiveness of our XSIAM-Engineer practice quiz, which is according to their aptitude, on-demand, maximum to provide users with better suited to their specific circumstances.

Get Success in Palo Alto Networks XSIAM-Engineer Certification Exam on First Attempt

So it is necessary to select our XSIAM-Engineer exam torrent to get your indispensable Palo Alto Networks XSIAM-Engineer valid certification, A recent study revealed the surprising fact that there is a growing gulf between rich and poor.

It is simple to use, No attackers will know your personal information.

- Exam XSIAM-Engineer Revision Plan □ Dumps XSIAM-Engineer Free Download □ XSIAM-Engineer Latest Braindumps Sheet □ Search for □ XSIAM-Engineer □ and download it for free on ➥ www.examcollectionpass.com □ website □XSIAM-Engineer Passing Score Feedback
- Updated Reliable XSIAM-Engineer Exam Dumps offer you accurate Dumps Cost | Palo Alto Networks Palo Alto Networks XSIAM Engineer □ Search for ⇛ XSIAM-Engineer ⇚ and download exam materials for free through 《 www.pdfvce.com 》 □XSIAM-Engineer Trustworthy Exam Content
- Professional Reliable XSIAM-Engineer Exam Dumps - Easy and Guaranteed XSIAM-Engineer Exam Success □ Search for ✔ XSIAM-Engineer □✔□ and download exam materials for free through □ www.dumpsmaterials.com □ □XSIAM-Engineer Dumps
- XSIAM-Engineer Dumps □ XSIAM-Engineer Test Dumps □ Exam XSIAM-Engineer Revision Plan □ Open ➤ www.pdfvce.com □ enter （ XSIAM-Engineer ） and obtain a free download □Valid Exam XSIAM-Engineer Braindumps
- Reliable XSIAM-Engineer Exam Dumps | Valid Palo Alto Networks XSIAM Engineer 100% Free Dumps Cost □ Search on （ www.prepawayexam.com ） for ✔ XSIAM-Engineer □✔□ to obtain exam materials for free download □Exam XSIAM-Engineer Preparation
- Certification XSIAM-Engineer Test Answers ↔ XSIAM-Engineer Dumps □ XSIAM-Engineer Valid Exam Tutorial □ Immediately open ▸ www.pdfvce.com ◂ and search for □ XSIAM-Engineer □ to obtain a free download □XSIAM-Engineer Test Dumps