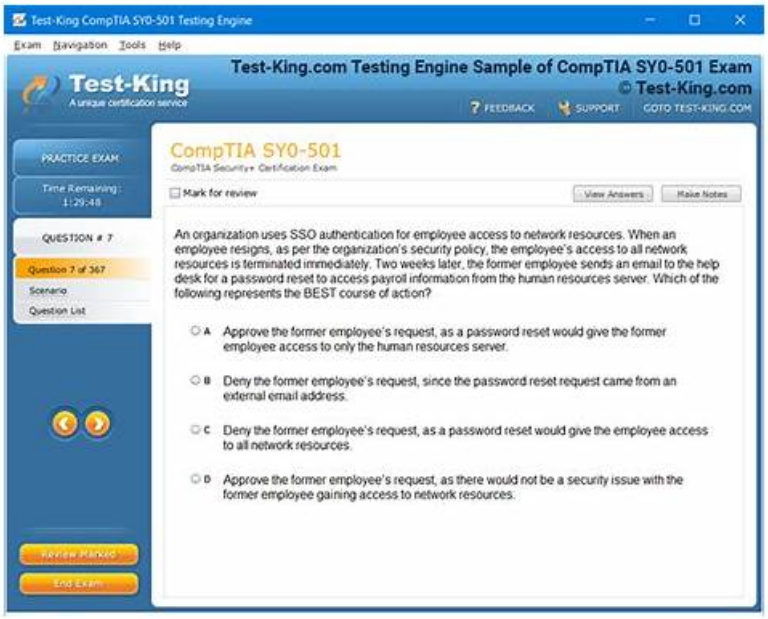
XSIAM-Engineer Latest Dumps Questions - Test XSIAM-Engineer Testking



P.S. Free 2025 Palo Alto Networks XSIAM-Engineer dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1SZwxYGxJljP4MztCEIH6NG71Y8Vq02T-

The web-based format gives results at the end of every Palo Alto Networks XSIAM-Engineer practice test attempt and points the mistakes so you can get rid of them before the final attempt. This online format of the Palo Alto Networks XSIAM Engineer (XSIAM-Engineer) practice exam works well with Android, Mac, Windows, iOS, and Linux operating systems.

XSIAM-Engineer Preparation materials will be the good helper for your qualification certification. We are concentrating on providing high-quality authorized XSIAM-Engineer study guide all over the world so that you can clear exam one time. XSIAM-Engineer reliable exam bootcamp materials contain three formats: PDF version, Soft test engine and APP test engine so that our products are enough to satisfy different candidates' habits and cover nearly full questions & answers of the real test.

>> XSIAM-Engineer Latest Dumps Questions <<

Test XSIAM-Engineer Testking, Clear XSIAM-Engineer Exam

PassExamDumps follows the career ethic of providing the first-class XSIAM-Engineer practice questions for you. Because we endorse customers' opinions and drive of passing the XSIAM-Engineer certificate, so we are willing to offer help with full-strength. With years of experience dealing with XSIAM-Engineer Learning Engine, we have thorough grasp of knowledge which appears clearly in our XSIAM-Engineer study quiz with all the keypoints and the latest questions and answers.

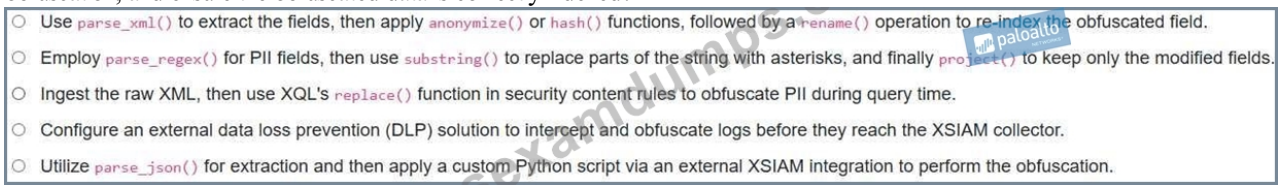
Palo Alto Networks XSIAM-Engineer Exam Syllabus Topics:

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	• 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.
Topic 4	• 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.

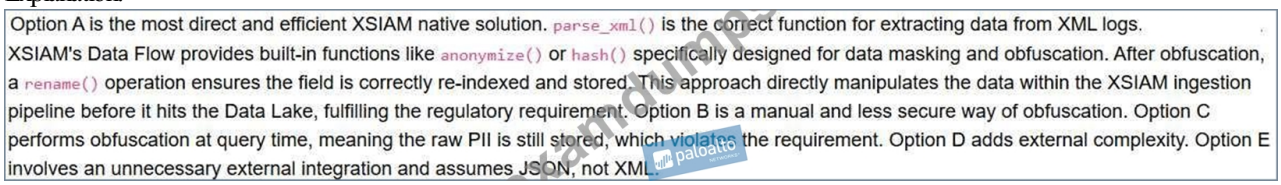
Palo Alto Networks XSIAM Engineer Sample Questions (Q392-Q397):

NEW QUESTION # 392
A new regulatory requirement mandates the obfuscation of specific Personally Identifiable Information (PII) fields (e.g., 'customer_ssn', 'patient_id') from logs originating from an application before they are stored in the XSIAM Data Lake. The raw logs are in a custom XML format. Which XSIAM Data Flow operation(s) would be most suitable to extract these fields, apply obfuscation, and ensure the obfuscated data is correctly indexed?

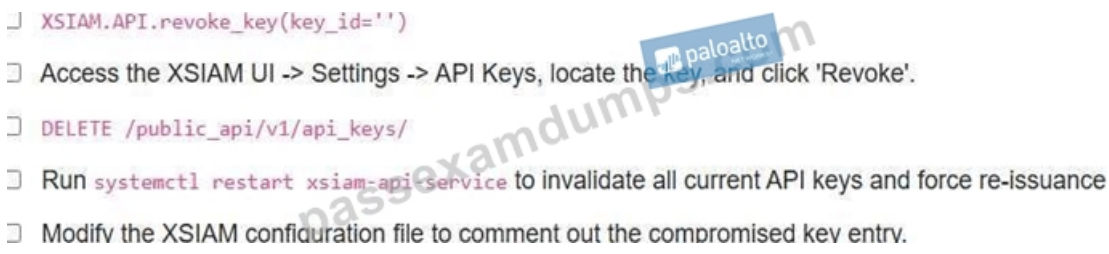


- A. Option E
- B. Option C
- C. Option D
- D. Option A
- E. Option B

Answer: D

Explanation:


NEW QUESTION # 393
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?

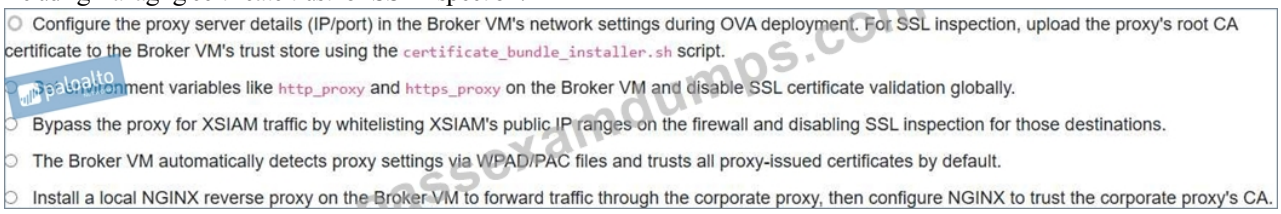


- A. Option E
- B. Option A
- C. Option D
- D. Option B
- E. Option C

Answer: D,E

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 # 394
An organization is deploying Broker VMS in geographically dispersed datacenters. They employ a strict network access control policy that restricts outbound internet access. All outbound traffic must traverse a corporate proxy server that performs SSL inspection. How can the Broker VM be configured to reliably communicate with the Cortex XSIAM cloud under these conditions, including managing certificate trust for SSL inspection?



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

Answer: D

Explanation:
To communicate through a corporate proxy with SSL inspection, the Broker VM needs two primary configurations: 1. Proxy settings: The Broker VM installation process or post-deployment configuration allows specifying proxy server details (IP/port). 2. Certificate Trust: Since the proxy performs SSL inspection, it re-signs the XSIAM certificates with its own CA. The Broker VM must trust this corporate proxy's root CA. This is achieved by uploading the proxy's root CA certificate to the Broker VM's trust store, typically using the provided Palo Alto Networks utility like Option B is insecure and not recommended. Option C bypasses the proxy, which violates the strict policy. Option certificate bundle installer. sh. D is incorrect; automatic detection and trusting all certificates is not how it works. Option E adds unnecessary complexity by introducing another proxy layer.

NEW QUESTION # 395
An XSIAM administrator is configuring a dashboard for endpoint security posture. A key metric is the 'Percentage of Endpoints with Outdated Antivirus Signatures'. The raw data in XSIAM's endpoint_status_logs includes a boolean field is_signature_current. Which XQL snippet would accurately represent this metric in a percentage format for a dashboard widget?

- A. 

- B.

```
dataset = endpoint_status_logs | count_distinct(endpoint_id) as total_endpoints | filter is_signature_current == false |
count_distinct(endpoint_id) as outdated_endpoints | eval percentage_outdated = (outdated_endpoints / total_endpoints)   100
```

- C.

```
dataset = endpoint_status_logs | filter is_signature_current == false | count(endpoint_id) as outdated_endpoints
```

- D.

```
-----------------------------------------------------------------------------------------------------------------
```

- E.

```
dataset = endpoint_status_logs | stats count(endpoint_id) as total_endpoints, sum(if(is_signature_current == false, 1, 0)) as outdated_count |
eval percentage_outdated = (outdated_count / total_endpoints)   100
```

Answer: E

Explanation:
To calculate the percentage of outdated antivirus signatures, you need two values: the total number of endpoints and the number of endpoints with outdated signatures. Option B correctly uses `stats count(endpoint_id) as total_endpoints` to get the total and `sum(if(is_signature_current == false, 1, 0)) as outdated_count` to conditionally count outdated endpoints. Finally, it uses `eval` to calculate the percentage. Option A attempts a similar logic but uses an incorrect flow for aggregation across different filtered states. Options C and D only count outdated endpoints or group by status without calculating the percentage. Option E has a syntactically incorrect approach for the division and conditional counting within the `eval` statement.

NEW QUESTION # 396
A sophisticated APT group is known to use custom exfiltration techniques involving DNS tunneling. They typically encode data within legitimate-looking DNS queries to external command and control (C2) domains that are rarely queried by legitimate enterprise applications. To detect this in XSIAM, a security engineer needs to craft a BIOC rule. The rule should focus on high-volume, repetitive DNS queries to unknown or suspicious domains, especially when originating from non-DNS server assets. Which combination of XSIAM XDR fields and query logic would be most effective for this BIOC, minimizing false positives?

- A.

```
-----------------------------------------------------------------------------------------------------------------
```

- B.

```
event_type = DNS AND network_direction = OUTBOUND AND Dns.ResponseCode != 'NOERROR' AND Process.Reputation = 'unknown'
```

- C.

```
-----------------------------------------------------------------------------------------------------------------
```

- D.

```
event_type = DNS AND network_direction = OUTBOUND AND Dns.QueryType = 'TXT' AND Dns.QueryName in (select Dns.QueryName from dns_events group by
Dns.QueryName having count( ) > 100)
```

- E.

```
event_type = DNS AND network_direction = OUTBOUND AND Dns.QueryName not in (select Dns.QueryName from dns_events where Device.Type =
'DNS_SERVER') AND Dns.QueryName not in external_reputation_good_domains AND Dns.QueryName length > 50 AND Process.Name !=
'dns.exe' group by Dns.QueryName, Source.Host.Name having count( ) > 50 AND time_window = 5m
```

Answer: E

Explanation:
Option C is the most effective and sophisticated BIOC for detecting DNS tunneling. Option A relies on known malicious domains, which might change. Option B specifically looks for TXT records and high volume, which is better but doesn't account for legitimate TXT use or source of queries. Option D is too simplistic. Option E focuses on response codes and process reputation, which is useful but might miss successful exfiltration or legitimate unknowns. Option C combines multiple strong indicators: outbound DNS, queries not seen from legitimate DNS servers, queries not in known good domains (leveraging XSIAM's external reputation), unusually long query names (indicative of encoded data), queries not from the legitimate DNS service itself, and a high volume from a single host within a short time window. This multi-faceted approach significantly reduces false positives while effectively targeting the described exfiltration technique.

NEW QUESTION # 397
.....

Due to professional acumen of expert's, our XSIAM-Engineer guide quiz has achieved the highest level in proficiency's perspective. For your particular inclination, we have various versions of our XSIAM-Engineer exam braindumps for you to choose:the PDF, the Software version and the APP online. Now take a look of their features and you can get realized of our XSIAM-Engineer Training Materials better. And as long as you purchase our XSIAM-Engineer study engine, you can enjoy free updates for one year long.

Test XSIAM-Engineer Testking: https://www.passexamdumps.com/XSIAM-Engineer-valid-exam-dumps.html

- www.examcollectionpass.com XSIAM-Engineer Palo Alto Networks XSIAM Engineer Exam Questions are Available in Three Different □ Open ➡ www.examcollectionpass.com □□□ enter □ XSIAM-Engineer □ and obtain a free download □XSIAM-Engineer Test Braindumps
- Palo Alto Networks certification XSIAM-Engineer exam best training materials □ Simply search for ➽ XSIAM-Engineer □ for free download on □ www.pdfvce.com □ □XSIAM-Engineer Valid Exam Pdf
- Free XSIAM-Engineer Braindumps □ XSIAM-Engineer Latest Test Online □ XSIAM-Engineer Valid Exam Objectives □ Search for ➠ XSIAM-Engineer □ and easily obtain a free download on ✔ www.exam4labs.com □✔□ □Free XSIAM-Engineer Braindumps
- Certification XSIAM-Engineer Training □ Exam XSIAM-Engineer Overview □ Free XSIAM-Engineer Braindumps □ ⇛ www.pdfvce.com ⇚ is best website to obtain □ XSIAM-Engineer □ for free download □Certification XSIAM-Engineer Training
- XSIAM-Engineer Complete Exam Dumps □ Interactive XSIAM-Engineer EBook □ Latest XSIAM-Engineer Test Format □ Open ➡ www.vce4dumps.com □□□ and search for ➠ XSIAM-Engineer □ to download exam materials for free □Test XSIAM-Engineer Study Guide
- Exam XSIAM-Engineer Overview □ XSIAM-Engineer Test Braindumps □ Valid Test XSIAM-Engineer Vce Free □ Copy URL “ www.pdfvce.com ” open and search for ➠ XSIAM-Engineer □ to download for free □XSIAM-Engineer Pass4sure
- XSIAM-Engineer Pass Guide □ XSIAM-Engineer Pass Guide □ XSIAM-Engineer Valid Test Prep □ Easily obtain free download of ➥ XSIAM-Engineer □ by searching on ➠ www.examcollectionpass.com □ □XSIAM-Engineer Valid Exam Pdf
- XSIAM-Engineer Latest Dumps Questions – 100% Pass-Rate Test Testking Providers for Palo Alto Networks XSIAM-Engineer: Palo Alto Networks XSIAM Engineer □ Easily obtain free download of ➥ XSIAM-Engineer □ by searching on 【 www.pdfvce.com 】 □Valid Test XSIAM-Engineer Testking
- Actual Palo Alto Networks XSIAM-Engineer Exam Questions In Different Formats □ □ www.prepawaypdf.com □ is best website to obtain □ XSIAM-Engineer □ for free download □Valid Test XSIAM-Engineer Vce Free
- XSIAM-Engineer Latest Dumps Questions – 100% Pass-Rate Test Testking Providers for Palo Alto Networks XSIAM-Engineer: Palo Alto Networks XSIAM Engineer □ Easily obtain □ XSIAM-Engineer □ for free download through ➤ www.pdfvce.com □ □Reliable XSIAM-Engineer Exam Online
- Palo Alto Networks certification XSIAM-Engineer exam best training materials □ Search for 「 XSIAM-Engineer 」 and obtain a free download on ▹ www.testkingpass.com ◃ □Latest XSIAM-Engineer Test Format
- whatoplay.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, myportal.utt.edu.tt, hcpedu.study, dorahacks.io, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.wcs.edu.eu, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2025 Palo Alto Networks XSIAM-Engineer dumps are available on Google Drive shared by PassExamDumps: https://drive.google.com/open?id=1SZwxYGxJljP4MztCEIH6NG71Y8Vq02T-