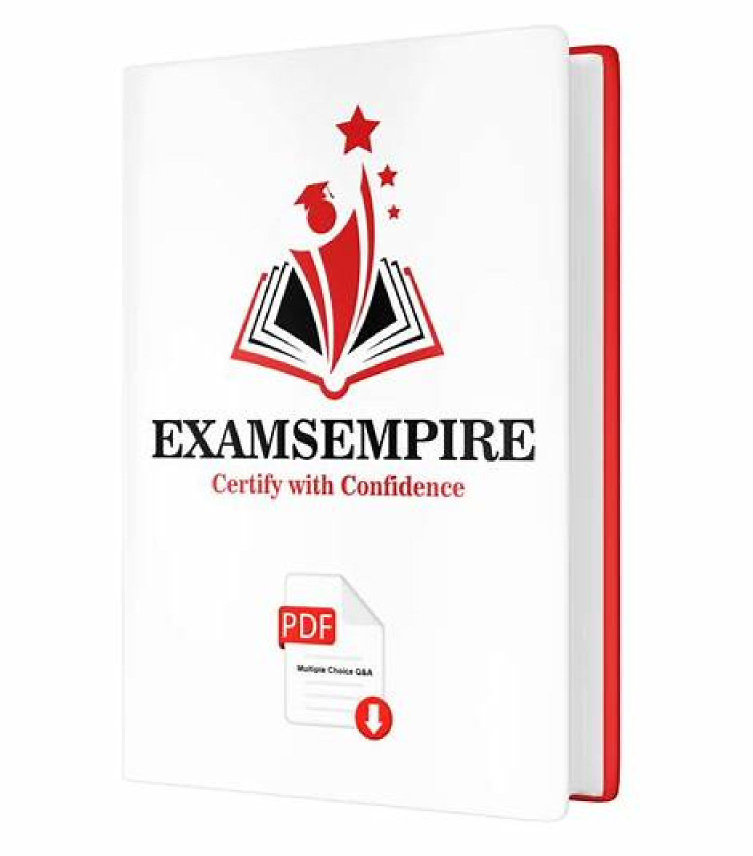
Free PDF Quiz Professional XSIAM-Engineer - Reliable Palo Alto Networks XSIAM Engineer Dumps Book



What's more, part of that ExamsLabs XSIAM-Engineer dumps now are free: https://drive.google.com/open?id=1ZRncGy4BS0Juwy80IhTOpINP5usycPuN

Continuous improvement is a good thing. If you keep making progress and transcending yourself, you will harvest happiness and growth. The goal of our XSIAM-Engineer latest exam guide is prompting you to challenge your limitations. People always complain that they do nothing perfectly. The fact is that they never insist on one thing and give up quickly. Our XSIAM-Engineer Study Dumps will assist you to overcome your shortcomings and become a persistent person. Once you have made up your minds to change, come to purchase our XSIAM-Engineer training practice.

Palo Alto Networks XSIAM-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 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.

>> Reliable XSIAM-Engineer Dumps Book <<

Latest XSIAM-Engineer Version - New XSIAM-Engineer Test Pdf

It is known to us that the error correction is very important for these people who are preparing for the XSIAM-Engineer exam in the review stage. It is very useful and helpful for a lot of people to learn from their mistakes, because many people will make mistakes in the same way, and it is very bad for these people to improve their accuracy. If you want to correct your mistakes when you are preparing for the XSIAM-Engineer Exam, the study materials from our company will be the best choice for you. Because our XSIAM-Engineer reference materials can help you correct your mistakes and keep after you to avoid the mistakes time and time again. We believe that if you buy the XSIAM-Engineer exam prep from our company, you will pass your exam in a relaxed state.

Palo Alto Networks XSIAM Engineer Sample Questions (Q10-Q15):

NEW QUESTION # 10
A large enterprise is implementing XSIAM and has a requirement to detect sophisticated insider threats involving data exfiltration over non-standard ports, correlated with user login activity from unusual geographical locations. The existing XSIAM rule set for data exfiltration is too broad, generating many false positives. Which of the following XSIAM Content Optimization strategies would be most effective in refining these detection rules to meet the specific requirements and reduce false positives, while ensuring high fidelity for actual threats?

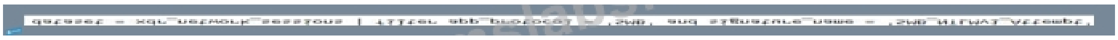
- A. Increase the severity of existing 'Data Exfiltration' rules and apply a global suppression for all alerts originating from internal IP ranges.
- B. Implement User and Entity Behavior Analytics (UEBA) without any custom rule creation, assuming UEBA will automatically identify the described threat.
- C. Create new correlation rules that combine 'Network Traffic Anomaly' events (specifically non-standard port usage) with 'Authentication' events (unusual login location) and 'Data Access' events (large file transfers), then tune thresholds for event counts over a defined time window.
- D. Modify existing rules by adding exclusion filters based on commonly used applications and services, without considering correlation with other event types.
- E. Disable all default XSIAM data exfiltration rules and rely solely on threat intelligence feeds for known exfiltration indicators.

Answer: C

Explanation:
Option B is the most effective strategy. It directly addresses the need for correlation by combining disparate event types (network, authentication, data access) to identify a sophisticated threat. Tuning thresholds ensures that the rule is specific enough to reduce false positives while catching true positives. Options A and E are too simplistic and likely to miss threats or generate more false positives. Option C is dangerous as it removes valuable baseline detections. Option D, while IJEBA is powerful, it often benefits from tuned correlation rules for specific, high-priority use cases.

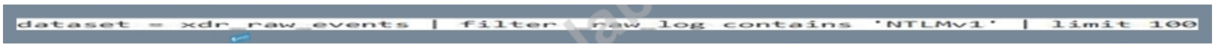
NEW QUESTION # 11
A large enterprise uses XSIAM for comprehensive security. They have a strict policy against the use of insecure authentication protocols like NTLMv1 , even for internal services. They want to create an ASM rule to detect any internal server or application

attempting to authenticate using NTLMv1. Given that XSIAM collects authentication logs from various sources (Active Directory, Linux authentication, network authentications), which of the following XQL approaches would be most effective for detecting NTLMv1 usage across their distributed environment?

- A. 

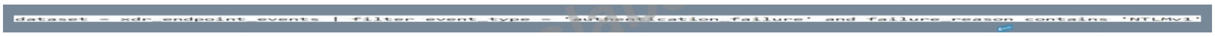
```
dataset = xdr_network_sessions | filter app_protocol = 'smb' and signature_name = 'smb_NTLMv1_Attempt'
```

- B.



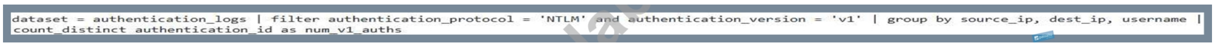
```
dataset = xdr_raw_events | filter raw_log contains 'NTLMv1' | limit 100
```

- C.



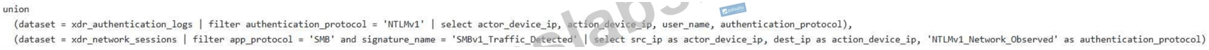
```
dataset = xdr_endpoint_events | filter event_type = 'authentication_failure' and failure_reason contains 'NTLMv1'
```

- D.



```
dataset = authentication_logs | filter authentication_protocol = 'NTLM' and authentication_version = 'v1' | group by source_ip, dest_ip, username |
count_distinct authentication_id as num_v1_auths
```

- E. Combine insights from 'xdr_authentication_logs' (for protocol details) and 'xdr_network_sessions' (for application protocol and potential deep packet inspection insights if available) to precisely identify NTLMv1. An example would be:



```
union
  (dataset = xdr_authentication_logs | filter authentication_protocol = 'NTLMv1' | select actor_device_ip, action_device_ip, user_name, authentication_protocol),
  (dataset = xdr_network_sessions | filter app_protocol = 'SMB' and signature_name = 'SMBv1_Traffic_Detected' | select src_ip as actor_device_ip, dest_ip as action_device_ip, 'NTLMv1_Network_Observed' as authentication_protocol)
```

Answer: E

Explanation:
Option E is the most comprehensive and effective approach for detecting NTLMv1 across a distributed environment in XSIAM. It leverages the 'union' operator to combine data from different relevant datasets. is ideal for explicit authentication protocol details, while can provide insights from network-level detections (like deep packet inspection signatures if available for NTLMv1 or related SMBv1 traffic, which often implies NTLMv1 usage). This multi-source correlation provides a more robust and complete picture. Option A is too broad and inefficient. Option B assumes a specific 'authentication_version' field, which might not be uniformly present across all authentication logs. Option C relies solely on a specific network signature, which might not always fire or be available for all NTLMv1 scenarios. Option D focuses only on failures and might miss successful NTLMv1 authentications.

NEW QUESTION # 12
What is the purpose of using rolling tokens to manage Cortex XDR agents?

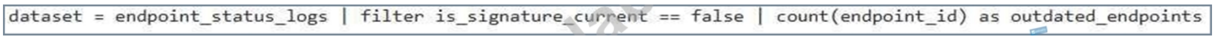
- A. To perform administration on agents without requiring static credentials
- B. To authorize agents to download and install content updates
  D To temporarily disable the agents during maintenance windows
- C. To periodically rotate encryption keys used for tenant communication

Answer: A

Explanation:
Rolling tokens in Cortex XDR are used to perform administration on agents without relying on static credentials. This improves security by providing time-limited, automatically rotating tokens that maintain agent management access without exposing long-lived credentials.

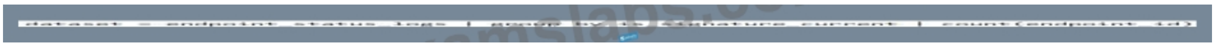
NEW QUESTION # 13
An XSIAM administrator is configuring a dashboard for endpoint security posture. A key metric is the 'Percentage of Endpoints with Outdated Antivirus Signatures'. The raw data in XSIAM's endpoint_status_logs includes a boolean field is_signature_current. Which XQL snippet would accurately represent this metric in a percentage format for a dashboard widget?

- A.



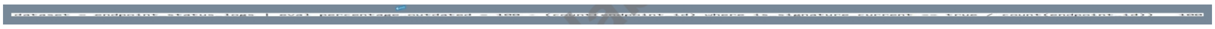
```
dataset = endpoint_status_logs | filter is_signature_current == false | count(endpoint_id) as outdated_endpoints
```

- B.



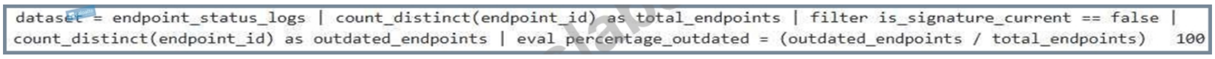
```
dataset = endpoint_status_logs | group by is_signature_current | count(endpoint_id)
```

- C.



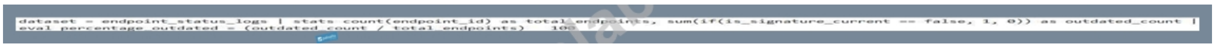
```
dataset = endpoint_status_logs | eval percentage_outdated = 100 - (count(endpoint_id) where is_signature_current == true / count(endpoint_id))   100
```

- D.



```
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
```

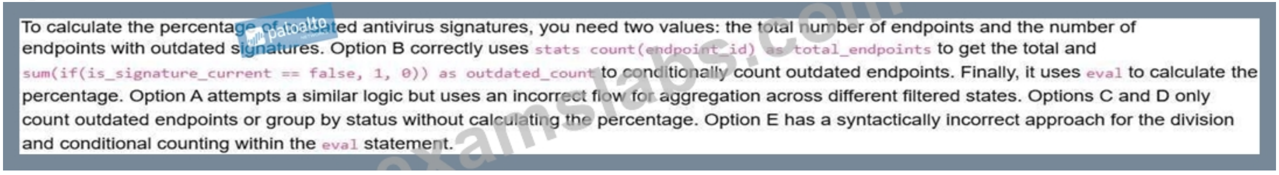
- E.



```
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 # 14

An organization is using XSIAM for its security operations. They have an on-premises network device that provides syslog data, but due to strict regulatory compliance, certain sensitive log fields (e.g., specific user IDs, internal IP subnets) must be obfuscated or redacted before the data leaves the on-premises network and reaches the XSIAM cloud. Simply dropping these fields is not enough; a specific masking format is required (e.g., replacing 'user_id_123' with 'user_id_XXXXX' and '192.168.1.5' with '192.168.1 .X'). Which XSIAM integration strategy, combined with an appropriate data manipulation technique, ensures this compliance requirement while maintaining data utility for other security analysis?

- A. Send all logs to a local SIEM first, which then performs the obfuscation. The SIEM then forwards the obfuscated logs to XSIAM. Issue: Adds complexity and cost of an unnecessary intermediate SIEM.
- B. Use XSIAM Playbooks to query the raw logs in the XSIAM Data Lake and then use 'Code' tasks to obfuscate sensitive fields in real-time before displaying them to analysts. Issue: Obfuscation happens post-ingestion, violating the pre-cloud requirement.
- C. Deploy an intermediate log forwarder (e.g., Splunk Universal Forwarder, Fluentd) on-premises. Configure this forwarder to receive syslog from the network device. Implement a pre-processing filter or a custom plugin within the forwarder to apply the required obfuscation/redaction using regular expressions or scripting before forwarding the modified logs to the XSIAM Data Broker. Issue: Adds an extra layer of management.
- D. Configure the network device to send syslog directly to an XSIAM Data Broker. XSIAM's custom data parsers will then apply regex-based obfuscation rules during ingestion in the cloud. Issue: Data is sent to the cloud before obfuscation.
- E. The network device itself should be configured to obfuscate the fields before sending syslog. If the device lacks this capability, this option is not viable. Issue: Assumes device capability which is often not present.

Answer: C

Explanation:
To ensure sensitive data is obfuscated before leaving the on-premises network and reaching the XSIAM cloud, an intermediate log forwarder deployed on-premises is the most suitable and common solution. Tools like Splunk Universal Forwarder or Fluentd (or even a custom Python script running as a service) can be configured to receive the raw syslog data. These forwarders have powerful pre-processing capabilities (e.g., regex-based transformations, custom plugins) to apply the required obfuscation/redaction rules to specific fields. Only the modified, compliant logs are then forwarded to the XSIAM Data Broker. While it adds an additional component to manage, it's the most reliable way to enforce data privacy at the source, adhering to strict regulatory requirements. Options A and E violate the 'before leaving the on-premises network' requirement. Option C relies on an often non-existent device capability. Option D adds unnecessary complexity and cost.

NEW QUESTION # 15

......

The XSIAM-Engineer study guide provided by the ExamsLabs is available, affordable, updated and of best quality to help you overcome difficulties in the actual test. We continue to update our dumps in accord with XSIAM-Engineer real exam by checking the updated information every day. The contents of XSIAM-Engineer Free Download Pdf will cover the 99% important points in your actual test. In case you fail on the first try of your exam with our XSIAM-Engineer free practice torrent, we will give you a full refund on your purchase.

Latest XSIAM-Engineer Version: https://www.examslabs.com/Palo-Alto-Networks/Security-Operations/best-XSIAM-Engineer-exam-dumps.html

- XSIAM-Engineer Test Tutorials □ XSIAM-Engineer Test Tutorials □ Latest XSIAM-Engineer Exam Materials □

Open website ➡ www.pdfdumps.com □□□ and search for ⇛ XSIAM-Engineer ⇚ for free download □XSIAM-Engineer Test Tutorials

- XSIAM-Engineer Certification Training □ Free XSIAM-Engineer Exam Questions □ Reliable XSIAM-Engineer Test Cost □ Open 《 www.pdfvce.com 》 and search for ▹ XSIAM-Engineer ◃ to download exam materials for free □ □XSIAM-Engineer Visual Cert Exam
- XSIAM-Engineer Test Torrent □ Search for ➥ XSIAM-Engineer □ on （ www.pdfdumps.com ） immediately to obtain a free download □New XSIAM-Engineer Mock Exam
- XSIAM-Engineer Valid Test Topics □ XSIAM-Engineer Actual Exam □ Exam XSIAM-Engineer Actual Tests □ Open website ➤ www.pdfvce.com □ and search for □ XSIAM-Engineer □ for free download □Best XSIAM-Engineer Study Material
- XSIAM-Engineer Test Torrent □ Immediately open ✔ www.troytecdumps.com □✔□ and search for 《 XSIAM-Engineer 》 to obtain a free download □XSIAM-Engineer Valid Test Topics
- Reliable XSIAM-Engineer Test Cost Ⓜ Reliable XSIAM-Engineer Test Cost □ XSIAM-Engineer Actual Exam □ Open website ➽ www.pdfvce.com □ and search for 「 XSIAM-Engineer 」 for free download □Best XSIAM-Engineer Study Material
- XSIAM-Engineer Valid Test Online □ XSIAM-Engineer Valid Test Online □ Exam XSIAM-Engineer Tutorials □ Open website { www.prepawaypdf.com } and search for ➡ XSIAM-Engineer □□□ for free download □Best XSIAM-Engineer Study Material
- Reliable XSIAM-Engineer Test Cost □ XSIAM-Engineer Valid Test Topics □ Free XSIAM-Engineer Exam Questions □ Copy URL 「 www.pdfvce.com 」 open and search for 《 XSIAM-Engineer 》 to download for free □XSIAM-Engineer Certification Training
- Valid XSIAM-Engineer Exam Questions □ Reliable XSIAM-Engineer Test Cost □ Exam XSIAM-Engineer Actual Tests □ Copy URL ☀ www.prep4sures.top □☀□ open and search for □ XSIAM-Engineer □ to download for free □ □XSIAM-Engineer Visual Cert Exam
- Reliable XSIAM-Engineer Dumps Book - Pass Guaranteed 2026 XSIAM-Engineer: Palo Alto Networks XSIAM Engineer First-grade Latest Version □ Search for ➤ XSIAM-Engineer □ and download exam materials for free through ▸ www.pdfvce.com ◂ □Exam XSIAM-Engineer Tutorials
- Quiz 2026 Palo Alto Networks XSIAM-Engineer – Trustable Reliable Dumps Book □ Open { www.prepawaypdf.com } enter ✔ XSIAM-Engineer □✔□ and obtain a free download □Reliable XSIAM-Engineer Test Cost
- hhi.instructure.com, www.stes.tyc.edu.tw, learning.bivanmedia.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, myskilluniversity.com, mpgimer.edu.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes