XSIAM-Engineer Test Pattern | Reliable Palo Alto Networks XSIAM-Engineer: Palo Alto Networks XSIAM Engineer

Crack the Palo Alto Networks XSIAM Engineer
Certification: Tools, Tips, and Training Insights

P.S. Free & New XSIAM-Engineer dumps are available on Google Drive shared by Lead1Pass: https://drive.google.com/open?id=1xhwN23PGSWd6pZbA3U5aipqR_4UeMIHQ

You can conveniently test your performance by checking your score each time you use our Palo Alto Networks XSIAM-Engineer practice exam software (desktop and web-based). It is heartening to announce that all Lead1Pass users will be allowed to capitalize on a free Palo Alto Networks XSIAM-Engineer Exam Questions demo of all three formats of Palo Alto Networks XSIAM-Engineer practice test.

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.

>> XSIAM-Engineer Test Pattern <<

Exam XSIAM-Engineer Duration & XSIAM-Engineer Reliable Exam Questions

The valid updated, and real Palo Alto Networks XSIAM-Engineer PDF questions and both practice test software are ready to download. Just take the best decision of your professional career and get registered in Palo Alto Networks XSIAM-Engineer certification exam and start this journey with Lead1Pass XSIAM-Engineer exam PDF dumps and practice test software. All types of Palo Alto Networks Exam Questions formats are available at the best price.It will enable you to perform well in the final XSIAM-Engineer Exam. Lead1Pass offers XSIAM-Engineer exam study material in the three best formats. Palo Alto Networks XSIAM-Engineer Exam Questions, Web-based and desktop practice exam software. All these formats play a vital role in your Palo Alto Networks XSIAM-Engineer exam preparation process.

Palo Alto Networks XSIAM Engineer Sample Questions (Q61-Q66):

NEW QUESTION # 61
A Cortex XSIAM engineer plans to add Kafka and Syslog Collectors to a Broker VM cluster.
What are two expected behaviors of the applets when they are added to the cluster? (Choose two.)

- A. Kafka Collector applet is automatically initiated, enters an active state on the primary node, and is on standby on the standby nodes.
- B. Kafka Collector applet is active on all cluster nodes, including primary and standby.
- C. Syslog Collector applet is active on all cluster nodes, including primary and standby.
- D. Syslog Collector applet is automatically initiated, enters an active state on the primary node, and is on standby on the standby nodes.

Answer: B,D

Explanation:
In a Broker VM cluster, the Syslog Collector applet runs in active/standby mode (active on the primary node, standby on others), while the Kafka Collector applet runs in active/active mode (active on all nodes). This design ensures both high availability and scalability for ingestion.

NEW QUESTION # 62
A security analyst is investigating a suspected lateral movement event within a corporate network. XSIAM has generated a high-fidelity alert based on a behavioral indicator of compromise (BIOC) rule. The alert details indicate an unusual process spawning activity followed by a successful SMB connection to a domain controller from a non-privileged workstation. The current BIOC rule for 'Lateral Movement via SMB' triggers on 'Process.CommandLine contains 'net use' AND Network.Protocol == 'SMB' AND Network.DestinationAddress in 'DomainControllersGroup''. This rule has a high false positive rate due to legitimate administrative activities. Which of the following modifications to the BIOC rule would most effectively reduce false positives while maintaining detection efficacy for malicious lateral movement attempts, considering the XSIAM context?

- A. Implement a new BIOC rule that correlates 'Process.Name == 'cmd.exe' OR Process.Name 'powershell.exe'' with 'Network.Protocol 'SMB' AND Network.DestinationAddress in 'DomainControllersGroup'' and a low-reputation 'Process.ParentProcess.ImageName'.
- B. Add an exclusion for 'User.IsInGroip('IT_Admins')' to the existing rule.
- C. Remove the 'Network.DestinationAddress in 'DomainControllersGroup'' condition to make the rule more general.
- D. Increase the severity of the existing rule and add a playbook action to automatically block the source IP address.
- E. Modify the rule to 'Process.CommandLine contains 'net use' AND Network.Protocol == 'SMB' AND Network.DestinationAddress in 'DomainControllersGroup' AND Process.ParentProcess.Name != 'explorer.exe''.

Answer: A

Explanation:
Option C offers the most effective approach. Simply excluding IT admins (A) might miss compromised admin accounts. Modifying parent process (B) is too restrictive and might still generate FPs. Increasing severity (D) doesn't address FPs. Removing the

destination address condition (E) would drastically increase FPs. Option C leverages behavioral correlation, looking for suspicious command execution (cmd.exe/powershell.exe) leading to SMB connections to sensitive assets, especially when initiated by a low-reputation parent process, which is a common pattern for lateral movement by attackers. This leverages XSIAM's ability to correlate diverse data sources for more accurate detection.

NEW QUESTION # 63

A large enterprise is migrating its legacy SIEM data into Palo Alto Networks XSIAM. The original SIEM data schema is highly denormalized, leading to redundant information and inefficient querying for threat hunting. To optimize content and improve query performance, a data normalization strategy is critical. Which of the following data modeling rules, when applied within XSIAM's content optimization framework, would be most effective in achieving Third Normal Form (3NF) for event data, specifically for a 'Login Event' dataset?

- A. Store all 'login_attempts' for a user within a nested array directly inside the 'user_profile' field to maintain contextual integrity.
- B. Create a separate lookup table for 'device_info' containing 'device_id', 'device_name', 'os_version', and 'device_owner', and link it to the main 'Login Event' table via 'device id'.
- C. Apply a rule to automatically normalize 'country_code' and 'city' from 'source_ip' using an external geo-IP database, storing them as separate attributes.
- D. Ensure that 'login_type' (e.g., 'SSO', 'Local', 'VPN') is directly dependent only on the 'event_id' and not on any other non-key attributes like 'source_ip'.
- E. Consolidate 'user_id', 'username', 'email', and 'department' into a single 'user_profile' field using a JSON object to minimize join operations.

Answer: B

Explanation:
To achieve 3NF, transitive dependencies must be eliminated. Option C directly addresses this by creating a separate table (or in XSIAM's context, a separate dataset or normalized entity) for device information. This ensures that 'device_name', 'os_version', and 'device_owner' are dependent on 'device_id' (a primary key in the 'device_info' entity) and not transitively dependent on the primary key of the 'Login Event' table via a non-key attribute. Option B describes 2NF, not strictly 3NF. Option A and D describe denormalization or semi-structured approaches that might be useful for performance in some NoSQL contexts but contradict the goal of 3NF for relational-like efficiency. Option E is about data enrichment, not normalization of existing schema attributes to higher forms.

NEW QUESTION # 64

Consider the following XSIAM correlation rule pseudo-code designed to detect a suspicious 'Golden Ticket' attack attempt, where an attacker might try to use a forged Kerberos ticket:

Based on a new threat intelligence report, a 'Golden Ticket' attack can now be executed without 'mimikatz.exe' and often involves a 'service ticket' request from a newly created user account. How should this XSIAM rule be optimized to align with the updated threat intelligence, while maintaining a low false positive rate?

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

Answer: A

Explanation:
Option A is the most effective and accurate optimization. The updated threat intelligence states that Mimikatz is not always present and new user accounts are involved, along with 'service_ticket' requests. Removing the Mimikatz correlation and adding a 'new_user_creation_log' correlation with an 'account_age' condition directly addresses these points. Adjusting the service_name to include 'service_ticket' broadens the initial detection phase to cover the new attack vector. Options B, C, D, and E either degrade the rule's effectiveness, introduce new false negatives, or are not directly relevant to the described threat intelligence update.

NEW QUESTION # 65

An advanced persistent threat (APT) group is suspected of targeting a high-value asset within an organization.
The security team wants to establish a real-time, bidirectional integration between XSIAM and their custom-built honeypot system to quickly identify and analyze APT activity.
The honeypot generates highly detailed JSON logs (e.g., attacker IP, commands executed, exploited vulnerabilities) and also offers an API to dynamically update honeypot configurations (e.g., block attacker IP, change honeypot persona).
Which XSIAM integration strategy would enable the most agile detection and response lifecycle, specifically for a high- fidelity, real-time threat scenario, including the code structure for a critical part of the integration?

- A. Honeypot logs are written to a local file, and an XSIAM Collector periodically ingests these files. An XSIAM Correlation Rule detects APT patterns. The response uses a 'Send Email' action to the honeypot admin. Code for API call is not directly applicable in XSIAM.
- B. The honeypot pushes JSON logs directly to an XSIAM Event Ingest API endpoint. An XSIAM Content Pack defines the data source and a custom 'Honeypot Incident' type. Upon ingestion, a real-time XSIAM Correlation Rule generates an incident. An XSIAM Playbook, triggered by this incident, contains a 'Code' task (Python script) to interact with the honeypot's API. This Python script should robustly handle API authentication, dynamic parameters, and error handling. For example, dynamically setting a block rule:
  □
- C. The honeypot sends SNMP traps for events to an XSIAM Broker. An XSIAM Playbook uses a 'Run Command' action to execute a shell script on an external server, which then updates the honeypot. Code for API call is external.
- D. XSIAM regularly pulls logs from the honeypot via SFTP. XSIAM then sends a notification to a third-party SOAR platform, which orchestrates the honeypot configuration updates. Code structure for XSIAM is limited to basic API calls.

Answer: B

Explanation:
For real-time, high-fidelity threat scenarios involving a custom honeypot, direct API integration with dynamic configuration capabilities is crucial. The honeypot pushing JSON logs directly to the XSIAM Event Ingest API endpoint ensures low-latency ingestion. A custom XSIAM Content Pack and Correlation Rule properly categorize and trigger incidents. The most agile response is achieved by an XSIAM Playbook utilizing a 'Code' task (Python script). This allows for highly customized API interactions, including dynamic parameter passing (e.g., the attacker IP from the incident) and robust error handling. The provided code snippet demonstrates fetching incident data, extracting the attacker IP, constructing an API payload, and making a POST request, which is exactly what's needed for dynamic honeypot updates. This approach minimizes external dependencies and keeps the automation within XSIAM for better management and auditing. Option A's generic 'Call API' might lack the flexibility and error handling of a 'Code' task for complex scenarios.

NEW QUESTION # 66

......

We provide our candidates with valid XSIAM-Engineer vce dumps and the most reliable pass guide for the certification exam. Our IT professionals written the latest XSIAM-Engineer test questions based on the requirement of the certification center, as well as the study materials and test content. By using our online training, you may rest assured that you grasp the key points of XSIAM-Engineer Dumps Torrent for the practice test.

Exam XSIAM-Engineer Duration: https://www.lead1pass.com/Palo-Alto-Networks/XSIAM-Engineer-practice-exam-dumps.html

Engineer Braindumps Files

- XSIAM-Engineer Exam Book □ XSIAM-Engineer Valid Exam Labs □ XSIAM-Engineer Updated Dumps □ Search for ➡ XSIAM-Engineer □□□ and easily obtain a free download on □ www.pdfvce.com □ □XSIAM-Engineer Valid Exam Labs
- XSIAM-Engineer Free Updates □ XSIAM-Engineer Reliable Test Materials ☮ Learning XSIAM-Engineer Materials □ Open website 《 www.examcollectionpass.com 》 and search for （ XSIAM-Engineer ） for free download □Exam Dumps XSIAM-Engineer Demo
- Exam Dumps XSIAM-Engineer Demo □ XSIAM-Engineer Updated Dumps □ Learning XSIAM-Engineer Materials □ □ Search for ☀ XSIAM-Engineer □☀□ and download it for free on □ www.pdfvce.com □ website □Exam XSIAM-Engineer Testking
- Palo Alto Networks XSIAM Engineer Exam Dumps Get Success With Minimal Effort □ The page for free download of “ XSIAM-Engineer ” on □ www.easy4engine.com □ will open immediately □XSIAM-Engineer Actual Braindumps
- XSIAM-Engineer Free Updates □ Learning XSIAM-Engineer Materials □ XSIAM-Engineer Reliable Test Materials □ ➥ www.pdfvce.com □ is best website to obtain 【 XSIAM-Engineer 】 for free download □XSIAM-Engineer Actual Braindumps
- XSIAM-Engineer Exam Book □ XSIAM-Engineer 100% Correct Answers □ Learning XSIAM-Engineer Materials □ □ Search for ▶ XSIAM-Engineer ◀ and download it for free on ➠ www.prepawaypdf.com □ website □XSIAM-Engineer Exam Book
- www.stes.tyc.edu.tw, www.hulkshare.com, www.stes.tyc.edu.tw, myportal.utt.edu.tt, 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, Disposable vapes

BTW, DOWNLOAD part of Lead1Pass XSIAM-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1xhwN23PGSWd6pZbA3U5aipqR_4UeMIHQ