Palo Alto Networks - XSIAM-Engineer Accurate Valid Test Review

BONUS!!! Download part of SurePassExams XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1hJvvyNtCDvoKGO8yezSAI-xeYiHmyQZ_

Only if you download our software and practice no more than 30 hours will you attend your test confidently. Because our XSIAM-Engineer exam torrent can simulate limited-timed examination and online error correcting, it just takes less time and energy for you to prepare the XSIAM-Engineer exam than other study materials. As is known to us, maybe you are a worker who is busy in your career. Therefore, purchasing the XSIAM-Engineer Guide Torrent is the best and wisest choice for you to prepare your test. If you buy our XSIAM-Engineer questions torrent, the day of regretting will not come anymore.

Palo Alto Networks XSIAM-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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.

>> Valid XSIAM-Engineer Test Review <<

High-Quality Valid XSIAM-Engineer Test Review & Fast Download Test XSIAM-Engineer Answers: Palo Alto Networks XSIAM Engineer

In the current market, there are too many products of the same type. It is actually very difficult to select the XSIAM-Engineer practice prep that you love the most with only product introduction. Our trial version of our XSIAM-Engineer Study Materials can be a good solution to this problem. For the trial versions are the free demos which are a small of the XSIAM-Engineer exam questions, they are totally free for our customers to download.

Palo Alto Networks XSIAM Engineer Sample Questions (Q385-Q390):

NEW QUESTION # 385
Which common issue can result in sudden data ingestion loss for a data source that was previously successful?

- A. Data source has reached its end of life for support.
- B. API key used for the integration has expired.
- C. Data source is using an unsupported data format.
- D. Data source has reached its maximum storage capacity.

Answer: B

Explanation:
A sudden data ingestion loss for a previously successful data source commonly occurs when the API key used for the integration has expired, breaking authentication and preventing further log collection.

NEW QUESTION # 386
An XSIAM deployment project is stalled due to an inability to obtain the necessary API keys and access credentials for a critical SaaS application (e.g., Salesforce, Workday) required for XSIAM's Identity & Access Management (IAM) module. The SaaS vendor has strict security policies requiring complex multi-factor authentication (MFA) and IP whitelisting for API access. What is the most practical and secure approach for the XSIAM team to obtain and manage these credentials for continuous data ingestion?

- A. Request a dedicated service account from the SaaS vendor with minimal privileges, use an API key from this account, and store it directly in the XSIAM connector configuration with encryption at rest.
- B. Utilize a secrets management solution (e.g., HashiCorp Vault, AWS Secrets Manager) to dynamically fetch and inject credentials into the XSIAM connector, minimizing exposure of sensitive data.
- C. Work with the IT security team to establish a secure network tunnel (e.g., IPSec VPN) from the XSIAM environment's egress IP to the SaaS vendor's API gateway, and then provide a service account API key.
- D. Manually generate API tokens for the SaaS application on a daily basis and update the XSIAM connector configuration each time to comply with token expiration policies.
- E. Implement an Identity Provider (IdP) integration with the SaaS application if available, and use OAuth 2.0 or OpenID Connect for token-based authentication, leveraging XSIAM's support for modern authentication.

Answer: B,E

Explanation:
Both B and E represent best practices for secure credential management with SaaS applications. Option B (IdP/OAuth) is ideal if supported by the SaaS application, as it provides a robust, token-based, and often MFA-aware authentication mechanism without storing static credentials in XSIAM. Option E (secrets management solution) is crucial for securely storing and distributing sensitive credentials like API keys, ensuring they are not hardcoded or exposed and can be rotated automatically. Option A is a basic approach but less secure than E. Option C is impractical and prone to errors. Option D addresses network access but not credential management itself.

NEW QUESTION # 387
An XSIAM Engineer observes that after a recent application update, security events from a critical business application are no longer triggering expected XSIAM correlation rules. Upon investigation, it's discovered that while the logs are being ingested, the '_time' field in XSIAM for these specific logs is consistently showing the ingestion time (e.g., now()), rather than the actual event timestamp present in the raw log, which is in ISO 8601 format (e.g., '2023-10-27 T 14:35:10.1237). The raw log field containing the timestamp is named 'eventTime'. What is the most likely cause and the precise XSIAM parsing rule configuration adjustment needed?

- A. The application update changed the timestamp format, and the XSIAM parsing rule's 'time_format' or 'time_field' setting is no longer correctly configured to extract and parse 'eventTime' as the primary timestamp for the event. The XSIAM parsing rule needs to explicitly set 'time_field: eventTime' and specify the correct 'time_format: IS08601 or a suitable 'strptime' pattern.
- B. The XSIAM license has expired, leading to partial data processing and timestamp issues. This would cause broader ingestion failures, not specific timestamp re-writes.
- C. The 'eventTime' field is being dropped during normalization because it's not mapped to a standard CIM field. This doesn't explain '_time' defaulting to ingestion time.
- D. The XSIAM Data Lake is experiencing high latency, causing delays in '_time' field indexing. This affects query performance, not the source of the '_time' value.
- E. The XSIAM Collector's internal clock is out of sync with the application server. Synchronize the NTP on the Collector. This would affect all logs, not just specific ones.

Answer: A

Explanation:
The '_time' field in XSIAM is crucial for correlation and accurate event timing. If it defaults to ingestion time, it means XSIAM's parser could not identify or correctly parse the actual event timestamp from the raw log. Option A correctly identifies that the 'time_field' and 'time_format settings in the parsing rule are responsible for this. An application update changing the log format is a common reason for such a failure. Options B, D, and E are general issues not specific to this problem. Option C would lead to the field being missing, not '_time' being incorrect.

NEW QUESTION # 388
Which action is required to enable use of a custom script in an alert layout?

- A. Tag the script with "dynamic-section," add a general purpose dynamic section, and edit the section settings to add the automation script.
- B. Tag the script with "general-purpose-dynamic-section," add a custom script section, and edit the section settings to add the automation script.
- C. Tag the script with "general-purpose-dynamic-section." add a general purpose dynamic section, and edit the section settings to add the automation script.
- D. Add a general purpose dynamic section and edit the section settings to add the automation script.

Answer: C

Explanation:
To use a custom script in an alert layout, the script must be tagged with "general-purpose-dynamic-section", then a general purpose dynamic section is added to the layout, and finally the section settings are edited to attach the automation script. This ensures the script executes and displays results dynamically within the alert layout.

NEW QUESTION # 389
A global enterprise has implemented Palo Alto Networks XSIAM for its security operations. They are concerned about lateral movement within their Kubernetes clusters and want to establish an ASM rule to detect 'Pod Escapes' or suspicious activities indicative of a container compromise leading to host-level access. Assume XSIAM ingests container runtime events and host-level process data'. Which combination of XQL data sources and logic would be most effective for this complex detection?

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

Answer: E

Explanation:
Option B is the most effective for detecting 'Pod Escapes' or container-to-host compromise. It directly looks for suspicious commands often used in container escapes ('nsenter', 'docker' commands like 'chroot' or 'mount /dev') in 'xdr_process_eventS at the host level. The 'inner join' with filtering for 'container_privileged = true' ensures that this suspicious activity is correlated with potentially vulnerable privileged containers, providing strong evidence of a potential escape. Option A is too generic network-wise.

Option C is a general host compromise indicator, not specific to container escape. Option D is valid Kubernetes audit, but 'kubectl exec' into a pod isn't a pod escape itself. Option E is a specific example of an attacker action after escape, but Option B covers the escape mechanism more broadly and correlates with privileged containers.

NEW QUESTION # 390

.....

Our supporter of XSIAM-Engineer study guide has exceeded tens of thousands around the world, which directly reflects the quality of them. Because the exam may put a heavy burden on your shoulder while our XSIAM-Engineer practice materials can relieve you of those troubles with time passing by. Just spent some time regularly on our XSIAM-Engineer Exam simulation, your possibility of getting it will be improved greatly. For your information, the passing rate of our XSIAM-Engineer training engine is over 98% up to now.