Latest XSIAM-Engineer Exam Torrent - XSIAM-Engineer Test Prep & XSIAM-Engineer Quiz Torrent

BONUS!!! Download part of PassExamDumps XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1Kc4yUFF5LBYoxZ3KhRCBS0s_vikIYDmg

Even though our XSIAM-Engineer training materials have received quick sale all around the world, in order to help as many candidates for the exam as possible to pass the exam and get the related certification at their first try, we still keep the most favorable price for our best XSIAM-Engineer test prep. In addition, if you keep a close eye on our website you will find that we will provide discount in some important festivals, we can assure you that you can use the least amount of money to buy the best product in here. We aim at providing the best XSIAM-Engineer Exam Engine for our customers and at trying our best to get your satisfaction.

Palo Alto Networks XSIAM-Engineer Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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 4	• 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.

>> XSIAM-Engineer Exam Topic <<

Trustable XSIAM-Engineer Exam Topic bring you Authorized Reliable XSIAM-Engineer Exam Guide for Palo Alto Networks Palo Alto Networks XSIAM Engineer

After our practice materials were released ten years ago, they have been popular since then and never lose the position of number one in this area. Our XSIAM-Engineer practice quiz has authority as the most professional exam material unlike some short-lived XSIAM-Engineer Exam Materials. Targeting exam candidates of the exam, we have helped over tens of thousands of exam candidates achieved success now. So you can be successful by make up your mind of our XSIAM-Engineer training guide.

Palo Alto Networks XSIAM Engineer Sample Questions (Q183-Q188):

NEW QUESTION # 183
An XSIAM engineer is troubleshooting a scenario where endpoint-based threat detections are occurring, but the correlated network flow data in XSIAM for those specific endpoints is incomplete or missing, hindering comprehensive investigation. The organization uses Palo Alto Networks NGFWs and Cortex XDR agents. Which of the following potential root causes and corresponding troubleshooting steps should the engineer investigate, and why?

- A. Root Cause: The NGFW is not configured to send traffic logs to the correct XSIAM ingestion profile. Troubleshooting: Verify NGFW log forwarding profiles and ensure the appropriate log types (e.g., Traffic, Threat) are being sent to the XSIAM collector/data lake.
- B. Root Cause: The XSIAM Broker VM responsible for NGFW log ingestion is offline or experiencing resource exhaustion. Troubleshooting: Check the Broker VM's status and resource utilization in the XSIAM console, and restart or scale up if necessary.
- C. Root Cause: The Cortex XDR agents are configured in 'Forensics Only' mode, which doesn't send real-time network connection data. Troubleshooting: Change the XDR agent profile to 'Full Protection' or 'Standard' mode to ensure continuous network telemetry is collected.
- D. Root Cause: XSIAM's data retention policy for network flow data is shorter than for endpoint data, causing older flow data to be purged. Troubleshooting: Review and adjust the data retention settings for network flow data in XSIAM to match investigation requirements.
- E. Root Cause: The endpoints in question are bypassing the NGFW (e.g., direct internet access, VPN exclusion). Troubleshooting: Review network architecture and firewall policies to ensure all relevant endpoint traffic is inspected by the NGFW and logs are generated.

Answer: A,B,C,D,E

Explanation:
This is a complex troubleshooting scenario involving multiple potential points of failure, which requires a systematic approach. All listed options are plausible root causes and valid troubleshooting steps: A. Root Cause: NGFW Log Forwarding (Correct): This is a primary suspect. If the NGFW isn't configured to send its traffic logs (which contain network flow data) to XSIAM, then XSIAM won't have the data. Troubleshooting involves verifying the NGFW's log forwarding profiles. B. Root Cause: Cortex XDR Agent Configuration (Incorrect): While the XDR agent does collect network connection data, the question specifically refers to 'network flow data' (implying NGFW/network device logs) correlated with endpoint detections. If XDR detections are occurring, the agent is sending some telemetry. The agent mode affects endpoint-level network visibility, but wouldn't explain missing NGFW network flow data . C. Root Cause: Broker VM Issues (Correct): If NGFW logs are forwarded via a Broker VM (common for on-premise deployments), then an issue with the Broker VM (offline, resource exhaustion) would directly impact log ingestion. Checking its status and resources is crucial. D. Root Cause: Network Bypass (Correct): If endpoint traffic doesn't pass through the NGFW, the NGFW won't generate logs for that traffic, resulting in missing network flow data in XSIAM. This points to a network architecture or policy misconfiguration. E. Root Cause: Data Retention Policy (Correct): XSIAM has configurable data retention. If network flow data has a shorter retention period than endpoint data, older investigations will find correlated network data missing because it has been purged. Adjusting retention is the solution.

NEW QUESTION # 184

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

Answer: C

NEW QUESTION # 185

Consider the following scenario: A Broker VM has been successfully deployed and registered with Cortex XSIAM. However, an analyst notices that logs from a specific Windows server, configured to send Sysmon events via a Winlogbeat forwarder, are not appearing in Cortex XSIAM. Other log sources connected to the same Broker VM are successfully sending data'. Which of the following is the most logical first step in troubleshooting this issue on the Broker VM?

- A. Log in to the Broker VM via SSH and check the status of the 'data-collector' service and its logs.
- B. Review the Cortex XSIAM 'Collector Health' dashboard for any alerts related to the specific Broker VM or data source.
- C. Inspect the Winlogbeat configuration file on the Windows server to confirm the correct Broker VM IP address and port.
- D. Verify the 'data-collector-profiles' configuration on the Broker VM via the XSIAM console to ensure a profile exists for Winlogbeat.
- E. Check the Broker VM's network interface statistics for incoming traffic on the port Winlogbeat is configured to send to.

Answer: A,C

Explanation:
If other log sources are working, the issue is specific to the Winlogbeat source. The most logical first steps are to confirm the source configuration on the Winlogbeat server (C) to ensure it's pointing correctly to the Broker VM. If that's correct, then checking the 'data-collector' service status and its logs on the Broker VM itself (E) is crucial to see if it's receiving, processing, or encountering errors with Winlogbeat data. Checking network interface statistics (A) is a good general step but less targeted than checking the service logs. Verifying data-collector-profiles (B) is important, but if other logs are flowing, the core service is likely running. The Collector Health dashboard (D) is a good overall health check but might not pinpoint a single specific data source issue as effectively as the Broker VM's local logs.

NEW QUESTION # 186

An organization is deploying XSIAM and needs to integrate with a custom internal application that generates critical audit logs in a proprietary JSON format, accessible via an authenticated REST API. The API only allows fetching data in chunks based on a timestamp range. The XSIAM team wants to ensure continuous and complete ingestion of these logs. Describe the essential components and logic required for a robust XSIAM integration for this scenario, including any specific XSIAM features that would be leveraged.

- A. Use a standard syslog forwarder to send the raw JSON data to XSIAM, relying on XSIAM's auto-parsing capabilities for JSON.
- B. Manually export the JSON logs from the application daily, compress them, and upload them via the XSIAM UI for batch ingestion.
- C. Configure the application to directly send JSON data to a generic HTTP Event Collector endpoint in XSIAM without any intermediary logic or parsing.
- D. Set up an AWS Lambda function that periodically invokes the application's API, converts the JSON to a simple CSV, and pushes it to an S3 bucket for XSIAM to collect.
- E. Deploy a dedicated XSIAM Data Collector configured with a custom parser to interpret the JSON. The Data Collector will need a 'stateful' pulling mechanism using an execution script to manage API calls, timestamp tracking, and error handling, pushing the parsed JSON to XSIAM's ingestion API.

Answer: E

Explanation:
Option A provides the most robust and complete solution. A dedicated XSIAM Data Collector is needed to establish connectivity and process the data. The 'stateful pulling mechanism' with an execution script is crucial for managing the timestamp-based API calls, ensuring no data loss and handling pagination/errors. A custom parser within XSIAM (or pre-processing in the script) is required for the proprietary JSON. Option B is unlikely to handle authenticated REST APIs and timestamp-based fetching. Option C is manual and not continuous. Option D introduces unnecessary AWS components. Option E implies the application can directly push, and doesn't address the timestamp-based pulling or proprietary format without pre-processing.

NEW QUESTION # 187

Your SOC is implementing a new 'Threat Hunting' workflow within XSIAM. For each 'Threat Hunting Result' incident type, analysts need to quickly see: 1) the XQL query that led to the finding, 2) the number of hits for that query, and 3) the top 5 affected assets identified by the query. This data needs to be presented concisely in the incident's summary. You also want to provide a clickable link to re-run the full XQL query directly from the incident. Which of the following content optimization features are essential to achieve this, and why?

- A. A custom incident layout for 'Threat Hunting Result' incidents, incorporating a custom field for the XQL query string. Use a 'Link Renderer' to make the query string clickable. For hits and top assets, leverage 'Data Transformers' on other custom fields that execute dynamic XQL sub-queries against the raw logs to derive these values, and then 'Table Renderers' or 'List Renderers' to display the top 5 assets.
- B. Storing all threat hunting queries in an external document and manually pasting results into XSIAM.
- C. Disabling the default incident summary and forcing analysts to review all raw logs.
- D. Creating an XSIAM dashboard specific to threat hunting that shows query results.
- E. Utilizing basic custom text fields for all information and relying on manual data entry.

Answer: A

Explanation:
To present the XQL query, hit count, top assets, and a clickable link to re-run the query concisely in the 'Threat Hunting Result' incident summary, the most comprehensive solution involves a combination of advanced XSIAM content optimization features. A custom incident layout specific to this type is crucial. For the query string and its re-run link, a custom field with a 'Link Renderer' is ideal. For dynamically calculating the number of hits and identifying the top 5 affected assets, 'Data Transformers' that execute XQL sub-queries are necessary. Finally, 'Table Renderers' or 'List Renderers' are vital for displaying the top assets in a structured, readable format. This integrates all required elements directly into the incident view, optimizing the hunting workflow. Options B, C, D, and E are either manual, lack dynamic capabilities, or do not provide the integrated experience within the incident summary.

NEW QUESTION # 188

......

- XSIAM-Engineer Exam Guide □ Verified XSIAM-Engineer Answers □ Latest XSIAM-Engineer Braindumps Sheet □ □ Search for 《 XSIAM-Engineer 》 and easily obtain a free download on ☀ www.examcollectionpass.com □☀□ □ □Verified XSIAM-Engineer Answers
- Reliable XSIAM-Engineer Learning Materials □ Valid XSIAM-Engineer Exam Cram □ Latest XSIAM-Engineer Braindumps Sheet □ ➥ www.pdfvce.com □ is best website to obtain ☀ XSIAM-Engineer □☀□ for free download □ □Valid XSIAM-Engineer Exam Cram
- New XSIAM-Engineer Test Sample □ XSIAM-Engineer Exam Guide □ New XSIAM-Engineer Practice Questions □ Open website □ www.exam4labs.com □ and search for 《 XSIAM-Engineer 》 for free download □Latest XSIAM-Engineer Braindumps Sheet
- 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, www.boostskillup.com, wjhsd.instructure.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, wjhsd.instructure.com, dorahacks.io, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

BTW, DOWNLOAD part of PassExamDumps XSIAM-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1Kc4yUFF5LBYoxZ3KhRCBS0s_vikIYDmg