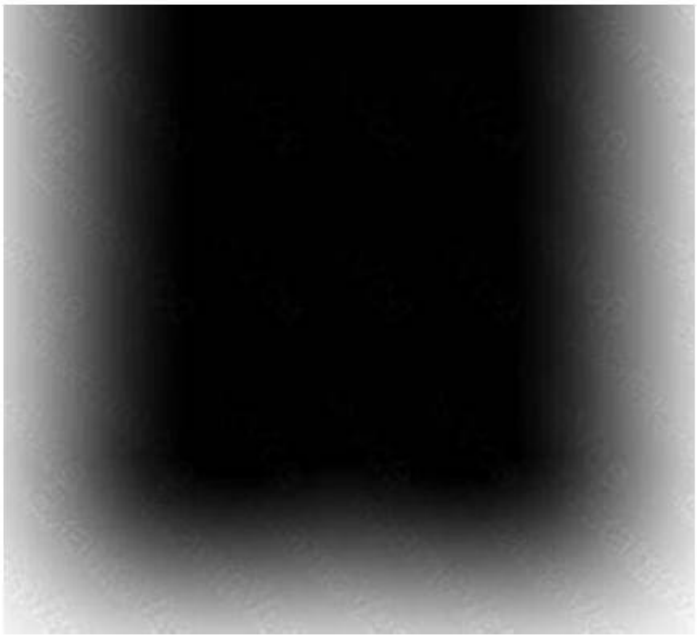
Dumps Palo Alto Networks XSIAM-Engineer Vce - XSIAM-Engineer Latest Study Materials



BTW, DOWNLOAD part of TestsDumps XSIAM-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=14j5kBkqnkgOOhLmRV56FxYEwsxYuWYMr

This version of the software is extremely useful. It may necessitate product license validation, but it does not necessitate an internet connection. If you have any issues, the TestsDumps is only an email away, and they will be happy to help you with any issues you may be having! This desktop XSIAM-Engineer practice test software is compatible with Windows computers. This makes studying for your test more convenient, as you can use your computer to track your progress with each Palo Alto Networks XSIAM-Engineer Mock Test. The software is also constantly updated, so you can be confident that you're using the most up-to-date version.

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 Latest Study Materials - Valid XSIAM-Engineer Exam Materials

This way you will be able to experience the actual Palo Alto Networks XSIAM Engineer exam environment and become a more prepared and confident candidate to step into the examination center. You will know where exactly you stand before the actual Palo Alto Networks XSIAM-Engineer Certification Exam. The actual Palo Alto Networks XSIAM-Engineer exam questions will make you familiar with the inside-out view of the exam pattern and syllabus.

Palo Alto Networks XSIAM Engineer Sample Questions (Q65-Q70):

NEW QUESTION # 65
Consider an XSIAM Engine deployed in a VMware ESXi environment. The Engine consistently shows high CPU utilization, even during periods of low data ingestion, and its data processing rate is lower than expected. The underlying ESXi host has ample physical CPU resources. Which of the following virtualization-specific optimizations and checks should be performed to diagnose and resolve this performance bottleneck?

- A. Migrate the XSIAM Engine VM to a different ESXi host within the same cluster without any further diagnostics, assuming the issue is host-specific.
- B. Configure a vCPU 'hot add' feature on the XSIAM Engine VM, as this resolves all performance issues.
- C. Verify that the ESXi host's CPU power management policy is set to 'High Performance' and check for CPU Ready Time (esxtop: %RDY) and Co-stop (%CSTP) metrics on the VM. Also, ensure CPU affinity settings are not restricting the VM.
- D. Increase the number of vCPUs assigned to the XSIAM Engine VM without considering CPU ready time or co-stop.
- E. Reduce the allocated RAM to the XSIAM Engine VM to free up resources for other VMS on the host.

Answer: C

Explanation:
High CPU utilization with low actual processing in a virtualized environment often points to CPU contention or misconfiguration at the hypervisor level. Option B correctly identifies critical virtualization metrics and settings. 'CPU Ready Time' (%RDY) indicates how long a VM is ready to run but waiting for CPU resources, while 'Co-stop' (%CSTP) shows the delay experienced by a multi-vCPU VM because not all vCPUs are available simultaneously. A 'High Performance' power policy prevents the hypervisor from throttling CPU frequencies. CPU affinity settings, if configured incorrectly, can restrict the VM to a subset of physical cores, leading to resource starvation. Option A can worsen the problem if contention is already present. Option C is a shot in the dark without diagnostics. Option D will negatively impact performance. Option E is incorrect; hot-add is a feature, not a performance panacea, and doesn't address underlying contention.

NEW QUESTION # 66
A Security Operations Center (SOC) using Palo Alto Networks XSIAM has implemented a new set of detection rules. After initial deployment, they observe a high volume of low-fidelity alerts for legitimate administrative activities, leading to alert fatigue. Which of the following content optimization strategies involving scoring rules would be most effective in mitigating this issue without completely suppressing valuable security alerts?

- A. Configure all alerts to automatically be suppressed for 24 hours after their initial generation.
- B. Create a new scoring rule that assigns a lower reputation score to alerts originating from known, whitelisted administrative IPs or specific service accounts when associated with 'successful login' events, effectively reducing their overall criticality.
- C. Increase the severity score of all newly generated alerts across the board to ensure critical events are prioritized.
- D. Modify the global alert threshold in XSIAM to only show alerts with a score above 90, ignoring all others.
- E. Disable all detection rules that are generating excessive alerts, regardless of their potential security value.

Answer: B

Explanation:
Option B is the most effective content optimization strategy. By using scoring rules to assign lower reputation scores to known benign activities (e.g., successful logins from whitelisted administrative IPs), the overall criticality of these alerts is reduced. This helps in de-prioritizing noise without completely suppressing the underlying detection rules, allowing the SOC to focus on higher-fidelity threats. Option A would exacerbate alert fatigue. Option C would lead to significant blind spots. Option D is a temporary band-aid and could hide legitimate threats. Option E is too blunt and would likely miss important alerts below the arbitrary threshold.

NEW QUESTION # 67
A company is planning to integrate XSIAM with its highly customized CMDB, which runs on a legacy database system without a modern API. The CMDB contains critical asset metadata (e.g., owner, criticality, patching status) that XSIAM needs for accurate alert context and prioritization. Given the constraints, what is the most effective and maintainable integration strategy?

- A. Manually update XSIAM lookup lists with CMDB data on a daily basis.
- B. Develop a custom ETL process that periodically extracts data from the legacy CMDB, transforms it, and loads it into a format ingestible by a XSIAM Data Collector (e.g., JSON, CSV over SFTP).
- C. Require the CMDB vendor to develop a modern API for XSIAM integration.
- D. Implement direct database connectivity from a XSIAM Data Collector to the legacy CMDB, ensuring proper firewall rules and credentials.
- E. Use a generic syslog forwarder to send raw database logs to XSIAM.

Answer: B

Explanation:
Given a legacy CMDB without a modern API, a custom ETL process (Option A) is the most effective and maintainable solution. It allows for data transformation, error handling, and provides a controlled ingestion pipeline into XSIAM without direct database exposure from XSIAM. Option B, direct database connectivity, is generally not recommended due to security and performance implications. Option C is unrealistic for an immediate deployment. Option D is manual and not scalable. Option E would send raw database logs, which is not suitable for enriching XSIAM alerts with structured CMDB data.

NEW QUESTION # 68
A critical XSIAM Broker VM is deployed in a hardened environment with strict outbound proxy requirements, including certificate inspection. After a Broker VM firmware update, the VM loses its ability to connect to the XSIAM cloud, and the XSIAM console reports 'Broker VM Offline'. The network team confirms proxy reachability. Analysis of the Broker VM's system logs reveals TLS handshake errors related to untrusted certificates. Which of the following is the most probable cause, and what configuration element on the Broker VM likely requires immediate attention?

- A. The proxy authentication credentials stored on the Broker VM were cleared during the update. Reconfigure the proxy username and password.
- B. The Broker VM's network interface configuration was reset, causing it to lose its default gateway. Reconfigure the network settings.
- C. The Broker VM's internal clock (NTP) is out of sync, causing certificate validation failures due to time discrepancies. Resynchronize NTP on the Broker VM.
- D. The XSIAM cloud-side certificate has expired, and all Broker VMS are affected. This requires Palo Alto Networks intervention.
- E. The Broker VM firmware update overwrote or corrupted the custom trusted CA certificates required to trust the proxy's inspection certificate. The proxy's root CA certificate needs to be re-imported into the Broker VM's trust store.

Answer: E

Explanation:
The key indicators are 'TLS handshake errors related to untrusted certificates' and the context of a 'hardened environment with strict outbound proxy requirements, including certificate inspection.' In such environments, the proxy often performs SSL/TLS decryption and re- encryption, presenting its own certificate to the Broker VM. For the Broker VM to trust this proxy-generated certificate, the proxy's root CA certificate must be imported into the Broker VM's trusted certificate store. A firmware update can sometimes reset or affect these custom configurations. Options A, C, and D are less direct fits for the specific error message. Option E would affect all Broker VMs, not just one after an update.

NEW QUESTION # 69
A security operations center (SOC) team wants to integrate their existing XDR solution (not XSIAM) with XSIAM to leverage XSIAM's advanced analytics and automation capabilities for threat hunting and incident response. The XDR solution can export security alerts and raw logs in JSON and CEF formats via REST APIs or syslog. Which XSIAM components and integration strategies are best suited for comprehensive data ingestion and automated threat response, considering the need for both structured alerts and unstructured log data?

- A. Configure the XDR solution to forward all data via syslog to an XSIAM Broker, and then use XSIAM's out-of-the-box XDR parsers. Automation would be driven by XSIAM's Correlation Rules.
- B. Develop custom XSIAM content packs with data source integrations that pull data via the XDR's REST APIs (for both JSON alerts and raw logs). Leverage XSIAM Playbooks for automated response and XSIAM Engines for data enrichment.
- C. Use an XSIAM Broker to collect all XDR data via SFTP transfer of CSV files, and then use XSIAM's search capabilities for manual threat hunting. Automation is not feasible with this approach.
- D. Integrate the XDR solution with a third-party message queue (e.g., Kafka), then configure XSIAM to consume messages from the queue. Use XSIAM's Alerting Engine to trigger automated actions.
- E. Utilize the XSIAM Data Lake Ingest API for JSON alerts and CEF for raw logs, and configure XSIAM playbooks to trigger on new data ingested, using XSIAM's native XDR integration module.

Answer: B

Explanation:
Developing custom XSIAM content packs with data source integrations that leverage the XDR's REST APIs provides the most flexibility and richness for both structured alerts (often available via APIs) and raw logs. This allows for precise control over data mapping and normalization. XSIAM Playbooks are the core for automated response, and XSIAM Engines can perform real-time data enrichment. While syslog is an option, APIs offer more control and context. XSIAM's native XDR integration module might not exist for every XDR, and relying solely on out-of-the-box parsers might miss crucial context.

NEW QUESTION # 70
.....

If you are still a student, you must have learned from the schoolmaster how difficult it is to go out to work now. If you have already taken part in the work, you must have felt deeply the pressure of competition in society. XSIAM-Engineer exam materials can help you stand out in the fierce competition. After using our XSIAM-Engineer Study Materials, you have a greater chance of passing the XSIAM-Engineercertification, which will greatly increase your soft power and better show your strength.

Easily obtain free download of □ XSIAM-Engineer □ by searching on □ www.pdfvce.com □ □Reliable XSIAM-Engineer Exam Camp

- Authoritative XSIAM-Engineer – 100% Free Dumps Vce | XSIAM-Engineer Latest Study Materials □ Download ➤ XSIAM-Engineer □ for free by simply entering 「 www.dumpsquestion.com 」 website □XSIAM-Engineer Book Pdf
- XSIAM-Engineer Real Question □ XSIAM-Engineer Exam Certification □ Test XSIAM-Engineer Practice □ Open 《 www.pdfvce.com 》 and search for ▹ XSIAM-Engineer ◃ to download exam materials for free □XSIAM-Engineer Valid Test Sample
- 100% Pass Reliable Palo Alto Networks - XSIAM-Engineer - Dumps Palo Alto Networks XSIAM Engineer Vce □ Open website ⇛ www.testkingpass.com ⇚ and search for □ XSIAM-Engineer □ for free download □Questions XSIAM-Engineer Exam
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, academy.frenchrealm.com, www.stes.tyc.edu.tw, pct.edu.pk, app.parler.com, 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.stes.tyc.edu.tw, peopleoffaithbiblecollege.org, 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, Disposable vapes

BTW, DOWNLOAD part of TestsDumps XSIAM-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=14j5kBkqnkgOOhLmRV56FxYEwsxYuWYMr