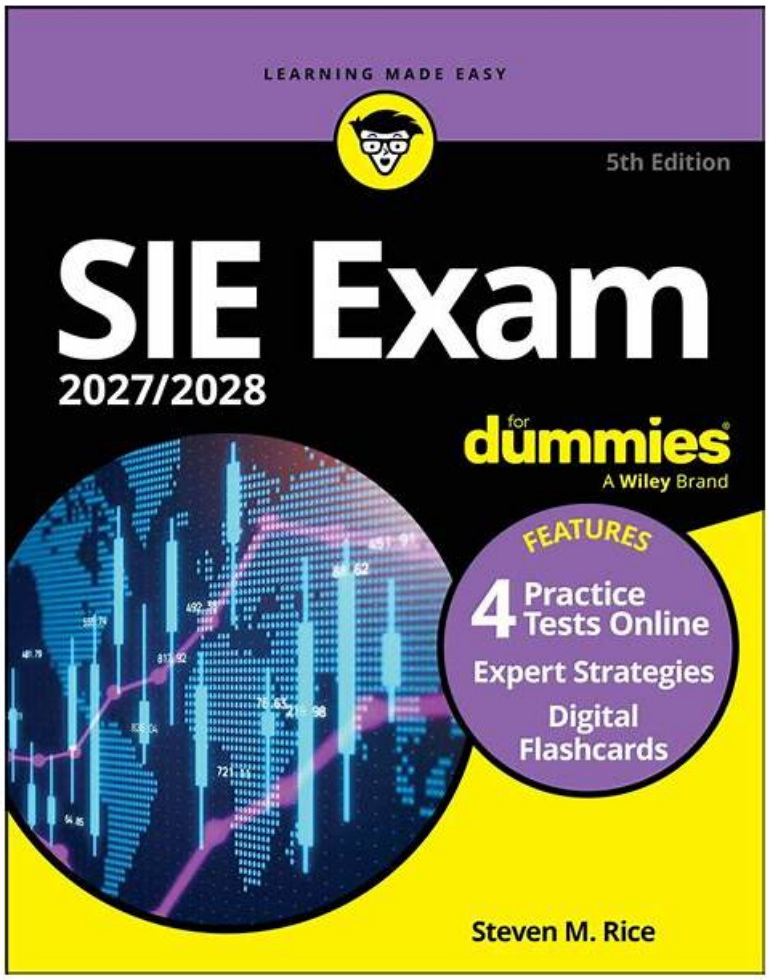
XSIAM-Engineer Exam Pass Guide | XSIAM-Engineer Actual Test Answers



DOWNLOAD the newest PrepAwayETE XSIAM-Engineer PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1tJ8EOmCQBXz8_E_WgX5j9MfPUfH_CKHp

Our XSIAM-Engineer test materials boost three versions and they include the PDF version, PC version and the APP online version. The clients can use any electronic equipment on it. If only the users' equipment can link with the internet they can use their equipment to learn our XSIAM-Engineer qualification test guide. They can use their cellphones, laptops and tablet computers to learn our XSIAM-Engineer Study Materials. The language is also refined to simplify the large amount of information. So the learners have no obstacles to learn our XSIAM-Engineer certification guide.

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	• 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	• 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.

XSIAM-Engineer Actual Test Answers, Reliable XSIAM-Engineer Study Notes

If you want to know our XSIAM-Engineer exam questions before your coming exam, you can just visit our website. And it is easy and convenient to free download the demos of our XSIAM-Engineer study guide, you just need to click on it. Then you wil find that all points of the XSIAM-Engineer Learning Materials are predominantly related with the exam ahead of you. Every page is full of well-turned words for your reference related wholly with the XSIAM-Engineer training prep.

Palo Alto Networks XSIAM Engineer Sample Questions (Q71-Q76):

NEW QUESTION # 71
During a routine audit of XSIAM's alert management, a new custom detection rule, 'Suspicious Process Creation by Admin', has been observed generating excessive alerts from a specific server used for automated patch deployment. This server's legitimate activities involve frequent process creations by an administrative account. The XSIAM team wants to reduce this noise without entirely disabling the valuable rule. Which two (2) configurations are valid and effective methods to address this within XSIAM's exception and exclusion capabilities?

- A. Implement a 'Global Exception' for all events originating from 'host.hostname =
- B. Integrate with a CMDB to dynamically tag as a 'Known_Baseline' host, and then configure the rule to ignore 'Known_BaseIine' hosts.
- C. Modify the rule to lower its threshold for the specific server's process creation events.
- D. Create a new 'Exclusion' for the 'Suspicious_Process_Creation_by_Admirf rule, filtering events where 'host.hostname = AND process.parent.name = 'patch_deployer.exe' .
- E. Set up an 'Alert Suppression Rule' in 'Alert Management' that matches 'alert_name = AND 'host.hostname = , with an action to 'Do Not Create Alert'.

Answer: D,E

Explanation:
Both B and C are valid and effective. Option B, creating an 'Exclusion' directly within the rule, prevents the alert from being generated at the source based on specific event criteria, which is a very clean approach for known false positives. Option C, an 'Alert Suppression Rule' with 'Do Not Create Alert' action, achieves a similar outcome by intercepting the alert before it's officially created in XSIAM. Both prevent alert generation. Option A is not a standard XSIAM feature for rule tuning based on host. Option D is too broad and creates a significant security blind spot. Option E is a good long-term strategy for managing baselines but isn't a direct exception/exclusion configuration for immediate noise reduction; it requires additional integration and rule modification.

NEW QUESTION # 72
An organization is migrating from a legacy EDR solution to Cortex XSIAM. During the planning phase, it's determined that several thousand endpoints are running older operating systems (e.g., Windows Server 2012 R2, CentOS 7) that are still critical but reaching end-of-life. What is the most significant consideration regarding XSIAM agent compatibility and support for these systems, and what strategic recommendation should the engineer provide?

- A. The XSIAM agent uses a universal kernel module compatible with all Linux kernel versions, making OS version irrelevant for Linux endpoints. Windows Server 2012 R2 is fully supported without limitations.
- B. Older OS versions might require a specific, older XSIAM agent build that lacks full feature parity or continuous updates. Recommend a phased OS upgrade plan concurrent with XSIAM deployment.
- C. The XSIAM agent automatically updates to support older OS versions indefinitely. No special consideration is needed; simply deploy the latest agent.
- D. XSIAM agents are not supported on any OS older than Windows 10 or RHEL 8. These systems cannot be protected by XSIAM and must be excluded from the deployment scope.
- E. Performance will be significantly degraded on older OS versions, but the agent will function. Recommend increasing RAM and CPU on these servers to compensate.

Answer: B

Explanation:
Option B is the most accurate. While Cortex XSIAM generally supports a wide range of OS versions, older operating systems, especially those approaching or past their end-of-life (like Windows Server 2012 R2 and CentOS 7), typically have limited or deprecated support. This often means they can only run specific, older agent versions that might not receive the latest features, bug fixes, or security updates. Continuous support for such legacy systems is not guaranteed, and eventually, support will cease. Therefore, the strategic recommendation must be to plan for OS upgrades or retirement of these systems in conjunction with the XSIAM deployment to ensure comprehensive and future-proof security coverage. Option A is incorrect; agent support has lifecycles. Option C is too extreme; some older versions are supported, albeit with limitations. Option D focuses on performance only, not the underlying support issue. Option E is incorrect; kernel modules are OS and kernel version specific, and Windows Server 2012 R2 has explicit support lifecycles.

NEW QUESTION # 73
An XSIAM engineer needs to create a custom content pack that includes a new integration for a proprietary internal vulnerability scanner. This integration will define several commands, one of which is `get_scan_results`, which accepts a `scan_id` and returns a JSON object containing scan findings. Another command, `trigger_scan`, initiates a scan and returns a `scan_id`. Which of the following components are absolutely essential for defining and making these commands usable within XSIAM playbooks, and what consideration is crucial for `get_scan_results`?

- An Integration YAML file, a Python script implementing the commands, and a Mapper for `trigger_scan` output.
  Crucial consideration for `get_scan_results`: Ensure the output JSON schema is strictly adhered to for XSIAM's UI rendering.
- An Integration YAML file, a Python script implementing the commands, and a Parser for `get_scan_results`.
  Crucial consideration for `get_scan_results`: Implement polling logic within the command if the vulnerability scanner's API is asynchronous.
- An Automation Rule, a Playbook that calls the commands, and a Dashboard Widget to display results.
  Crucial consideration for `get_scan_results`: Optimize API calls to prevent rate limiting on the scanner.
- A Data Connector for continuous ingestion of scan results, and Correlation Rules to identify vulnerabilities.
  Crucial consideration for `get_scan_results`: Define specific data types for all returned fields in the XSIAM schema.
- Only a Python script with the commands is sufficient; XSIAM automatically detects and registers them.
  Crucial consideration for `get_scan_results`: Manage pagination if the scan results are large.

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

Answer: E

Explanation:

To define custom integrations and their commands in XSIAM, you absolutely need an Integration YAML file (which describes the integration, its parameters, and the commands it supports) and a Python script that implements the actual logic for each command. A Parser is essential for `get_scan_results` to transform the raw JSON output from the vulnerability scanner into structured XSIAM data (e.g., incidents, artifacts, or indicators) that can be easily consumed by playbooks, search, and the UI. Crucially, for `get_scan_results`, if `trigger_scan` is asynchronous (which is common for long-running scans), the `get_scan_results` command's implementation in the Python script must often include polling logic . This means it repeatedly queries the scanner's API for the status of the scan using the `scan_id` until the results are ready, or a timeout is reached. This is a common design pattern for integrating with asynchronous external systems. Options A, C, D, E miss these fundamental requirements or considerations.

NEW QUESTION # 74
Your XSIAM deployment is integrated with an external vulnerability management system. A recent scan has identified several legitimate, but unpatched, internal web servers that are generating 'Web Application Vulnerability Detected' alerts from an XSIAM Correlation Rule. Due to business constraints, these servers cannot be patched immediately. You need to create an exclusion that dynamically adapts to new web server deployments within a specific subnet (172.16.10.0/24) while still alerting on any other web application vulnerabilities outside this specific, known-vulnerable context. Which XSIAM exclusion configuration snippet, applied to the 'Web Application Vulnerability Detected' rule, would achieve this? Assume and are relevant fields.

```
alert_name: 'Web Application Vulnerability Detected'
exclusion_filters:
  - 'dest_ip IN 172.16.10.0/24'
  - 'alert_description CONTAINS "Known Unpatched Vulnerability"'
match_all: 'true'
```

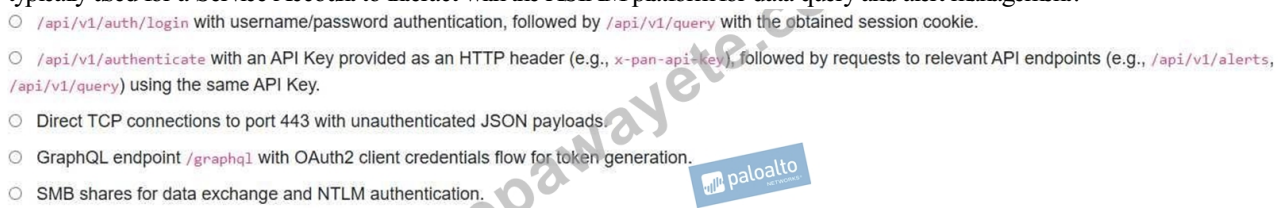
- A.
```
scope: 'rule'
rule_id: 'CORR-WEB-001'
exclusion_condition:
  - field: 'dest_ip'
    operator: 'in_subnet'
    value: '172.16.10.0/24'
suppression_action: 'Drop'
valid_until: 'never'
```
- B.
- C.
```
exclusion_type: 'AlertSuppression'
query: 'alert_name="Web Application Vulnerability Detected" AND dest_ip IN ("172.16.10.0/24")'
expiration: 'none'
severity_change: 'Informational'
```
- D.
```
exclusion:
  rule_filter: 'detection_rule_id = "your_rule_id_here"'
  event_filter: 'dest_ip IN CIDR("172.16.10.0/24") AND alert_description CONTAINS "Known Unpatched Vulnerability"'
  enabled: true
```
- E.
```
rule_name: 'Web Application Vulnerability Detected'
exclusion_condition:
  - field: 'dest_ip'
    operator: 'in_subnet'
    value: '172.16.10.0/24'
  - field: 'alert_description'
    operator: 'contains'
    value: 'Known Unpatched Vulnerability'
logical_operator: 'AND'
```

Answer: D

Explanation:
Option D accurately reflects the likely structure and fields for creating an exclusion in XSIAM that targets a specific detection rule and applies conditions to the events themselves Cevent_filter'). The use of for subnet matching and 'CONTAINS' for text matching within the 'event_filter' is crucial for dynamically excluding all servers in that subnet with a specific vulnerability description, without

requiring manual updates for new servers. This ensures the rule is still active for other vulnerabilities or IPs. Options A and C use non-standard or generic exclusion syntax. Option B lacks the specific alert description condition, making it too broad. Option E is more akin to a general suppression rule rather than a direct rule exclusion and modifies severity, which is not the primary goal.

NEW QUESTION # 75
During the planning phase for an XSIAM deployment, an organization decides to utilize a Service Account for programmatic access to the XSIAM API for custom integrations and automation. Which of the following API endpoints and authentication methods are typically used for a Service Account to interact with the XSIAM platform for data query and alert management?



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

Answer: E

Explanation:
Palo Alto Networks XSIAM primarily uses API Keys for programmatic access via Service Accounts. The API Key is a long-lived credential passed in an HTTP header (commonly 'x-pan-api-key' or 'Authorization: Bearer '). This allows direct authentication for subsequent API calls to various endpoints for querying data, managing alerts, and other operations. Option A describes user-based authentication. Options C, D, and E are incorrect for XSIAM API interaction.

NEW QUESTION # 76
.....

Nowadays the competition in the job market is fiercer than any time in the past. If you want to find a good job， you must own good competences and skillful major knowledge. So owning the XSIAM-Engineer certification is necessary for you because we will provide the best study materials to you. Our XSIAM-Engineer exam torrent is of high quality and efficient, and it can help you pass the test successfully. The product we provide with you is compiled by professionals elaborately and boosts varied versions which aimed to help you learn the XSIAM-Engineer Study Materials by the method which is convenient for you. They check the update every day, and we can guarantee that you can get a free update service from the date of purchase.

- XSIAM-Engineer New Test Bootcamp □ Vce XSIAM-Engineer Exam □ XSIAM-Engineer Official Cert Guide □ ✔ www.vceengine.com □✔□ is best website to obtain ▸ XSIAM-Engineer ◂ for free download □XSIAM-Engineer Latest Torrent
- 100% Pass Quiz 2026 Newest Palo Alto Networks XSIAM-Engineer: Palo Alto Networks XSIAM Engineer Exam Pass Guide □ Download ➽ XSIAM-Engineer □ for free by simply searching on ➡ www.pdfvce.com □□□ □Testking XSIAM-Engineer Learning Materials
- Detail XSIAM-Engineer Explanation □ XSIAM-Engineer Exam Tutorial □ XSIAM-Engineer Official Cert Guide ◴ Go to website ➽ www.pdfdumps.com □ open and search for ▹ XSIAM-Engineer ◃ to download for free □Testking XSIAM-Engineer Learning Materials
- Free PDF 2026 XSIAM-Engineer: Authoritative Palo Alto Networks XSIAM Engineer Exam Pass Guide □ Download ➡ XSIAM-Engineer □□□ for free by simply searching on { www.pdfvce.com } □Test XSIAM-Engineer Sample Questions
- Valid Braindumps XSIAM-Engineer Ppt □ XSIAM-Engineer Exam Tutorial □ Valid XSIAM-Engineer Exam Pattern □ □ The page for free download of " XSIAM-Engineer " on ➥ www.vce4dumps.com □ will open immediately □Pdf XSIAM-Engineer Pass Leader
- bookmarkassist.com, adamclbf911430.blgwiki.com, majaiwns969782.wikibyby.com, trackbookmark.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, qasimoprs338175.wikiexcerpt.com, gerardgfcl591512.blogdun.com, haimacpwv144788.wikiparticularization.com, owainfvrl250692.lotrlegendswiki.com, allennxsy111715.blog4youth.com, Disposable vapes

BONUS!!! Download part of PrepAwayETE XSIAM-Engineer dumps for free: https://drive.google.com/open?id=1tJ8EOmCQBXz8_E_WgX5j9MfPUfH_CKHp