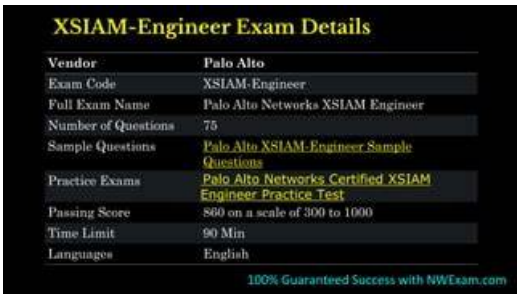
XSIAM-Engineer Fragen&Antworten, XSIAM-Engineer Quizfragen Und Antworten



Laden Sie die neuesten ZertPruefung XSIAM-Engineer PDF-Versionen von Prüfungsfragen kostenlos von Google Drive herunter: https://drive.google.com/open?id=1mD4IxReUa7RZ5pJh1xAWhHDK08lezh6Q

Die Konkurrenz in der IT-Branche wird immer heftiger. Wie können Sie sich beweisen, dass Sie wichig und unerlässlich ist? Die Zertifizierung der Palo Alto Networks XSIAM-Engineer zu erwerben macht es überzeugend. Was wir für Sie tun können ist, dass Ihnen helfen, die Palo Alto Networks XSIAM-Engineer Prüfung mit höhere Effizienz und weniger Mühen zu bestehen. Mit langjährigen Entwicklung besitzt jetzt ZertPruefung große Menge von Ressourcen und Erfahrungen. Immer verbesserte Software gibt Ihnen bessere Vorbereitungsphase der Palo Alto Networks XSIAM-Engineer Prüfung.

Palo Alto Networks XSIAM-Engineer Prüfungsplan:

Thema	Einzelheiten
Thema 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.
Thema 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.
Thema 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.
Thema 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 Fragen&Antworten <<

XSIAM-Engineer Quizfragen Und Antworten, XSIAM-Engineer Deutsch Prüfungsfragen

Wofür zögern Sie noch? Sie haben nur eine Chance. Jetzt können Sie die vollständige Version zur Palo Alto Networks XSIAM-Engineer Zertifizierungsprüfung bekommen. Sobald Sie die ZertPruefung klicken, wird Ihr kleiner Traum verwirklicht werden. Sie haben die besten Schulungsunterlagen zur Palo Alto Networks XSIAM-Engineer Zertifizierungsprüfung gekriegen. Benutzen Sie beruhigt unsere Palo Alto Networks XSIAM-Engineer Prüfungsfragen und Antworten, werden Sie sicher die Palo Alto Networks XSIAM-Engineer Prüfung bestehen.

Palo Alto Networks XSIAM Engineer XSIAM-Engineer Prüfungsfragen mit Lösungen (Q93-Q98):

93. Frage
An engineer modifies a production playbook before deploying the updated version. What is the recommended best practice?

- A. Reinstall all Content Packs.
- B. Restart all Cortex XSIAM agents.
- C. Test the playbook in a non-production environment.
- D. Delete existing incidents.

Antwort: C

Begründung:
Testing updated playbooks in a non-production environment verifies functionality before deployment. This reduces operational risk, prevents unintended automation behavior, and helps ensure reliable execution in production.

94. Frage
A complex XSIAM automation playbook is being developed for advanced threat hunting, which involves querying multiple external threat intelligence sources (MISP, VirusTotal, Mandiant Advantage) and then aggregating and normalizing their responses. The normalization process for each source is unique and computationally intensive. The resulting aggregated data needs to be pushed back into XSIAM's Data Lake as a new custom event type for further analysis. Which XSIAM automation components would be crucial for efficient execution and data handling?

- A. XSIAM Dashboards for real-time visualization and XQL queries for data extraction.
- B. XSIAM 'Pre-processing Rules' for initial data filtering and 'Post-processing Rules' for final data enrichment.
- C. XSIAM 'Fetch Incident' and 'Update Incident' actions for managing data.
- D. Only built-in XSIAM threat intel feeds are supported for direct integration; external sources require manual upload.
- E. XSIAM 'Custom Integrations' to connect to each external TIP, 'Transform' steps for normalization, and 'Ingest' actions to push data to the Data Lake.

Antwort: E

Begründung:
For complex integrations with multiple external sources, 'Custom Integrations' are essential for connecting to each TIP's API. 'Transform' steps within the playbook are critical for normalizing the diverse responses from each source into a consistent format. Finally, 'Ingest' actions (or 'Send Event' actions) are used to push the aggregated and normalized data into XSIAM's Data Lake as a new custom event type, making it available for XQL queries and further analysis. Options A, B, C are either for visualization/querying, incident management, or general rule processing, not directly for complex multi-source data ingestion and normalization from external APIs. Option E is incorrect, as XSIAM is highly extensible.

95. Frage
Which two alert notification options can be configured without creating a playbook? (Choose two.)

- A. Slack
- B. SMS
- C. Email
- D. Pager Duty

Antwort: A,C

Begründung:
Cortex XSIAM allows configuring Email and Slack as direct alert notification options without requiring a playbook. PagerDuty and

SMS integrations, however, require orchestration through playbooks.

96. Frage
Consider a large enterprise that uses XSIAM and also has a sophisticated internal messaging platform (like an enterprise-grade Slack or Teams equivalent) for SOC communication. The security team wants to automate the process of notifying relevant stakeholders in specific messaging channels when critical XSIAM incidents are created or updated, including incident details and a direct link to the XSIAM incident. Additionally, they want to allow certain actions (e.g., 'Acknowledge Incident', 'Quarantine Host') to be triggered directly from the messaging platform, feeding back into XSIAM. Which combination of XSIAM features and integration techniques is required to achieve this bidirectional, interactive messaging integration, and what are the security implications?

- A. Outbound: Develop a custom XSIAM content pack that includes a messaging integration, leveraging the internal platform's REST API for sending formatted messages. Inbound: Configure the messaging platform's interactive components (e.g., buttons, slash commands) to send HTTP POST requests to a custom XSIAM 'Ingest API' endpoint, triggering a playbook. The playbook would validate the request, extract parameters, and call the XSIAM Incident Management API. Security implication: Requires secure exposure of an XSIAM API endpoint (e.g., behind an API Gateway with authentication), robust input validation within the playbook, and careful management of API tokens for both platforms.
- B. Outbound: Use a generic XSIAM notification template to send emails to a messaging platform's email-to-channel gateway. Inbound: Rely on human operators to manually translate messaging platform actions into XSIAM commands. Security implication: Limited automation, relies heavily on manual intervention, less interactive.
- C. Outbound: Manually copy-paste XSIAM incident details into the messaging platform. Inbound: Manually update XSIAM incidents based on discussions in the messaging platform. Security implication: High risk of human error and data inconsistency, minimal security benefit.
- D. Outbound: Configure XSIAM to export incident data to a shared network drive, and a script periodically reads this and posts to the messaging platform. Inbound: Configure the messaging platform to dump chat logs to a SIEM, and the SIEM forwards to XSIAM for analysis. Security implication: Introduces significant latency, potential for data leakage on shared drive, and complex log parsing.
- E. Outbound: XSIAM Playbooks triggered by incident creation/updates using an 'Outgoing Webhook' action to send messages to the internal platform's API endpoint. Inbound: Configure the messaging platform to send messages to XSIAM's email ingestion service, then use XSIAM playbooks to parse the email and update incidents based on keywords. Security implication: Requires careful handling of API keys for the messaging platform within XSIAM and ensuring XSIAM's email ingestion service is robust.

Antwort: A

Begründung:
For robust, interactive, bidirectional messaging integration, the best approach involves direct API interaction. Outbound notifications from XSIAM are best handled by custom content packs leveraging the messaging platform's REST API for rich message formatting. For inbound actions, the messaging platform's interactive components (e.g., buttons) should be configured to send HTTP POST requests to a secure XSIAM 'Ingest API' endpoint. This endpoint would trigger a playbook that validates the request (e.g., signature verification, IP whitelisting), extracts the desired action and incident ID, and then uses XSIAM's Incident Management API to perform the requested action. Security implications are paramount: securely exposing an XSIAM endpoint, implementing strong authentication (e.g., API keys, OAuth tokens) and authorization, and robust input validation in the playbook are critical to prevent unauthorized actions or injection attacks. API token management for both platforms must be handled securely (e.g., XSIAM Vault).

97. Frage
You are debugging an XSOAR integration script that interacts with an external Security Information and Event Management (SIEM) system. The script uses the 'requests' library to make API calls. You suspect a 'SSL/TLS handshake failure' due to certificate issues, but the integration's logs are not verbose enough to show the full certificate chain validation details. How can you most effectively gather more detailed SSL/TLS debugging information within the XSOAR script environment?

- A. Temporarily set 'verify=False' in the 'requests.get()' or 'requests.post()' calls to bypass SSL validation and confirm if it's an SSL issue.
- B. Add at the beginning of the Python script to enable debug logging for the 'requests' library.
- C. Use 'openssl s_client -connect : -showcertS from the XSOAR engine's command line to manually check the certificate.
- D. Modify the XSOAR engine's Docker container settings to increase log verbosity for network connections.
- E. Set the environment variable 'REQUESTS CA BUNDLE' to a specific CA bundle file path within the XSOAR integration configuration.

Antwort: B

Begründung:
To get more detailed SSL/TLS debugging information within the script's execution context , enabling debug logging for the 'requests library is the most direct and effective method. (B) will output verbose details about the HTTP requests, including the SSL handshake process, to the XSOAR integration's log. Option D can help confirm if it's an SSL issue, but doesn't provide detailed debugging. A requires modifying the engine's environment, which is less ideal for quick script debugging. C is for specifying a CA bundle, not for debugging verbosity. E is an external manual check, not integrated into the script's logging.

98. Frage
.....

ZertPruefung stehen Ihnen eine Abkürzung zum Erfolg zur Verfügung. Dabei erspart ZertPruefung Ihnen viel Zeit und Energie. ZertPruefung wird Ihnen gute Fragenpool zur Palo Alto Networks XSIAM-Engineer Zertifizierungsprüfung bieten und Ihnen helfen , die Palo Alto Networks XSIAM-Engineer Zertifizierungsprüfung zu bestehen. Wenn Sie auch die relevante Materialien auf anderen Websites sehen, schauen Sie mal weiterhin, dann werden Sie finden, dass diese Materialien eigentlich aus ZertPruefung stammen. Unsere ZertPruefung bieten die umfassendste Information und aktualisieren am schnellsten.