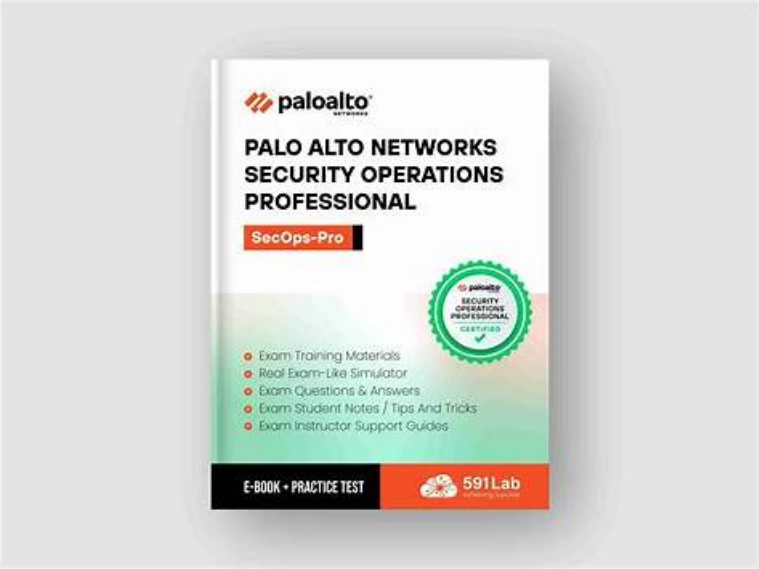
Pass Guaranteed Palo Alto Networks - SecOps-Pro - Accurate Palo Alto Networks Security Operations Professional Exam Duration



2026 Latest Actual4test SecOps-Pro PDF Dumps and SecOps-Pro Exam Engine Free Share: https://drive.google.com/open?id=1Gx_D2X_MGTPOm9fGpTwWt-vgVsll0oSS

There are many benefits both personally and professionally to having the SecOps-Pro test certification. Higher salaries and extended career path options. The Palo Alto Networks SecOps-Pro test certification will make big difference in your life. Now, you may find the fast and efficiency way to get your SecOps-Pro exam certification. Do not be afraid, the Palo Alto Networks SecOps-Pro will give you helps and directions. SecOps-Pro questions & answers almost cover all the important points which will be occurred in the actual test. You just need to take little time to study and prepare, and passing the SecOps-Pro actual test will be a little case.

Palo Alto Networks SecOps-Pro Exam Syllabus Topics:

Section	Weight	Objectives
Detection and Analysis	30%	- Endpoint and Network Forensics - Log Analysis (XSIAM/Prisma) - Malware Triage
Reporting and Metrics	20%	- SOC Performance Metrics - Dashboard Customization - Incident Reporting
XSOAR Automation and Orchestration	30%	- Integration Management - Playbook Development - Incident Classification and Severity
Security Operations Foundations	20%	- SOC Roles and Responsibilities - Threat Intelligence Frameworks - Incident Response Lifecycle

>> SecOps-Pro Exam Duration <<

SecOps-Pro New APP Simulations - SecOps-Pro Test Study Guide

You can absolutely assure about the high quality of our products, because the contents of SecOps-Pro training materials have not only been recognized by hundreds of industry experts, but also provides you with high-quality after-sales service. Before purchasing

SecOps-Pro exam torrent, you can log in to our website for free download. During your installation, SecOps-Pro exam questions hired dedicated experts to provide you with free remote online guidance. During your studies, SecOps-Pro Exam Torrent also provides you with free online services for 24 hours, regardless of where and when you are, as long as an email, we will solve all the problems for you. At the same time, if you fail to pass the exam after you have purchased SecOps-Pro training materials, you just need to submit your transcript to our customer service staff and you will receive a full refund.

Palo Alto Networks Security Operations Professional Sample Questions (Q20-Q25):

NEW QUESTION # 20
Which operational responsibility is a role of a security operations center (SOC) manager?

- A. Collecting raw security data and managing the initial confirmation of alerts
- B. Performing technical analysis and threat hunting for major incidents
- C. Developing and implementing necessary crisis communication plans
- D. Monitoring the service health of all data sources sending telemetry

Answer: C

Explanation:
A SOC manager is responsible for overseeing operations, including coordinating incident response at a strategic level and ensuring proper communication during crises, which includes developing and implementing crisis communication plans.

NEW QUESTION # 21
Which solution will minimize mean time to resolution (MTTR) when, as a result of previous malware infection, a company's Windows endpoint is suffering a small amount of file corruption and modified registry keys?

- A. Use Live Terminal to connect to the machine and upload files to replace the corrupted files.
- B. Use group policy objects to push new files and registry key changes to the endpoint.
- C. Use remediation suggestions to restore the affected files and registry modifications.
- D. Issue a new laptop from the help desk to expedite a clean system.

Answer: C

Explanation:
Cortex XDR includes a powerful feature designed specifically to reduce MTTR (Mean Time to Resolution) after a security incident: Remediation Suggestions .
* Automated Rollback: When Cortex XDR analyzes an incident, it identifies every change the malicious process made-including files created, registry keys modified, and processes spawned.
* Efficiency: Instead of manual rebuilding (Option A) or manual scripting (Option B), the analyst can simply review the "Remediation Suggestions" in the Incident view and click "Apply." This automatically deletes malicious files and restores registry keys to their original state.
* Speed: This is the fastest way to return a system to its "Known Good" state without the overhead of hardware replacement or complex GPO deployments (Option C).

NEW QUESTION # 22
A sophisticated ransomware attack has breached your network. Your Cortex XSIAM deployment generated an incident for 'Ransomware Activity' on several endpoints. During the investigation, you observe encrypted files with a new extension and a ransom note. You also find suspicious PowerShell activity attempting to disable security features. To enhance your immediate response and create a high-fidelity 'incident response' rule, you need to enrich the incident details by automatically adding relevant threat intelligence, and more aggressively alert on this specific ransomware variant across your entire infrastructure. Which combination of Cortex XSIAM features, XQL, and incident enrichment capabilities would best achieve this, including automating a response action? (Select all that apply)

- A. From the existing 'Ransomware Activity' incident, use the 'Action Center' to 'Add Indicators' (e.g., file hash of the ransom note, the new extension, C2 domains found in logs). Configure an 'Automation Rule' in XSIAM that triggers on new 'Ransomware Activity' incidents, enriches the incident with external Threat Intelligence via an integration (e.g., VirusTotal lookup for file hashes), and initiates a 'Containment' playbook to isolate affected endpoints and block C2 communication at

the firewall.

- B. Develop a new 'Correlation Rule' that links: 1) File modification events for known sensitive directories with a new, unknown extension. 2) Process creation of 'powershell.exe' with 'Disable-MpProtection' arguments. 3) Network connections to suspicious, high-entropy domains. The XQL would involve multiple 'join' statements. Set the rule to 'Critical' and trigger a 'Security Playbook' to collect forensic data and notify the incident response team.
- C. Create a 'Custom Widget' on the Dashboard displaying file modification events with the new extension. Then, manually export logs related to PowerShell activity and network connections to an external SIEM for correlation. This approach will provide a visual overview and external correlation.
- D. Utilize the 'Indicator' page in XSIAM to add the new ransomware file extension (e.g., '.locked') and the ransom note file name (e.g., 'HOW_TO_DECRYPT.txt') as 'Custom Indicators'. Set their severity to 'Critical' and configure an 'Automated Response' action to isolate any host where these indicators are observed.
- E. Create a new 'Detection Rule' of type 'Behavioral' with the following XQL:

```
dataset = xdr_data | filter event_type = 'file' and (action_file_extension = 'new_ransom_ext' or file_name = 'ransom_note.txt') or (event_type =
'process' and action_process_image_name = 'powershell.exe' and command_line contains 'Disable-MpProtection') | group count() by host_name |
where count() > 1
```

Answer: A,B

Explanation:
Options C and D are the most effective and aligned with advanced Cortex XSIAM capabilities for immediate response and high-fidelity incident handling. Option C: This leverages XSIAM's direct incident enrichment and automation features. Adding indicators directly from the incident to XSIAM's indicator store (which then feeds into detection engines) is a rapid response action. Configuring an 'Automation Rule' to trigger on specific incident types is key for automating playbooks for containment (like host isolation and firewall blocking) and enriching incidents with external threat intelligence (e.g., VirusTotal for hashes found on the compromised host). This is a core XSIAM strength for incident response. Option D: Creating a new 'Correlation Rule' is precisely how you build high-fidelity detections for multi-stage attacks like ransomware. Linking file encryption, security feature disablement, and C2 communication within a specific timeframe provides a very strong signal. Setting it to 'Critical' and triggering a comprehensive 'Security Playbook' (which can include automated containment, data collection, and notification) is the ideal programmatic response for a sophisticated threat. The XQL would indeed be complex, involving multiple joins, but this is the necessary approach for high-fidelity correlation. This proactively identifies future instances of this specific ransomware variant's behavior. Option A is good for adding indicators but doesn't fully capture the multi-faceted nature of the attack for rule creation and advanced automation. Option B's behavioral rule is too broad for high fidelity and might generate false positives without proper time-based correlation between the events. Option E involves manual steps and external systems, which is less efficient and proactive than XSIAM's integrated capabilities for immediate response.

NEW QUESTION # 23
What is the function of a Causality View?

- A. To present alerts from multiple data sources as individual incidents in the console
- B. To consolidate multiple security tools into a single interface to improve analyst productivity
- C. To provide users access to collaborate and execute CLI commands in Cortex XDR and Cortex XSIAM
- D. To present the alerts and process execution chain of all activity pertaining to the same event

Answer: D

Explanation:
A Causality View presents the alerts and process execution chain for all activity related to the same event, providing context for investigation.

NEW QUESTION # 24
A company is migrating its critical applications to a cloud environment and is using Cortex XDR for unified security. The security team needs to ensure that all access to sensitive cloud resources by service accounts is meticulously logged, auditable, and subject to 'break-glass' procedures for emergency access. Describe how Cortex XDR, in conjunction with cloud provider capabilities, supports this, specifically addressing user roles, log management, and compliance.

- A. Cortex XDR integrates with cloud provider's native logging services (e.g., AWS CloudTrail, Azure Activity Logs) to ingest service account activity into the Cortex Data Lake. Custom XQL queries are used for audit trails. 'Break-glass' access is managed via cloud IAM with alerts forwarded to Cortex XDR, and specific XDR roles are defined to monitor these alerts.
- B. Cortex XDR's network protection module actively blocks all service account access to cloud resources unless explicitly whitelisted in XDR. XDR's compliance module generates a report showing all unapproved cloud access. 'Break-glass' is a

manual process initiated outside of XDR.

- C. Cortex XDR's Agent provides direct monitoring of cloud service account activity. Custom roles are created in XDR to allow 'break-glass' access for specific analysts, bypassing cloud IAM. XDR's Data Lake stores all cloud access logs, which are then certified for PCI DSS compliance by Palo Alto Networks.
- D. Cortex XDR's Identity Threat Detection & Response (ITDR) module monitors cloud service accounts. Specific Cortex XDR roles are designed to allow granular control over which service accounts can access which cloud resources. All log data is stored on-premise for compliance reasons, regardless of cloud location.
- E. Cortex XDR automatically generates new, temporary service accounts for all cloud interactions, which are then deleted after use. These accounts are assigned the 'Cloud Admin' role in XDR. Compliance is achieved by exporting all XDR alerts to a GRC platform daily.

Answer: A

Explanation:
The most effective and realistic approach involves integrating Cortex XDR with the cloud provider's native logging capabilities. This allows Cortex XDR to ingest comprehensive service account activity logs into the Cortex Data Lake, enabling powerful XQL queries for audit trails and compliance. 'Break-glass' procedures are best managed through the cloud provider's IAM (e.g., AWS IAM roles with specific conditions, Azure AD PIM), with alerts from these actions forwarded to Cortex XDR for centralized monitoring and incident response. Specific Cortex XDR roles can then be defined to enable authorized personnel to monitor and respond to these critical 'break-glass' alerts, aligning with the principle of least privilege and comprehensive auditability.

NEW QUESTION # 25
.....

As we all know, the SecOps-Pro certificate has a very high reputation in the global market and has a great influence. But how to get the certificate has become a headache for many people. Our SecOps-Pro learning materials provide you with an opportunity. Once you choose our SecOps-Pro exam practice, we will do our best to provide you with a full range of thoughtful services. Our products are designed from the customer's perspective, and experts that we employed will update our SecOps-Pro Learning Materials according to changing trends to ensure the high quality of the SecOps-Pro study material.

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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 Palo Alto Networks SecOps-Pro dumps are available on Google Drive shared by Actual4test: https://drive.google.com/open?id=1Gx_D2X_MGTPOm9fGpTwWt-vgVsll0oSS