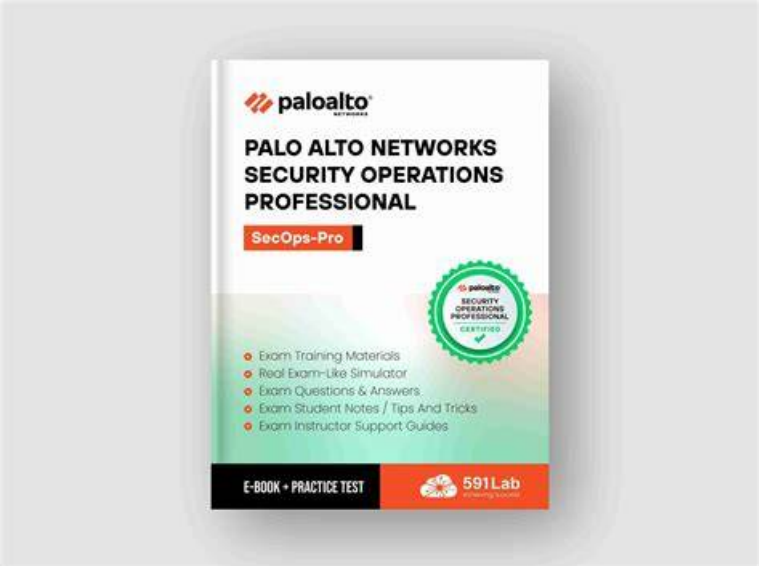
Features of Palo Alto Networks SecOps-Pro Web-Based Practice Test Software



P.S. Free & New SecOps-Pro dumps are available on Google Drive shared by RealExamFree: https://drive.google.com/open?id=1myIwrCiO1a3WHWvLnCojBOdXgobkAgUB

The Palo Alto Networks SecOps-Pro Certification is a valuable certificate that is designed to advance the professional career. With the Palo Alto Networks Security Operations Professional (SecOps-Pro) certification exam seasonal professionals and beginners get an opportunity to demonstrate their expertise. The Palo Alto Networks Security Operations Professional certification exam recognizes successful candidates in the market and provides solid proof of their expertise.

Palo Alto Networks SecOps-Pro Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Palo Alto Cortex Platform Operations	15%	- Automation and orchestration in Cortex - Cortex XDR architecture and core capabilities - Cortex Data Lake and data management
Topic 2: Security Operations Fundamentals	25%	- Security monitoring principles and requirements - Compliance and regulatory frameworks in SOC - SOC roles, responsibilities and workflows - Threat intelligence concepts and application
Topic 3: Threat Detection and Analysis	25%	- Detection rules, alerts and tuning - Indicators of Compromise (IOC) and Indicators of Attack (IOA) - Behavioral analytics and anomaly detection - Log and data collection, normalization and correlation
Topic 4: Incident Investigation and Response	25%	- Investigation methodologies and evidence gathering - Containment, eradication and recovery procedures - Post-incident activities and reporting - Incident classification, prioritization and triage
Topic 5: Cloud and Hybrid Security Monitoring	10%	- Integration with network and endpoint security tools - Cloud service visibility and threat detection - Hybrid environment monitoring strategies

>> Frenquent SecOps-Pro Update <<

Updated Frenquent SecOps-Pro Update Spend Your Little Time and Energy to Clear Palo Alto Networks SecOps-Pro: Palo Alto Networks Security

Operations Professional exam

Propulsion occurs when using our SecOps-Pro practice materials. They can even broaden amplitude of your horizon in this line. Of course, knowledge will accrue to you from our SecOps-Pro practice materials. There is no inextricably problem within our SecOps-Pro practice materials. Motivated by them downloaded from our website, more than 98 percent of clients conquered the difficulties. All contents of SecOps-Pro practice materials are being explicit to make you have explicit understanding of this exam. Their contribution is praised for their purview is unlimited.

Palo Alto Networks Security Operations Professional Sample Questions (Q76-Q81):

NEW QUESTION # 76
Your organization uses Cortex XSIAM to monitor both cloud and on-premise infrastructure. A security researcher identified a novel supply chain attack vector involving compromised open-source libraries used in your CI/CD pipelines. This compromise results in specific, low-volume outbound HTTP POST requests to an unusual domain from build servers, followed by dynamic library loading on production containers. You need to develop a rule in Cortex XSIAM that correlates these two distinct events to create a high-fidelity alert, while minimizing false positives from legitimate cloud traffic. Which rule type and XQL query best achieve this correlation?

- A. Rule Type: Correlation. XQL:

```
// First stage: Outbound POST to specific domain from build servers
stage_1 = xdr_data | filter event_type = 'network' and action_type = 'http_request' and http_method = 'POST' and dest_domain = 'malicious.attacker.com' and src_ip in (list_of_build_server_ips)

// Second stage: Dynamic library loading on production containers
stage_2 = xdr_data | filter event_type = 'process' and process_image_name in ('containerd', 'dockerd') and command_line contains ('dlopen', 'LD_PRELOAD', 'RTLD_LAZY') and host_type = 'container_runtime'

// Correlate the two stages with a time window and common identifier
join (stage_1, stage_2) on src_ip as correlated_ip | where stage_2._time > stage_1._time and stage_2._time < stage_1._time + duration('10m') | limit 100
```

- B. Rule Type: Anomaly. XQL:

```
dataset = xdr_data | filter event_type = 'network' and http_method = 'POST' and dest_domain in (malicious_domain_list) or event_type = 'process'
and process_image_name contains 'containerd' and command_line contains 'dlopen' | track by host_name, event_type | time series by 1m |
detect anomalies with baseline(metric=count(), interval='1d', threshold=5)
```

- C. Rule Type: Correlation. XQL:

```
network_events = dataset('xdr_data', '1h') | filter event_type = 'network' and action_type = 'http_request' and http_method =
'POST' and dest_domain = 'malicious.attacker.com' | fields src_ip, _time as network_time | process_events = dataset('xdr_data', '1h') |
filter event_type = 'process' and process_image_name contains 'containerd' and command_line contains 'dlopen' | fields host_ip as src_ip, _time
process_time | join kind=inner network_events on src_ip | where process_time > network_time and process_time < network_time + duration('5m')
| limit 100
```

- D. Rule Type: Simple Query. XQL:

```
dataset = xdr_data | filter (event_type = 'network' and http_method = 'POST' and dest_domain = 'malicious.attacker.com') or (event_type = 'process'
and process_image_name contains 'containerd' and command_line contains 'dlopen') | limit 10000
```

- E. Rule Type: Behavioral. XQL:

```
dataset = xdr_data | filter event_type = 'network' and action_type = 'http_request' and http_method = 'POST' and dest_domain =
'malicious.attacker.com' | group count() as count by src_ip, dest_domain | where count > 1 | join (dataset = xdr_data | filter event_type =
'process' and process_image_name = 'containerd' and command_line contains 'dlopen') on src_ip | limit 100
```

Answer: A

Explanation:
Option D provides the most accurate and robust correlation rule. Rule Type: Correlation: This is explicitly designed for linking distinct, multi-stage events, which is precisely the requirement. Named Sub-queries C stage_1', 'stage_2): This improves readability and modularity, making the complex query easier to manage and debug. Specific Filters for Each Stage: in for stage 1 directly addresses minimizing false positives by focusing on known build servers. For stage 2, in ('containerd', and multiple keywords for dynamic loading ('dlopen', 'RTLD_LAZY) are crucial for comprehensive detection on containers. Explicit 'join' with src_ip as correlated_ip': This correctly links the two stages via the originating IP, which is a common identifier in this attack pattern. Time Window (where stage_2._time > stage_1 ._time and stage_2._time < stage_1 ._time + duration('10m')'): This is critical for high-fidelity correlation, ensuring the second event happens after and within a reasonable timeframe of the first, significantly reducing false positives. Option B is also a 'Correlation' rule and gets close, but Option D's use of named sub-queries, more comprehensive stage 2 filtering, and explicit IP correlation ("correlated_ip') make it superior for this complex scenario. Option A uses 'join' but is formatted as a 'Behavioral' rule, which typically focuses on aggregations or single-event deviations. Option C uses 'Anomaly' which is not suitable for a specific, known multi-stage correlation. Option E is a simple 'OR query, which lacks the necessary correlation logic and time-based linking for a high-fidelity alert.

NEW QUESTION # 77
An organization is deploying Cortex XSOAR for advanced threat intelligence management. They have a requirement to create a custom indicator feed that aggregates specific threat intelligence from an internal API endpoint. This API returns data in a unique

XML format, and the organization needs to parse this XML, extract specific indicator types (e.g., SHA256 hashes, C2 domains), map them to XSOAR's internal indicator fields, assign a dynamic confidence score based on an XML attribute, and then ingest them. Which set of XSOAR configurations and steps is necessary to achieve this complex custom feed integration?

- A. Use an existing 'Threat Intelligence Feed' type and upload the XML file manually via the XSOAR I-Jl. Then, run a 'Data Transformation' playbook on the uploaded file to extract and map indicators.
- B. Develop a standalone external script that parses the XML and pushes the data to XSOAR using the XSOAR API. This script would then trigger an 'Indicator Playbook' to process the new indicators.
- C. Configure a 'Web Hook' to receive the XML data, then create an 'Incoming Mapper' to parse the XML and map fields. Use an 'Incident Type' to categorize the incoming data as threat intelligence.
- D. Configure a new 'Generic API Feed' instance, use a built-in XSOAR 'Mapper' with XPath expressions for XML parsing, and set a static confidence score within the feed configuration.
- E. Create a new 'Custom Feed' integration. Implement a custom Python script for the 'Fetch Indicators' command that handles the API call, XML parsing, indicator extraction, mapping, and dynamic confidence scoring. Define the indicator types in the script and ensure the script returns indicators in the expected XSOAR format.

Answer: E

Explanation:
Option B is the most appropriate and powerful solution for a complex custom feed with unique XML parsing and dynamic confidence scoring. 'Custom Feed' integration: This allows for complete control over the fetching logic. Custom Python script for 'Fetch Indicators': This script will contain the logic to: Make the API call to the internal endpoint. Parse the unique XML format (e.g., using Python's "xml.etree.ElementTree'). Extract the specific indicator types (SHA256, C2 domains). Map them to XSOAR's 'value' , 'type, 'expiration' reputation' , and crucially, dynamically calculate and assign the 'score (confidence) based on the XML attribute. This level of dynamic scoring and parsing is typically beyond standard Mappers. Return the data in the format XSOAR expects for indicators. Options A's built-in mapper might struggle with dynamic scoring and highly unique XML structures. Option C is for manual ingestion and lacks automation. Option D is for receiving data, not actively fetching it from an API endpoint, and is more geared towards incident creation. Option E is an external solution that bypasses XSOAR's native feed management capabilities, making it less integrated and harder to manage within XSOAR itself.

NEW QUESTION # 78
A critical server environment is running a legacy application that frequently executes unsigned scripts from a specific network share. To minimize false positives, the security team wants to allow these known legitimate scripts while blocking any other unsigned executables or scripts from running, especially if they originate from unusual locations or exhibit suspicious behavior. How can Cortex XDR's sensor policies be configured to achieve this granular control?

- A. By setting the entire policy to 'Block all unsigned files' and then manually whitelisting each individual legitimate script by its hash.
- B. By leveraging a combination of Execution Policy rules: creating an 'Allow' rule for the specific network share path and script names, and a separate 'Block' rule for unsigned executables/scripts from other locations, with the 'Allow' rule having higher precedence.
- C. Cortex XDR cannot differentiate between legitimate and malicious unsigned scripts; all unsigned scripts must be either allowed or blocked universally.
- D. By using the Local Analysis engine to automatically learn and whitelist all unsigned scripts that have executed successfully in the past.
- E. By deploying Cortex XDR in 'Monitor Only' mode on these servers and relying on manual review of alerts.

Answer: B

Explanation:
Cortex XDR's Execution Policy allows for very granular control over what can execute on an endpoint. This scenario specifically calls for allowing a known set of unsigned scripts while blocking others. This is best achieved by combining 'Allow' and 'Block' rules with precedence. An 'Allow' rule can be configured for the specific path (network share) and potentially file names of the legitimate scripts. A broader 'Block' rule can then be set for unsigned executables/scripts from other locations. Policies are evaluated in order of precedence (user-defined rules often precede default/system rules), allowing the specific 'Allow' rule to take priority for the legitimate scripts. Option A is impractical for frequently changing scripts. Option C is not how Local Analysis works for whitelisting. Option D defeats the purpose of prevention. Option E is incorrect as Cortex XDR offers sophisticated policy controls.

NEW QUESTION # 79

How is WildFire typically used by Cortex XDR?

- A. To serve as a cloud-based sandboxing and a malware analysis engine
- B. To display the compared artifacts with known bad SHA256 hashes
- C. To be an extension of the Unit 42 incident response team
- D. To build custom correlation rules using XQL

Answer: A

Explanation:
WildFire is a cloud-based sandbox and malware analysis engine used by Cortex XDR to detect and classify unknown threats.

NEW QUESTION # 80
A Security Operations Center (SOC) using Palo Alto Networks (PAN-OS) next-generation firewalls observes a sudden surge in outbound DNS requests to unusual top-level domains from a critical internal server. Threat intelligence feeds indicate recent campaigns leveraging DNS exfiltration. In the context of the NIST Incident Response Plan, which of the following actions best aligns with the 'Detection and Analysis' phase for this scenario, preceding further containment efforts?

- A. Notify executive leadership about a potential breach and prepare a public statement.
- B. Isolate the server from the network and begin forensic imaging, assuming compromise has occurred.
- C. Immediately block all outbound DNS traffic from the affected server using a PAN-OS Security Policy Rule.
- D. Update all antivirus signatures on endpoints across the entire network.
- E. Initiate a full packet capture on the firewall for all traffic from the affected server and analyze DNS query content for suspicious patterns, while also correlating with DNS Security logs.

Answer: E

Explanation:
The 'Detection and Analysis' phase focuses on determining if an event is an incident, its scope, and nature. While blocking traffic (A) might be a containment step, immediate full packet capture and correlation with DNS Security logs (B) provide crucial data for analysis without prematurely impacting legitimate services, which is essential for accurate incident classification. Isolating the server (C) and notifying leadership (D) are typically 'Containment, Eradication, and Recovery' or 'Post-Incident Activity' steps, and updating antivirus signatures (E) is a general security hygiene practice, not a primary detection and analysis step for a specific observed anomaly.

NEW QUESTION # 81
.....

download of ☀ SecOps-Pro □☀□ by searching on ➤ www.pdfvce.com □ □SecOps-Pro Reliable Test Review

- Hot Frenquent SecOps-Pro Update - How to Prepare for Palo Alto Networks SecOps-Pro Exam □ Go to website ➡ www.prep4sures.top □□□ open and search for " SecOps-Pro " to download for free □Valid SecOps-Pro Dumps Demo
- SecOps-Pro Reliable Test Review □ Download SecOps-Pro Fee □ SecOps-Pro Certified □ Search for { SecOps-Pro } and obtain a free download on □ www.pdfvce.com □ □SecOps-Pro Training Solutions
- Dumps SecOps-Pro Torrent □ New SecOps-Pro Braindumps Sheet □ SecOps-Pro Latest Exam Guide □ Easily obtain ➤ SecOps-Pro □ for free download through 「 www.easy4engine.com 」 □SecOps-Pro Exam Book
- SecOps-Pro Training Solutions □ SecOps-Pro Examcollection Questions Answers □ SecOps-Pro Training Tools □ Enter { www.pdfvce.com } and search for ➠ SecOps-Pro □ to download for free □SecOps-Pro Certified
- Quiz Palo Alto Networks - SecOps-Pro - Palo Alto Networks Security Operations Professional High Hit-Rate Frenquent Update □ Search for ✔ SecOps-Pro □✔□ and easily obtain a free download on ⇛ www.troytecdumps.com ⇚ □SecOps-Pro Passed
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free 2026 Palo Alto Networks SecOps-Pro dumps are available on Google Drive shared by RealExamFree: https://drive.google.com/open?id=1myIwrCiO1a3WHWvLnCojBOdXgobkAgUB