Quiz 2026 Palo Alto Networks SecOps-Pro: High-quality Palo Alto Networks Security Operations Professional Test Dumps.zip

For a guaranteed path to success in the Palo Alto Networks Security Operations Professional (SecOps-Pro) certification exam, DumpsReview offers a comprehensive collection of highly probable Palo Alto Networks SecOps-Pro Exam Questions. Our practice questions are meticulously updated to align with the latest exam content, enabling you to prepare efficiently and effectively for the SecOps-Pro examination. Don't leave your success to chance—trust our reliable resources to maximize your chances of passing the Palo Alto Networks SecOps-Pro exam with confidence.

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-Prolearning 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. Whenever you have questions about our SecOps-Pro study guide, our service will give you the most professional advice.

>> SecOps-Pro Test Dumps.zip <<

High Pass-Rate Palo Alto Networks SecOps-Pro Test Dumps.zip & Trustable DumpsReview - Leading Provider in Qualification Exams

Free demo is available for SecOps-Pro training materials, so that you can have a better understanding of what you are going to buy. Free demo will represent you what the complete version is like. We suggest you try free domo before buying. In addition, SecOps-Pro training materials are high quality and accuracy, since we have a professional team to collect the latest information of the exam. Therefore if you choose SecOps-Pro Exam Dumps of us, you can get the latest version timely. We provide you with free update version for one year for SecOps-Pro training materials.

Palo Alto Networks Security Operations Professional Sample Questions (Q197-Q202):

NEW QUESTION # 197
A Security Operations Center (SOC) using Cortex XSIAM has identified a highly sophisticated, multi-stage attack involving lateral movement and data exfiltration through an unknown C2 channel. The SOC analyst needs to rapidly contain the threat and enrich the incident data for forensic analysis. Which combination of Cortex XSIAM automation and integration components would be most effective in orchestrating an immediate, robust response?

- A. Playbooks triggered by custom XQL queries, integrating with external EDR solutions for host isolation and SIEM for log ingestion.
- B. Built-in MITRE ATT&CK correlation engine for threat identification, coupled with a manual API call to a SOAR platform for remediation.
- C. Alert grouping and deduplication for noise reduction, followed by a scheduled report generation for management review.
- D. Manual investigation using the XSIAM Investigation Canvas and then escalating to a ticketing system for follow-up.

- E. Automated incident creation from a single XDR alert, using built-in actions to quarantine endpoints and block suspicious IPs via NGFW integration.

Answer: E

Explanation:
Option D describes the most effective and automated approach. Cortex XSIAM's strength lies in its ability to automate responses directly from XDR alerts. Automatically quarantining endpoints and blocking IPs via NGFW integration provides immediate containment, which is critical for a multi-stage attack. While Playbooks (A) are powerful, 'custom XQL queries' suggest a more manual trigger or a less immediate, pre- defined response than an alert-driven automation. Option B involves manual intervention. Options C and E are reactive and lack immediate containment capabilities.

NEW QUESTION # 198
A security incident escalates to a full-scale breach investigation. Logs from Cortex Data Lake reveal suspicious outbound connections to multiple, previously unknown IP addresses (198.51.100.1, 198.51.100.2, 198.51.100.3) originating from internal compromised hosts, along with a newly observed file hash (d41d8cd98fOOb20=4e980998ecf8427e) associated with a dropper. The incident response team needs to quickly identify all historical instances of these indicators, determine their reputation, and deploy countermeasures across a global network. Which programmatic solution, combining XQL, Cortex XSOAR, and NGFW APIs, offers the most efficient and scalable approach?

- A. Deploy a 'Live Response' script via Cortex XDR to all endpoints to search for the file hash and delete it. For IPs, rely on DNS Security to block access to resolved malicious domains, not direct IP blocking.
- B. Utilize Cortex XSOAR's 'IOC Feed' integration to ingest the IPs and file hash. Configure this feed to automatically update the firewall's 'Anti-Spyware' profile for IPs and 'Threat Prevention' profile for the file hash, then generate a report from Cortex Data Lake.
- C. Run multiple XQL queries manually in Cortex XDR for each IP address and the file hash. Then, manually add each IP to a Custom URL Category on the NGFW, and manually create a WildFire custom signature for the file hash.
- D. Create a new 'Analytics Rule' in Cortex XDR to alert on future occurrences of the IPs and file hash. Then, email the list of IPs and the hash to the network team for manual firewall rule creation.
- E.

Answer: E

Explanation:
Option A provides the most efficient, scalable, and automated programmatic solution leveraging the indicated Cortex products and their integration capabilities: 1. XQL Query for Historical Lookup: The XQL query shown is powerful and scalable for querying Cortex Data Lake (which underpins Cortex XDR's data) for both IP addresses and file hashes across a specified time range. This efficiently identifies all historical instances. 2. Enrichment via AutoFocus/Unit 42: Cortex XSOAR (through its 'ip' and 'file' commands, which abstract integrations like AutoFocus and Unit 42) can instantly fetch reputation and context for the indicators. This is crucial for confirming their maliciousness and understanding the threat. 3. Dynamic Blocking (NGFW and XDR): IPs: XSOAR can dynamically update an External Dynamic List (EDL) on the NGFW via API. EDLs are highly efficient for blocking large numbers of IPs without manual configuration or commit operations, ensuring network-wide prevention. File Hash: XSOAR can programmatically update Cortex XDR's prevention policies (e.g., 'Malware Prevention' policy) to block the execution of the specific file hash across all managed endpoints. This provides endpoint-level prevention. 4. Automated Incident Creation/Response: The script triggers an incident in XSOAR if historical data is found, allowing for further automated or manual investigation and remediation via playbooks. Option B is too manual and not scalable. Option C's method of updating Anti-Spyware/Threat Prevention profiles for specific IPs/hashes via generic IOC feeds might not be as granular or flexible as EDLs and XDR prevention policies, and it lacks the comprehensive XQL historical lookup and automated response. Option D is reactive (deletion) and focuses only on endpoints for the file, and its IP blocking strategy is indirect. Option E is reactive and completely manual for network countermeasures.

NEW QUESTION # 199
Consider a scenario where an XSOAR playbook needs to dynamically query a vulnerability management system (VMS) for asset vulnerabilities and then update a CMDB with remediation status. The VMS has a REST API that requires OAuth 2.0 client credentials grant type for authentication, and the CMDB uses a SOAP API. How would an XSOAR developer architect the integration to handle these authentication and communication complexities within a single playbook task?

- A. Use the
- B. Configure a generic HTTP integration for the VMS and a generic SOAP integration for the CMDB, relying on XSOAR's

built-in authentication mechanisms for OAuth 2.0.

- C. Utilize XSOAR's native integrations for VMS and CMDB, assuming they both support OAuth 2.0 and SOAP respectively, and then map the fields in the playbook.
- D. Export VMS data to a CSV, manually import into XSOAR, then use a scheduled script to push to CMDB.
- E. Develop a Python integration for the VMS using the

Answer: E

Explanation:
This scenario requires handling distinct authentication (OAuth 2.0) and communication protocols (REST, SOAP). Option B directly addresses this by recommending custom Python integrations. For OAuth 2.0, requests_oauthlib is a standard library. For SOAP, suds-py3 (or similar) is appropriate. These custom integrations provide the necessary flexibility and control over authentication flows and API interactions, which are then exposed as commands to the playbook. Option C is incomplete as XSOAR's generic integrations may not fully handle complex OAuth 2.0 flows without custom code. Option A is insecure and not idiomatic for XSOAR. Options D and E are either too manual or assume out-of-the-box support that might not exist for specific VMS/CMDB versions or their authentication requirements.

NEW QUESTION # 200
During the 'Recovery' phase of the NIST Incident Response Plan, after a data exfiltration incident, a SOC analyst needs to ensure the integrity of critical data and systems before bringing them back online. Which of the following technical validation steps, incorporating Palo Alto Networks capabilities, is crucial for a robust recovery and prevents re-infection?

- A. Implement an entirely new network architecture, replacing all compromised hardware, before restoring any data.
- B. Confirm service availability by pinging critical servers and checking website uptime, then update all system passwords across the organization.
- C. After restoring systems, leverage Cortex XDR's post-infection analysis to scan for any residual malicious files or processes, and cross-reference logs with WildFire verdicts for newly seen executables.
- D. Restore data from the latest backup, then perform a full network vulnerability scan using an external scanner to identify remaining open ports.
- E. Deploy a new set of firewall rules that block all outbound traffic from the recovered segment, then conduct user training on phishing awareness.

Answer: C

Explanation:
The 'Recovery' phase involves restoring affected systems and services. Option C is key for robust recovery and preventing re-infection. Simply restoring from backup (A) doesn't guarantee the backup itself wasn't compromised or that new malware wasn't introduced during recovery. Using Cortex XDR's post-infection analysis for residual threats and correlating with WildFire verdicts ensures that restored systems are clean from known and potentially new (zero-day) malware, providing a high level of confidence before full reintegration. Blocking all outbound traffic (B) is too restrictive for recovery, and user training is for prevention. Pinging servers (D) is a basic availability check, not a security validation. Implementing a completely new network architecture (E) is an extreme and often impractical step for most recovery scenarios.

NEW QUESTION # 201
A threat hunter discovers a suspicious executable file, 'update.exe' , with a SHA256 hash of 'e3b0c44298fc1 c149afbf4c8996fb92427ae41 e4649b934ca495991 b7852b85S on several workstations. This hash is not immediately present in any standard threat intelligence feeds. Further investigation reveals 'update.exe' is communicating with an external IP address over a non-standard port '49152. The file was found in Which of the following approaches leverages Palo Alto Networks security capabilities most effectively for further investigation and to proactively hunt for other infected hosts, given that WildFire and Advanced Threat Prevention are enabled?

- A. Add 192.0.2.10' to a custom Block List EDL on the Palo Alto Networks firewall and apply it to all outbound security policies. Configure a new Antivirus profile with 'reset-both' action for all executables. Search the Palo Alto Networks firewall logs in Panorama for connections to ' 192.0.2.10' on port '49152.
- B. Since the hash is unknown, it's likely a zero-day. Immediately isolate the affected workstations. Then, configure an IPS signature on the Palo Alto Networks firewall to block traffic to '192.0.2.1ff on '49152. Use Cortex XDR to search for the filename 'update.exe' across all endpoints.
- C. Submit the file to WildFire. If malicious, WildFire will generate a signature. Then, configure a custom URL filtering category for '192.0.2.10' and block it. Perform a Log Forwarding query in Panorama to find 'update.exe' by filename and

verify its network activity. Use objects url-filtering custom- url-category to verify the configuration.

- D. Submit the SHA256 hash 'e3bOc44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b85S to Wildfire for analysis. once a verdict is received, use the WildFire analysis report to identify associated network patterns and behaviors. Then, utilize the Palo Alto Networks CLI command threat type wildfire hash to check if any other firewalls have seen this hash.
- E. Upload 'update.exe' to an external sandbox service for analysis. Create a custom URL filtering profile to block '192.0.2.10' and apply it to relevant security policies. Use the Panorama device's 'Custom Reports' feature to search for 'update.exes filename in traffic logs.

Answer: D

Explanation:
The most effective approach leverages WildFire's capabilities directly. Submitting the SHA256 hash to WildFire (Option B) is the correct first step as it provides a verdict and detailed behavioral analysis, even for previously unknown files. WildFire will then distribute the signature if malicious. The subsequent use of 'show threat type wildfire hash' is excellent for hunting across the entire firewall estate for other instances of this specific malicious file based on its hash. While other options have valid steps, they don't fully leverage the integrated capabilities or are less efficient for this specific scenario. Option A uses an external sandbox and relies on filename in logs which can be easily changed. Option C adds to an EDL, which is good for blocking, but doesn't get the initial verdict or detailed analysis like WildFire. Option D jumps to isolation and assumes zero-day without leveraging the primary analysis tool. Option E describes a similar process to B but doesn't explicitly mention using the hash for hunting across other firewalls effectively.

NEW QUESTION # 202
.....

Reliable Exam Online

- SecOps-Pro Test Preparation: Palo Alto Networks Security Operations Professional - SecOps-Pro Exam Lab Questions □ □ Search for [SecOps-Pro] on 【 www.pdfvce.com 】 immediately to obtain a free download □Valid Test SecOps-Pro Bootcamp
- SecOps-Pro Valid Exam Tutorial □ Guaranteed SecOps-Pro Passing □ Valid SecOps-Pro Test Vce □ Open ➠ www.vceengine.com □ enter ➤ SecOps-Pro □ and obtain a free download □SecOps-Pro Latest Exam Experience
- Let SecOps-Pro Test Dumps.zip Help You Pass The Palo Alto Networks Security Operations Professional □ Search for " SecOps-Pro " and download it for free immediately on 「 www.pdfvce.com 」 □SecOps-Pro Latest Exam Experience
- 100% Pass Quiz Palo Alto Networks - SecOps-Pro - Pass-Sure Palo Alto Networks Security Operations Professional Test Dumps.zip □ Open ➥ www.examcollectionpass.com □ and search for ➠ SecOps-Pro □ to download exam materials for free □SecOps-Pro Valid Exam Tips
- New SecOps-Pro Study Plan □ SecOps-Pro Examcollection Questions Answers □ Latest SecOps-Pro Exam Papers □ □ Open [www.pdfvce.com] enter ➤ SecOps-Pro □ and obtain a free download □Latest SecOps-Pro Exam Papers
- SecOps-Pro PDF Guide □ SecOps-Pro Brain Exam □ SecOps-Pro Brain Exam □ Search on □ www.vce4dumps.com □ for □ SecOps-Pro □ to obtain exam materials for free download □SecOps-Pro PDF Guide
- Authorized SecOps-Pro Pdf □ SecOps-Pro Valid Exam Tips □ Examcollection SecOps-Pro Dumps Torrent □ Search for □ SecOps-Pro □ on ⇒ www.pdfvce.com ⇐ immediately to obtain a free download □SecOps-Pro Valid Exam Tutorial
- Valid Test SecOps-Pro Bootcamp □ SecOps-Pro Latest Exam Experience □ SecOps-Pro Examcollection Questions Answers □ Enter 「 www.testkingpass.com 」 and search for ➥ SecOps-Pro □ to download for free □SecOps-Pro Reliable Exam Online
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, jmaelearning.net, www.stes.tyc.edu.tw, gdf.flyweis.in, 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, bbs.t-firefly.com, Disposable vapes