Quiz Palo Alto Networks SecOps-Pro - Palo Alto Networks Security Operations Professional Fantastic New Exam Pdf

ExamCost Palo Alto Networks Security Operations Professional (SecOps-Pro) practice exam (desktop and web-based) keep track of the previous attempts. These Palo Alto Networks Security Operations Professional (SecOps-Pro) practice tests also show mistakes on every attempt. So this feature helps you reduces your chance of failure in the SecOps-Pro actual examination. The Palo Alto Networks SecOps-Pro Exam Questions are instantly downloadable right after your purchase. In the same way,ExamCost provides a money back guarantee if in any case you don't ace the SecOps-Pro exam after using our product. Terms and conditions are mentioned on the guarantee page.

Annual test syllabus is essential to predicate the real SecOps-Pro questions. So you must have a whole understanding of the test syllabus. After all, you do not know the SecOps-Pro exam clearly. It must be difficult for you to prepare the SecOps-Pro exam. Then our study materials can give you some guidance. All questions on our SecOps-Pro study materials are strictly in accordance with the knowledge points on newest test syllabus. Also, our experts are capable of predicating the difficult knowledge parts of the SecOps-Pro Exam according to the test syllabus. We have tried our best to simply the difficult questions. In order to help you memorize the SecOps-Pro study materials better, we have detailed explanations of the difficult questions such as illustration, charts and referring website. Every year some knowledge is reoccurring over and over. You must ensure that you master them completely.

>> New SecOps-Pro Exam Pdf <<

UPDATED Palo Alto Networks SecOps-Pro PDF QUESTIONS [2026]-QUICK TIPS TO PASS

We constantly improve and update our SecOps-Pro study materials and infuse new blood into them according to the development needs of the times and the change of the trend in the industry. We try our best to teach the learners all of the related knowledge about the test SecOps-Pro Certification in the most simple, efficient and intuitive way. We pay our experts high remuneration to let them play their biggest roles in producing our SecOps-Pro study materials.

Palo Alto Networks Security Operations Professional Sample Questions (Q258-Q263):

NEW QUESTION # 258
A SOC analyst is reviewing a high-fidelity alert in Cortex XSIAM indicating 'Malicious Scheduled Task Creation'. The alert details show a 'schtasks.exe' command creating a task that points to a suspicious executable. To fully understand the scope of compromise and identify other potentially affected endpoints, the analyst needs to pivot from this single alert to identify: 1. All other endpoints where this exact suspicious executable (identified by its SHA256 hash) has been observed. 2. Any network connections made by this executable across the entire environment. 3. Instances where the scheduled task was executed, rather than just created. Which sequence of actions within Cortex XSIAM's capabilities would be the most efficient and comprehensive approach to this investigation? (Select all that apply)

- A. Utilize the 'Timeline' view for the affected host from the alert to understand the process execution chain. Use 'Quick Query' on the SHA256 hash to find all instances. For network connections, go to the 'Network' tab on the host timeline or search globally with 'dataset = network_flows I filter file_sha256 = To identify task executions, create a custom XQL rule 'dataset = xdr_data I filter event_type = 'process' and action_process_image_name = 'powershell.exe' and command_line contains 'extracted_task_name''.
- B. From the alert, utilize the 'Investigate' button which takes you to the Incident Graph. In the graph, pivot on the identified SHA256 hash to automatically see all related events, including executions across hosts and associated network connections. For verifying scheduled task executions, examine process creation events where the parent process is commonly 'taskhostw.exe' or 'svchost.exe' (which launches 'taskeng.exe'), and the child process is the suspicious executable or a known task runner, by building an XQL query like:

  ▫
- C. From the alert, extract the SHA256 hash of the executable. Navigate to the 'Search' page, perform a query 'dataset = xdr_data I filter file_sha256 = 'extracted_hash'' to find all executions. Then, refine the same query to 'dataset = xdr_data I filter file_sha256 = 'extracted_hash' and event_type = 'network'' to find network connections. Finally, search 'dataset = xdr_data I filter action_process_image_name = 'schtasks.exe' and command_line contains 'extracted_task_name' and event_type = 'process_creation'' for execution.
- D. Extract the SHA256 hash and the scheduled task name from the alert. From the 'Search' page, run 'dataset = xdr_data I filter file_sha256 = 'extracted_hash' I dedup host_name' to get unique affected hosts. Then, for network connections, use 'dataset = xdr_data I filter file_sha256 = 'extracted_hash' and event_type = 'network_connection'' with the 'Distinct Values' aggregation on 'dest_ip, dest_port'. For task execution, construct a query like 'dataset = xdr_data I filter event_type = 'process' and action_process_image_name = 'powershell.exe' and parent_process_image_name = 'taskhostw.exe' and command_line contains 'extracted task namer.
- E. From the alert's 'Incident Details' page, leverage the 'Artifacts' section to identify the SHA256 hash. Then, use the 'XDR Process Explorer' to trace process activities related to the hash. For broader environmental search, initiate a 'Live Query' or a 'Historical Query' for the SHA256 hash across all endpoints. To find network connections, pivot from the 'Network Story' in the incident or query 'dataset = xdr_data I filter event_type = 'network' and file_sha256 = 'extracted_hash'&. For scheduled task executions, query 'dataset = xdr_data I filter event_type = 'process' and action_process_image_name contains 'taskeng.exe' and parent_process_image_name contains 'svchost.exer and then filter by the scheduled task name or process ID from the creation event.

Answer: B,E

Explanation:
Options C and E represent the most comprehensive and efficient approaches within Cortex XSIAM. Option C: Leveraging 'Incident Details' and 'Artifacts' is a standard starting point. 'Live Query' or 'Historical Query' are purpose-built for broad environmental searches of artifacts. 'Network Story' is an excellent, visualized way to understand network activity. The suggested XQL for scheduled task execution ('taskeng.exe' often being launched by 'svchost.exe') is accurate for identifying scheduled task executions as distinct from creation. Option E: The 'Investigate' button leading to the Incident Graph is a core XSIAM capability specifically designed for interconnected investigations. Pivoting on artifacts like SHA256 in the graph automatically reveals related executions and network connections, greatly simplifying step 1 and 2. For step 3, the XQL provided accurately targets typical parent processes for scheduled task execution ('taskhostw.exe' on newer Windows, or 'svchost.exe' launching 'taskeng.exe' for older/other contexts) and then looks for the suspicious executable or the specific task command, allowing for robust detection of the execution phase. Both options prioritize XSIAM's built-in investigation tools and efficient XQL queries. Options A, B, and D are less comprehensive, less efficient, or contain inaccuracies in their proposed XQL or workflow.

NEW QUESTION # 259

During a critical incident response involving a sophisticated ransomware attack, a security analyst uses Cortex XSOAR's War Room. The analyst wants to document a key finding, specifically a unique registry key dropped by the malware, and ensure this information is immediately accessible to all incident responders, while also being automatically added to the incident's evidence locker for future forensic analysis. Which War Room feature(s) would the analyst leverage, and what is the most efficient way to achieve this comprehensive documentation and evidence collection?

- A. The analyst should use the 'Add Note' feature in the War Room, manually paste the registry key, and then manually attach the note to the evidence locker. The analyst must also remember to tag the note appropriately for discoverability.
- B. The analyst should leverage the 'Command Line Interface' within the War Room to execute a playbook task that has an associated 'Evidence' output. This task could then log the registry key directly into the War Room and the evidence locker simultaneously, ensuring automation and consistency.
- C. The analyst should use the 'Journal' tab to record the finding, ensuring it's time-stamped. For evidence collection, they would then need to navigate to the 'Evidence' tab and manually add a new evidence item, referencing the journal entry.
- D. The analyst should utilize the 'Add Entry' feature, specifically choosing an 'Evidence' entry type. They can then input the

registry key, and XSOAR will automatically link it to the incident and record it in the evidence locker, making it searchable within the War Room and incident context.

- E. The analyst should execute a custom War Room command like key=HKEY_LOCAL_MACHINE\SOFTWARE\MalwareDrop' which not only adds it as a War Room entry but also automatically classifies it as evidence and tags it for future search. This command ensures it's instantly visible to all collaborators.

Answer: E

Explanation:
Option C is the most efficient and robust method. Cortex XSOARs War Room supports various commands, including custom ones or those from integrations, that can directly add evidence, notes, or entries with specific types. Using a command like (or a similar pre-configured command/script) allows for a single action to achieve multiple objectives: adding a structured War Room entry, classifying it as evidence, tagging it for search, and making it immediately visible to all collaborators. While options B and E are plausible, C specifically highlights the power of direct command execution for structured data entry and automated evidence handling, which is a key strength of the War Room for efficient incident response. Option B describes adding an entry, but 'Evidence' entry type is often tied to specific evidence collection commands or outputs. Option E is more about a playbook task's output, not necessarily a direct analyst action within the War Room CLI for immediate evidence logging.

NEW QUESTION # 260
A SOC manager is reviewing the current state of their threat detection capabilities. They notice that the SIEM frequently generates alerts for 'Port Scan' events, but a significant number are benign network scans from IT operations tools, leading to high false-positive rates. They want to refine these detections using a combination of their Palo Alto Networks SIEM (e.g., Splunk with Palo Alto Networks add-ons) and Cortex XDR, moving towards a behavior-based approach to identify truly malicious port scans and associated activity.
Which of the following strategies, leveraging the specific capabilities, would be most effective?

- A. Increase the sensitivity of the 'Vulnerability Protection' profile on the NGFW to detect more types of port scan attacks, and use WildFire to analyze any associated suspicious files.
- B. Implement 'User-ID' and 'App-ID' on the NGFW to identify traffic sources and applications. In the SIEM, enrich port scan events with User-ID and App-Ld context. Additionally, in Cortex XDR, leverage 'Behavioral Threat Protection' (BTP) to detect suspicious sequences of network events (e.g., port scan followed by suspicious process execution or data access patterns) rather than just the scan itself. For known benign IT scanners, create XDR 'Exclusion Policies' based on process hash or digital signature.
- C. Disable all default 'Port Scan' alerts in the SIEM and rely solely on Cortex XDR's 'Threat Prevention' module to block known malicious port scans.
- D. Configure the SIEM to only alert on port scans that originate from external IP addresses, completely ignoring internal scans.
- E. Create an allow-list in the NGFW's 'Security Policy' for the IP addresses of IT operations tools performing scans, and configure the SIEM to ignore these specific IPs.

Answer: B

Explanation:
This scenario requires a sophisticated, multi-layered approach to reduce false positives while improving true positive detection for port scans, moving from signature-based to behavior-based.
1. User-ID and App-ID on NGFW (and SIEM Enrichment): This is crucial for context. User-ID links network activity to specific users, and App-Ld identifies the actual application. This allows the SIEM to differentiate between a legitimate IT scan tool (e.g., Nessus, identified by App-ID, run by an IT user via User-ID) and a malicious scan. Enriching SIEM alerts with this context is vital for analysis.
2. Cortex XDR Behavioral Threat Protection (BTP): This is the core of the behavior-based approach. Instead of just flagging a port scan, BTP looks for the sequence of events. A standalone port scan might be benign, but a port scan followed by a suspicious login, process execution, or data access pattern is highly indicative of malicious intent. This helps identify 'living off the land' attacks.
3. XDR Exclusion Policies: For known legitimate IT operations tools (e.g., vulnerability scanners, network inventory tools), creating specific exclusions in Cortex XDR based on reliable identifiers (process hash, digital signature) prevents these tools from triggering BTP alerts, significantly reducing false positives.
Let's analyze other options:
A: Disabling all alerts is reckless. Relying only on 'Threat Prevention' is too simplistic for behavioral detection.
B: While creating allow-lists is a common practice for reducing noise, it relies on static IPs and doesn't address the behavioral aspect of advanced threats. It's a good step but not the most effective for a comprehensive behavior-based approach.

D: Ignoring all internal scans is a severe security gap, as internal lateral movement is a common attack vector.
E: Increasing sensitivity of 'Vulnerability Protection' might just lead to more false positives. WildFire is for file analysis, not directly for refining port scan detections or behavioral analysis of network activity.

NEW QUESTION # 261

Your organization uses Cortex XSIAM to proactively hunt for sophisticated 'living off the land' attacks. You suspect an attacker is leveraging legitimate Windows utilities like 'certutil.exe' to download malicious payloads and 'bitsadmin.exe' for persistence, avoiding direct malware drops. You need to create a single XQL query that identifies instances where 'certutil.exe' downloads an executable or script from a public file-sharing service (e.g., pastebin.com, raw.githubusercontent.com) AND, on the same host, 'bitsadmin.exe' is used to create a background transfer job involving a suspicious file type within a 30-minute window. This query must be efficient for a large dataset.

- A. □
- B. □
- C. □
- D. □
- E. □

Answer: C

Explanation:
Option E is the most accurate, robust, and efficient XQL query for this complex hunting scenario. Clear Stage Separation: It correctly separates the two distinct stages ('certutil_events' and 'bitsadmin_events') into named sub-queries, improving readability and maintainability. Precise Filtering for Each Stage: 'certutil.exe': Checks for 'command_line contains '-urlcache -f'' (download command) and 'command_line like_any ('%.exe', '%.dll', '%.psl' '%.vbs', '%.js')' for suspicious file extensions. Using 'like_any' is more robust than ''contains' for specific extensions. It also correctly filters by 'dest_domain' for public file-sharing services. 'bitsadmin.exe': Checks for 'command_line contains '/addfile'' and 'command_line like_any ('%.exe', '%.dll', '%.psl')' for suspicious file types. Efficient Time Filtering: Applying '_time > now() - early in each sub-query significantly prunes the dataset, making the joins more efficient, especially for a large environment. Correct Join Logic: 'join kind=inner certutil_events on host_name I join bitsadmin_events on host_name' ensures that only events from the same host are correlated. Accurate Time Window Correlation: 'where bits time > cert time and bits time < cert time + duration('30m')' precisely implements the required 30-minute window, ensuring the 'bitsadmin' event occurs after the 'certutil' download and within the specified time, leading to high fidelity. Relevant Field Selection and Sorting: 'select host_name, cert_time, cert_cmd, bits_time, bits_cmd I sort by cert_time dese provides all necessary details in a logical order. Option B is very similar but uses multiple 'join' statements which can be less efficient or syntactically ambiguous depending on XQL version compared to chaining. Option A and C attempt to combine conditions with 'AND directly on a single dataset, which is semantically incorrect for correlating two distinct events . Option D uses 'union', which would combine rows but not correlate them based on host and time window.

NEW QUESTION # 262

During a proactive threat hunt, a Palo Alto Networks Security Operations Professional observes a pattern of outbound connections from several internal Linux servers to IP addresses listed on a newly acquired threat intelligence feed as known C2 infrastructure for a sophisticated APT group. The connections are primarily over TCP port 8080 and exhibit very low data transfer volumes, but consistent heartbeat-like communication. Existing security policies do not explicitly block port 8080. Which of the following actions, in conjunction with relevant CLI commands or configurations on a Palo Alto Networks firewall, would be the MOST appropriate immediate response to investigate and contain this potential compromise, assuming the firewall is configured to send logs to an external SIEM and has URL filtering/WildFire enabled?

- A. Perform a 'test security policy match' on the Palo Alto Networks firewall to understand why the traffic isn't blocked. Then, enable strict URL filtering profiles on the affected security rules. Finally, configure a new vulnerability protection profile with 'reset-both' for all medium and high severity threats on the relevant security rules, and wait for the firewall to automatically block future connections.
- B. Given the 'heartbeat-like' communication and low data volume, this suggests command and control. The most effective immediate response should focus on disrupting the C2. Prioritize creating a new security policy at the top of the rulebase to block outbound TCP 8080 traffic from the affected Linux servers to the identified C2 IP addresses. Simultaneously, initiate packet captures for these specific flows and escalate to the incident response team for forensic analysis on the compromised servers. The firewall command to capture might be packet-capture stage firewall match source <src_ip> destination <dest_ip> port 8080 count 1000</code></pre>'.
- C. Immediately create a new security policy to block all outbound traffic on TCP port 8080 from the affected Linux servers.

Then, run a packet capture on the firewall for these specific connections using '<pre><code>debug flow basic <src_ip> and analyze the pcap for malicious payloads.

- D. Configure a custom application signature on the Palo Alto Networks firewall to identify the specific C2 communication protocol based on traffic patterns and payload content. Once identified, create a security policy to block this custom application. Concurrently, use the session all filter destination <C2 command to identify active sessions and terminate them using session id
- E. Update the external dynamic list (EDL) on the Palo Alto Networks firewall with the new C2 IP addresses. Configure a new security policy rule with an 'alert' action for traffic matching the EDL, then review the threat logs for hits. Initiate a WildFire analysis on any suspicious file hashes observed from these connections using wildfire status</code></pre>'.

Answer: B

Explanation:
This is a critical C2 indicator. Option D represents the most appropriate immediate response. Blocking the C2 traffic is paramount for containment, and a targeted block specific to the affected servers and C2 IPs on port 8080 is an effective initial step. Simultaneously capturing packets provides crucial evidence for further investigation without disrupting all 8080 traffic. Escalating to the IR team for forensic analysis is also a critical next step. Option A is too broad with the block. Option B is reactive and might not immediately disrupt active C2; EDLs update periodically. Option C is a good long-term solution for detecting the specific application, but signature creation takes time and isn't an immediate containment action. Option E is investigative and reactive, not an immediate containment.

NEW QUESTION # 263
......

Our SecOps-Pro exam questions boost 3 versions and varied functions. The 3 versions include the PDF version, PC version, APP online version. You can use the version you like and which suits you most to learn our SecOps-Pro test practice materials. The 3 versions support different equipment and using method and boost their own merits and functions. For example, the PC version supports the computers with Window system and can stimulate the real exam. Each version of our SecOps-Pro Study Guide provides their own benefits to help the clients learn the SecOps-Pro exam questions efficiently.

Exam SecOps-Pro Simulator: https://www.examcost.com/SecOps-Pro-practice-exam.html

Your SecOps-Pro exam success is guaranteed with learning of our SecOps-Pro exam questions pdf, The SecOps-Pro pdf dumps file is the most efficient and time-saving method of preparing for the Palo Alto Networks SecOps-Pro exam, There are many benefits after you pass the SecOps-Pro certification such as you can enter in the big company and double your wage, We will definitely guarantee the quality of our SecOps-Pro pass4sure pdf and services, so don't worry about it.

Was this a viable vision and how far along are we, We still make no attempt to optimize router selection by distributing more detailed routes, Your SecOps-Pro Exam Success is guaranteed with learning of our SecOps-Pro exam questions pdf.

Desktop Based Palo Alto Networks SecOps-Pro Practice Test Software

The SecOps-Pro pdf dumps file is the most efficient and time-saving method of preparing for the Palo Alto Networks SecOps-Pro exam, There are many benefits after you pass the SecOps-Pro certification such as you can enter in the big company and double your wage.

We will definitely guarantee the quality of our SecOps-Pro pass4sure pdf and services, so don't worry about it, The following are the reasons why to choose SecOps-Pro study dumps.

- Pass Guaranteed Quiz Palo Alto Networks - SecOps-Pro –Professional New Exam Pdf □ Search for □ SecOps-Pro □ and download it for free immediately on ✔ www.testkingpass.com □✔□ □Exam SecOps-Pro Questions
- Palo Alto Networks Security Operations Professional sure pass dumps - SecOps-Pro actual training pdf □ Open ▶ www.pdfvce.com ◀ and search for " SecOps-Pro " to download exam materials for free □SecOps-Pro Valid Exam Tips
- Authoritative New SecOps-Pro Exam Pdf Supply you Trusted Exam Simulator for SecOps-Pro: Palo Alto Networks Security Operations Professional to Prepare easily □ Open website ⇛ www.practicevce.com ⇚ and search for □ SecOps-Pro □ for free download □Exam SecOps-Pro Certification Cost
- SecOps-Pro Cert Exam □ Exam SecOps-Pro Certification Cost □ SecOps-Pro Reliable Test Test □ Search for 「SecOps-Pro」 and download exam materials for free through ➽ www.pdfvce.com □ □Valid SecOps-Pro Exam Question
- Enhance Your Success Rate with www.testkingpass.com's Palo Alto Networks SecOps-Pro Exam Dumps □ Search for

□ SecOps-Pro □ and easily obtain a free download on ➥ www.testkingpass.com □ □SecOps-Pro Braindumps

- Palo Alto Networks Security Operations Professional sure pass dumps - SecOps-Pro actual training pdf □ Open ▷ www.pdfvce.com◁ and search for ✔ SecOps-Pro □✔□ to download exam materials for free □SecOps-Pro Test Discount Voucher
- SecOps-Pro Reliable Test Test □ SecOps-Pro Valid Test Sample ✈ Exam SecOps-Pro Questions □ Open website ➡ www.exam4labs.com □□□ and search for ☀ SecOps-Pro □☀□ for free download □SecOps-Pro Reliable Test Test
- SecOps-Pro EXAM DUMPS WITH GUARANTEED SUCCESS □ Search for □ SecOps-Pro □ and easily obtain a free download on 《 www.pdfvce.com 》 □Study SecOps-Pro Materials
- Palo Alto Networks Security Operations Professional practice vce dumps - SecOps-Pro latest exam guide - Palo Alto Networks Security Operations Professional test training torrent □ Download ➠ SecOps-Pro □ for free by simply searching on 「 www.vceengine.com 」 □Dump SecOps-Pro Collection
- SecOps-Pro Test Discount Voucher □ SecOps-Pro Valid Exam Tips □ Exam SecOps-Pro Questions □ Search for ➠ SecOps-Pro □ and obtain a free download on 《 www.pdfvce.com 》 □Exam SecOps-Pro Questions
- Authoritative New SecOps-Pro Exam Pdf Supply you Trusted Exam Simulator for SecOps-Pro: Palo Alto Networks Security Operations Professional to Prepare easily □ Open □ www.exam4labs.com □ enter □ SecOps-Pro □ and obtain a free download □SecOps-Pro Vce Exam
- 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, 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, classrooms.deaduniversity.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, cliqcourses.com, www.stes.tyc.edu.tw, Disposable vapes