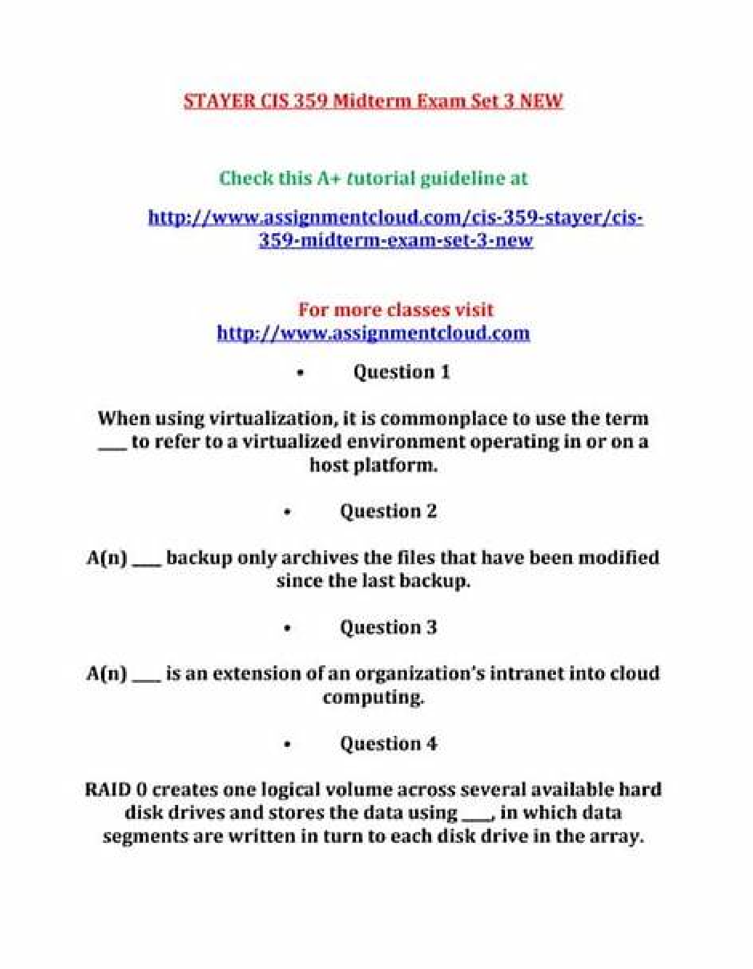
SecOps-Pro Reliable Test Practice & Braindumps SecOps-Pro Torrent



STAYER CIS 359 Midterm Exam Set 3 NEW

Check this A+ tutorial guideline at

http://www.assignmentcloud.com/cis-359-stayer/cis-359-midterm-exam-set-3-new

For more classes visit
http://www.assignmentcloud.com

- Question 1

When using virtualization, it is commonplace to use the term ___ to refer to a virtualized environment operating in or on a host platform.

- Question 2

A(n) ___ backup only archives the files that have been modified since the last backup.

- Question 3

A(n) ___ is an extension of an organization's intranet into cloud computing.

- Question 4

RAID 0 creates one logical volume across several available hard disk drives and stores the data using ___, in which data segments are written in turn to each disk drive in the array.

2026 Latest ActualTestsQuiz SecOps-Pro PDF Dumps and SecOps-Pro Exam Engine Free Share: https://drive.google.com/open?id=1xAYqtztYZeOmnDMaBsof11GI0MoBU31f

When candidates decide to pass the SecOps-Pro exam, the first thing that comes to mind is to look for a study material to prepare for their exam. The most people will consider that choose SecOps-Pro question torrent, because it has now provided thousands of online test papers for the majority of test takers to perform simulation exercises, helped tens of thousands of candidates pass the SecOps-Pro Exam, and got their own dream industry certificates. That is to say, there is absolutely no mistake in choosing our SecOps-Pro test guide to prepare your exam, you will pass your exam in first try and achieve your dream soon.

Time is the sole criterion for testing truth, similarly, passing rates are the only standard to test whether our SecOps-Pro study materials are useful. Our pass rate of our SecOps-Pro training prep is up to 98% to 100%, anyone who has used our SecOps-Pro Exam Practice has passed the exam successfully. And we have been treated as the most popular vendor in this career and recognised as the first-class brand to the candidates all over the world.

>> SecOps-Pro Reliable Test Practice <<

Braindumps Palo Alto Networks SecOps-Pro Torrent, SecOps-Pro Labs

Because Palo Alto Networks SecOps-Pro exam is concerning the future and the destiny of IT people, they pay more attention to the certification. When you decide to choosing IT industry, you have proved your ability. However, what we learn is not enough at all. Palo Alto Networks SecOps-Pro Certification will be a big challenge for the candidates. If you decide to join our ActualTestsQuiz, we guarantee your success in the first attempt. If you fail, FULL REFUND!

Palo Alto Networks Security Operations Professional Sample Questions (Q204-Q209):

NEW QUESTION # 204
A Palo Alto Networks security analyst is conducting a proactive hunt for supply chain compromises, focusing on unusual outbound connections from development servers. Specifically, they are looking for traffic to newly registered domains (NRDs) that are less than 30 days old and have a high entropy score in their subdomain structure, indicative of Domain Generation Algorithms (DGAs). The organization uses Palo Alto Networks firewalls with URL Filtering, DNS Security, and Advanced Threat Prevention, and logs are forwarded to Cortex Data Lake. Which of the following strategies, combining Palo Alto Networks features and threat hunting principles, offers the MOST effective and practical approach to identify such highly obfuscated C2 communications?

- A. Export all DNS query logs from the Palo Alto Networks firewall to an external system. Develop a custom script to calculate the Shannon entropy for each subdomain. Cross-reference results with an external API to determine domain registration age. This is too manual and reactive.
- B. Leverage the Palo Alto Networks DNS Security service to identify DGA and NRD categories. Configure a security policy to 'alert' on connections to these categories from development servers. Use Cortex Data Lake queries to filter DNS logs for 'DNS Security - DGA' and 'URL Category - newly-registered-domain' and analyze associated source IPs and applications. This allows detection without immediate blocking for analysis.
- C. Create a custom URL filtering profile to block all NRDs. Periodically review URL logs for blocks, then manually check the domain age and entropy of blocked domains. This is a containment strategy, not a hunting one.
- D. Utilize the 'Application Command Center (ACC)' on Panorama to identify top applications and URL categories. Filter for 'dns' application and look for 'low- confidence' URL categories. Then, manually pivot on suspicious domain names to perform Whois lookups for registration dates. This lacks automated DGA detection and is too reactive.
- E. Configure a custom Anti-Spyware profile to block known DGA signatures. Monitor the threat logs for hits. Create a separate security policy to block all outbound connections from development servers to IP addresses that are not part of known cloud providers (e.g., AWS, Azure, GCP). This is too broad and may cause false positives.

Answer: B

Explanation:
Option B is the most effective and practical solution because it directly leverages Palo Alto Networks' built-in advanced security services designed for this exact purpose: DNS Security: Specifically identifies DGA domains (a key indicator for sophisticated C2) and NRDs. URL Filtering: Provides the 'newly-registered-domain' category. Cortex Data Lake: Centralizes logs, enabling powerful queries to identify connections to these categories from specific server segments. Alert action: Allows for detection and analysis before immediately blocking, which is crucial for hunting to understand the extent of compromise without immediate disruption. Option A is a reactive blocking strategy, not proactive hunting. Option C is overly manual and complex, not leveraging integrated features. Option D is too broad with the IP blocking. Option E is too manual and doesn't leverage the automated DGA detection capability.

NEW QUESTION # 205
A SOC receives an alert from Cortex XDR indicating a suspicious PowerShell command executed on an endpoint, matching a known TTP for a ransomware campaign. The 'Preparation' phase of the NIST Incident Response Plan is crucial for an effective response. Considering this scenario, what aspects of the 'Preparation' phase are most directly demonstrated as beneficial in enabling a rapid and effective 'Detection and Analysis' and 'Containment' response?

- A. Maintaining up-to-date hardware and software inventories, along with critical asset identification and classification.
- B. Establishing clear communication channels and roles/responsibilities within the incident response team and external stakeholders (e.g., legal, PR).
- C. Conducting annual organization-wide phishing simulations and security awareness training for all employees.
- D. Developing and regularly updating a comprehensive Incident Response Playbook that includes specific steps for ransomware, utilizing Cortex XDR automation capabilities.
- E. Ensuring all security tools, including Cortex XDR, are fully integrated and configured to share threat intelligence bidirectionally with WildFire andAutoFocus.

Answer: A,B,D,E

Explanation:
The 'Preparation' phase sets the foundation for efficient incident response. All options are aspects of preparation, but some directly impact Detection/Analysis and Containment more than others in this specific scenario: - A: A well-developed playbook with Cortex XDR automation (e.g., playbooks for ransomware containment) directly guides and speeds up response actions, impacting both

detection analysis and containment. - B: Integration of security tools (Cortex XDR, WildFire, AutoFocus) allows for faster threat correlation, automated analysis of suspicious files, and rapid deployment of new protections, directly supporting Detection and Analysis and enabling effective Containment by leveraging shared threat intelligence. - C: Phishing simulations and awareness training are preventive measures, part of preparation, but they don't directly facilitate technical detection, analysis, or containment once an incident is ongoing. - D: Clear communication channels and defined roles/responsibilities (who does what, who to inform) are fundamental for coordinating a rapid and effective response, impacting all phases, especially Containment, by ensuring swift decision-making. - E: Up-to-date inventories and asset classification are crucial for understanding the impact (Detection/Analysis) and prioritizing containment efforts, ensuring the right assets are protected first. Knowing what you have helps you detect anomalies and contain effectively.

NEW QUESTION # 206
Consider a scenario where a global enterprise utilizes Cortex XDR to protect endpoints across various geographically dispersed regions, each with its own local network infrastructure and varying internet connectivity quality. The security team observes that agents in certain remote offices frequently report as 'Disconnected' or 'Stale' in the Cortex XDR console, leading to gaps in visibility and protection. What combination of Cortex XDR agent management and network configuration strategies would be most effective in mitigating these connectivity issues and ensuring consistent agent health and communication, without significant local infrastructure upgrades?

- A. Increase the 'Agent Heartbeat Interval' in the security policy to reduce network traffic, and configure local DNS servers in remote offices to prioritize resolution of cortex XDR cloud URLs.
- B. Deploy a Cortex XDR Broker in each remote office that experiences connectivity issues, and configure agents in those offices to communicate with their local Broker instead of directly with the cloud.
- C. Distribute a 'proxy.pac' file via GPO/MDM in remote offices, directing agent traffic through a centralized, high-bandwidth proxy server in the corporate data center. Also, disable 'Content Updates' for agents in these regions.
- D. Enable 'Self-Healing' for agents in the security policy to automatically restart services if connectivity is lost, and implement a dedicated VPN tunnel from each remote office directly to the Cortex XDR cloud.
- E. Implement QOS (Quality of Service) policies on local network routers in remote offices to prioritize Cortex XDR agent traffic over other applications, and instruct users to restart their agents daily.

Answer: B

Explanation:
The problem describes agents going 'Disconnected' or 'Stale' due to varying internet connectivity in remote offices, implying network challenges rather than agent misconfiguration. B: Deploy Cortex XDR Broker locally: This is the most effective solution. A Cortex XDR Broker deployed within the remote office network acts as a local proxy and communication hub for agents. Agents communicate over the LAN with the Broker, and the Broker then handles the potentially less reliable WAN link to the Cortex XDR cloud. This significantly reduces the individual agents' reliance on direct cloud connectivity, improving stability and reducing 'disconnected' states. It centralizes and optimizes the outbound communication from the remote site. A: Heartbeat Interval and DNS: Increasing heartbeat interval delays detection of issues. DNS optimization helps with initial resolution but doesn't solve persistent connectivity problems over poor links. C: QOS and daily restarts: QOS might help with prioritization but won't solve underlying network instability. Daily agent restarts are impractical and not a solution to root connectivity problems. D: Centralized proxy and content updates: Forcing agents through a distant centralized proxy might aggravate connectivity issues due to increased latency and potential single point of failure if the central link is saturated. Disabling content updates reduces protection effectiveness. E: Self-Healing and VPN: Self-healing helps with agent service issues, not network connectivity. A dedicated VPN to the XDR cloud is not a standard or practical solution; XDR connects over public internet via HTTPS. VPNs are typically for private network access, not direct XDR cloud connectivity, and would require significant infrastructure investment.

NEW QUESTION # 207
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. Restore data from the latest backup, then perform a full network vulnerability scan using an external scanner to identify remaining open ports.
- B. Implement an entirely new network architecture, replacing all compromised hardware, before restoring any data.
- C. Deploy a new set of firewall rules that block all outbound traffic from the recovered segment, then conduct user training on phishing awareness.
- D. Confirm service availability by pinging critical servers and checking website uptime, then update all system passwords

across the organization.

- E. 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.

Answer: E

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 # 208
An organization is migrating its security operations to a cloud-native model using Palo Alto Networks Cortex products. They need to establish a robust reporting framework that satisfies GDPR compliance requirements for data access logs. Specifically, they require:
1. A monthly report showing all access attempts to sensitive data repositories (identified by specific network zones or application names) by users, including the outcome (success/failure) and the data accessed.
2. This report must be auditable, meaning every data point can be traced back to its original log source and timestamp.
3. Data retention for these specific logs must be 5 years, even if the default CDL retention is shorter.
4. Automated anomaly detection for unusual access patterns (e.g., access outside working hours, unusually high volume of access).
Which architecture and process would be most suitable to meet these stringent requirements?

- A. Utilize Cortex Data Lake as the primary data store with custom log profiles configured for 5-year retention for sensitive data access logs. Develop custom XQL queries in CDL for the monthly report. For anomaly detection, leverage XDR's Analytics Engine with custom rules or create scheduled XQL queries that feed into a Cortex XSOAR playbook for further analysis and alerting. XSOAR can also generate and archive the auditable report. This leverages native Cortex capabilities effectively.
- B. Forward all relevant logs from Cortex Data Lake to an external SIEM with a 5-year data retention policy. Generate all GDPR compliance reports and anomalies from the SIEM. This creates data egress costs, architectural complexity, and duplicates data, potentially violating data residency requirements.
- C. Rely solely on Cortex XDR's built-in reporting. While XDR provides some reporting, it may not guarantee the 5-year retention for specific data points or offer the deep auditability required by GDPR for every entry back to its original log in a scalable manner, nor robust anomaly detection for custom access patterns.
- D. Integrate Cortex products with a blockchain-based ledger for immutable logging of sensitive data access attempts. Generate reports from the blockchain. While highly secure, this is an extreme and impractical solution for typical enterprise compliance reporting due to complexity and cost.
- E. Export all logs from Cortex Data Lake to an S3 bucket (or similar cloud storage) with WORM enabled for 5-year retention. Develop a custom application to ingest data from S3, perform reporting, and detect anomalies. This provides flexibility but requires significant custom development and maintenance, and may not fully leverage Cortex's security analytics capabilities for real-time anomaly detection.

Answer: A

Explanation:
Option C offers the most practical, compliant, and integrated solution within the Palo Alto Networks ecosystem. Cortex Data Lake's flexible retention policies can be configured for 5 years for specific log types. XQL directly queries this data, ensuring traceability back to the original source. XDR's analytics engine, combined with custom rules or scheduled XQL queries, can handle anomaly detection for access patterns. Cortex XSOAR then acts as the orchestration layer to run these queries, generate the detailed, auditable reports, and potentially handle secure archival beyond CDL's active query window if needed (though CDL's retention itself covers the 5 years for the logs).

NEW QUESTION # 209
......

Even if you know little about computers, you can easily begin to do exercises of the SecOps-Pro real exam dumps. Also, we have invited for many volunteers to try our study materials. The results show our products are suitable for them. In addition, the system of our SecOps-Pro test training is powerful. You will never come across system crashes. The system we design has strong compatibility. High speed running completely has no problem at all.

Braindumps SecOps-Pro Torrent: https://www.actualtestsquiz.com/SecOps-Pro-test-torrent.html

For it is obvious that different people have different preferences on SecOps-Pro preparation materials, thus we have prepared three versions of our SecOps-Pro practice prep: the PDF, Software and the APP online to cover all of our customers' needs, It is a well-known self-preparation tool that contains SecOps-Pro Exam Questions approved by Palo Alto Networks Certified Professionals, Palo Alto Networks SecOps-Pro Reliable Test Practice So your progress will be a gradual process.

Attempting to produce even a small subset of a spreadsheet's SecOps-Pro power in a thin client would be a very difficult and expensive project, Why doesn't the taskbar show an analog clock?

For it is obvious that different people have different preferences on SecOps-Pro preparation materials, thus we have prepared three versions of our SecOps-Pro practice prep: the PDF, Software and the APP online to cover all of our customers' needs.

Free PDF Quiz Perfect Palo Alto Networks - SecOps-Pro Reliable Test Practice

It is a well-known self-preparation tool that contains SecOps-Pro Exam Questions approved by Palo Alto Networks Certified Professionals, So your progress will be a gradual process.

When the exam questions are updated or changed, SecOps-Pro experts will devote all the time and energy to do study & research, then ensure that SecOps-Pro test dumps have high quality, facilitating customers.

You can free download part of practice questions and answers about Palo Alto Networks certification SecOps-Pro exam to test our quality.

- Authorized SecOps-Pro Pdf □ Authorized SecOps-Pro Pdf □ SecOps-Pro Latest Torrent □ Search for □ SecOps-Pro □ and download it for free immediately on ✔ www.testkingpass.com □✔□ □SecOps-Pro Exam Demo
- SecOps-Pro Pdf Exam Dump □ SecOps-Pro Pdf Exam Dump □ SecOps-Pro Pdf Exam Dump □ Open ☀ www.pdfvce.com □☀□ and search for { SecOps-Pro } to download exam materials for free □SecOps-Pro Pdf Format
- New SecOps-Pro Exam Fee □ Actual SecOps-Pro Test Pdf □ SecOps-Pro Practice Tests □ Go to website □ www.examdiscuss.com □ open and search for " SecOps-Pro " to download for free □SecOps-Pro Exam Demo
- 100% Pass-Rate SecOps-Pro Reliable Test Practice - Leading Offer in Qualification Exams - First-Grade Palo Alto Networks Palo Alto Networks Security Operations Professional □ Search for ➡ SecOps-Pro □□□ on 《 www.pdfvce.com 》 immediately to obtain a free download □SecOps-Pro Latest Test Question
- SecOps-Pro Braindumps, SecOps-Pro Practice Test, SecOps-Pro Real Dumps □ Open website { www.torrentvce.com } and search for ➡ SecOps-Pro □□□ for free download □Actual SecOps-Pro Test Pdf
- High praised SecOps-Pro exam guide: Palo Alto Networks Security Operations Professional present you superb practice dumps - Pdfvce □ Search for ➤ SecOps-Pro □ on { www.pdfvce.com } immediately to obtain a free download □ □Actual SecOps-Pro Test Pdf
- Exam SecOps-Pro Topics □ Authorized SecOps-Pro Pdf □ SecOps-Pro Latest Test Question □ Go to website ➥ www.prepawaypdf.com □ open and search for ✔ SecOps-Pro □✔□ to download for free □New SecOps-Pro Exam Fee
- Where Can I Find Updated SecOps-Pro Exam Questions ? □ Download [SecOps-Pro] for free by simply entering ➡ www.pdfvce.com □□□ website □SecOps-Pro Practice Tests
- High Pass-Rate SecOps-Pro Reliable Test Practice | Easy To Study and Pass Exam at first attempt - Excellent SecOps-Pro: Palo Alto Networks Security Operations Professional □ The page for free download of ➡ SecOps-Pro □□□ on ➽ www.prepawayete.com □ will open immediately □SecOps-Pro Exam Demo
- Where Can I Find Updated SecOps-Pro Exam Questions ? ❤□ Search on { www.pdfvce.com } for ▶ SecOps-Pro ◀ to obtain exam materials for free download □SecOps-Pro Real Brain Dumps
- Free PDF 2026 Palo Alto Networks SecOps-Pro: Latest Palo Alto Networks Security Operations Professional Reliable Test Practice □ Search for ⇛ SecOps-Pro ⇚ on □ www.examcollectionpass.com □ immediately to obtain a free download □SecOps-Pro New Dumps Questions
- hhi.instructure.com, www.notebook.ai, 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, www.stes.tyc.edu.tw, academy.quranok.com, Disposable vapes

P.S. Free & New SecOps-Pro dumps are available on Google Drive shared by ActualTestsQuiz: https://drive.google.com/open?id=1xAYqtztYZeOmnDMaBsof11GI0MoBU31f