NetSec-Analyst높은통과율인기시험자료100%합격보장가능한최신공부자료

참고: DumpTOP에서 Google Drive로 공유하는 무료, 최신 NetSec-Analyst 시험 문제집이 있습니다: https://drive.google.com/open?id=1TBGtoyRFyBVqJYxiK-yd0v90G1aK62qG

DumpTOP의 Palo Alto Networks 인증 NetSec-Analyst시험덤프공부자료는 pdf버전과 소프트웨어버전 두가지 버전으로 제공되는데 Palo Alto Networks 인증 NetSec-Analyst실제시험예상문제가 포함되어있습니다.덤프의 예상문제는 Palo Alto Networks 인증 NetSec-Analyst실제시험의 대부분 문제를 적중하여 높은 통과율과 점유율을 자랑하고 있습니다. DumpTOP의 Palo Alto Networks 인증 NetSec-Analyst덤프를 선택하시면 IT자격증 취득에 더할것 없는 힘이 될것입니다.

Palo Alto Networks NetSec-Analyst 시험요강:

주제	소개
주제 1	• Troubleshooting: This section of the exam measures the skills of Technical Support Analysts and covers the identification and resolution of configuration and operational issues. It includes troubleshooting misconfigurations, runtime errors, commit and push issues, device health concerns, and resource usage problems. This domain ensures candidates can analyze failures across management systems and on-device functions, enabling them to maintain a stable and reliable security infrastructure.
주제 2	• Policy Creation and Application: This section of the exam measures the abilities of Firewall Administrators and focuses on creating and applying different types of policies essential to secure and manage traffic. The domain includes security policies incorporating App-ID, User-ID, and Content-ID, as well as NAT, decryption, application override, and policy-based forwarding policies. It also covers SD-WAN routing and SLA policies that influence how traffic flows across distributed environments. The section ensures professionals can design and implement policy structures that support secure, efficient network operations.
주제 3	• Object Configuration Creation and Application: This section of the exam measures the skills of Network Security Analysts and covers the creation, configuration, and application of objects used across security environments. It focuses on building and applying various security profiles, decryption profiles, custom objects, external dynamic lists, and log forwarding profiles. Candidates are expected to understand how data security, IoT security, DoS protection, and SD-WAN profiles integrate into firewall operations. The objective of this domain is to ensure analysts can configure the foundational elements required to protect and optimize network security using Strata Cloud Manager.

주제 4	• Management and Operations: This section of the exam measures the skills of Security Operations Professionals and covers the use of centralized management tools to maintain and monitor firewall environments. It focuses on Strata Cloud Manager, folders, snippets, automations, variables, and logging services. Candidates are also tested on using Command Center, Activity Insights, Policy Optimizer, Log Viewer, and incident-handling tools to analyze security data and improve the organization overall security posture. The goal is to validate competence in managing day-to-day firewall operations and responding to alerts effectively.

최신 NetSec-Analyst높은 통과율 인기 시험자료 공부자료

DumpTOP는 고객님께서 첫번째Palo Alto Networks NetSec-Analyst시험에서 패스할수 있도록 최선을 다하고 있습니다. 만일 어떤 이유로 인해 고객이 첫 번째 시도에서 실패를 한다면, DumpTOP는 고객에게Palo Alto Networks NetSec-Analyst덤프비용 전액을 환불 해드립니다.환불보상은 다음의 필수적인 정보들을 전제로 합니다.

최신 Network Security Administrator NetSec-Analyst 무료샘플문제 (Q269-Q274):

질문 # 269
An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

- A. Security policy = deny. Gambling category in URL profile = block
- B. Security policy = allow, Gambling category in URL profile = alert
- C. Security policy = drop, Gambling category in URL profile = allow
- D. Security policy = allow. Gambling category in URL profile = allow

정답：B

질문 # 270
Consider an environment where new IoT devices are frequently onboarded. The security team wants to automate the process of categorizing these devices and applying appropriate security policies. Which Palo Alto Networks feature, often integrated with an IoT Security Profile, allows for dynamic device classification and policy enforcement without manual intervention for each new device?

- A. External Dynamic Lists (EDLs) populated with known IoT device IP addresses.
- B. Security profiles based on Source/Destination IP addresses and Service ports only.
- C. Static MAC Address Filtering and a default 'Any-Any' security rule.
- D. User-ID and Group Mapping to assign IoT devices to specific user groups.
- E. IoT Security with Device-ID and IoT Device Groups, dynamically populated by the firewall's visibility engine or third-party IoT security platforms (e.g., Zingbox, now part of Palo Alto Networks).

정답：E

설명：
Option C is the most effective. Palo Alto Networks' IoT Security solution, powered by Device-ID and integration with specialized IoT security platforms, can automatically discover, classify, and group IoT devices based on their attributes (vendor, model, OS, observed behavior, etc.). These dynamically populated 'IoT Device Groups' can then be used as source/destination objects in security policies, allowing for automated and context-aware policy enforcement as new devices are onboarded. Options A, B, D, and E are either manual, lack device context, or are not designed for dynamic IoT device classification.

질문 # 271
A security auditor requires proof that all outbound DNS traffic from internal networks is strictly controlled and only allowed to specific, approved internal DNS servers. The auditor is concerned about DNS exfiltration. Which Command Center dashboard and

subsequent Policy Optimizer action would best demonstrate this control and harden the posture?

- A. Command Center: 'Network Activity' dashboard, filtering for destination port 53 and reviewing destination IP addresses. Policy Optimizer: Use 'Rule Usage' to identify rules allowing DNS to unapproved destinations and then restrict them.
- B. Command Center: 'Threat Activity' dashboard for DNS-related threats. Policy Optimizer: Apply a DNS Security profile to all outbound rules.
- C. Command Center: 'User Activity' for DNS queries. Policy Optimizer: Enable DNS Sinkholing on all zones.
- D. Command Center: 'Application Usage' dashboard filtered by 'DNS'. Policy Optimizer: Identify and delete unused DNS rules.
- E. Command Center: 'Top Applications' dashboard for DNS. Policy Optimizer: Reorder DNS rules to ensure specific allow rules are at the top.

정답：A

설명:
To prove strict control over outbound DNS, the 'Network Activity' dashboard in Command Center, filtered by destination port 53, allows the analyst to see exactly where DNS queries are going. This directly addresses the auditor's concern about unapproved destinations. Subsequently, Policy Optimizer's 'Rule Usage' feature helps pinpoint which specific rules are permitting this traffic, allowing for targeted modification or restriction to only approved internal DNS servers, thereby hardening the posture against exfiltration.

질문 # 272
Which feature would be useful for preventing traffic from hosting providers that place few restrictions on content, whose services are frequently used by attackers to distribute illegal or unethical material?

- A. Palo Alto Networks Known Malicious IP Addresses
- B. Palo Alto Networks Bulletproof IP Addresses
- C. Palo Alto Networks High-Risk IP Addresses
- D. Palo Alto Networks C&C IP Addresses

정답：B

설명:
To block hosts that use bulletproof hosts to provide malicious, illegal, and/or unethical content, use the bulletproof IP address list in policy.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for- bulletproof-isps#:~:text=A%20new%20built%2Din%20external,%2C%20illegal%2C%20and%20unethical%20content.

질문 # 273
A financial institution is under strict regulatory compliance to ensure that all sensitive data egress is inspected by a Data Loss Prevention (DLP) profile and that no unapproved services or applications are running on critical database servers. After initial policy deployment, the CISO demands real-time verification of DLP effectiveness and continuous assurance that only whitelisted applications are active on the database segment. How can Command Center and Activity Insights best be leveraged to meet these stringent requirements?

- A. Command Center: Check 'Policy Hit Counts' for DLP rules. Activity Insights: Review 'Bandwidth Usage' for database traffic.
- B. Command Center: Review 'System Logs' for DLP incidents. Activity Insights: Provide a historical view of application usage on database servers.
- C. Command Center: Create a custom widget to display sessions with 'data-filtering' security profile matches, specifically for traffic from database servers. Set up an alert for 'unknown' applications from the database segment. Activity Insights: Use 'Application Filters' to create a baseline of approved applications for the database segment and alert on deviations.
- D. Command Center: Monitor the 'URL Filtering' dashboard for sensitive data patterns. Activity Insights: Use 'User Activity' to track who is accessing database servers.
- E. Command Center: Monitor 'Threat Activity' for DLP alerts and 'Application Usage' for top applications. Activity Insights: Generate reports on overall DLP policy hit counts.

정답：C

설명：
This question focuses on real-time verification and continuous assurance. Command Center's ability to create custom widgets allows for specific monitoring of DLP profile matches on critical traffic flows (e.g., from database servers). Critically, setting up alerts for 'unknown' applications from the database segment provides real-time notification of deviations from the approved whitelist. Activity Insights, while generally for historical trends, can be used to establish a baseline of approved applications through its 'Application Filters' and then trigger alerts (often integrated with logging/SIEM) when applications outside this baseline are observed, providing continuous assurance.

질문 # 274
.....