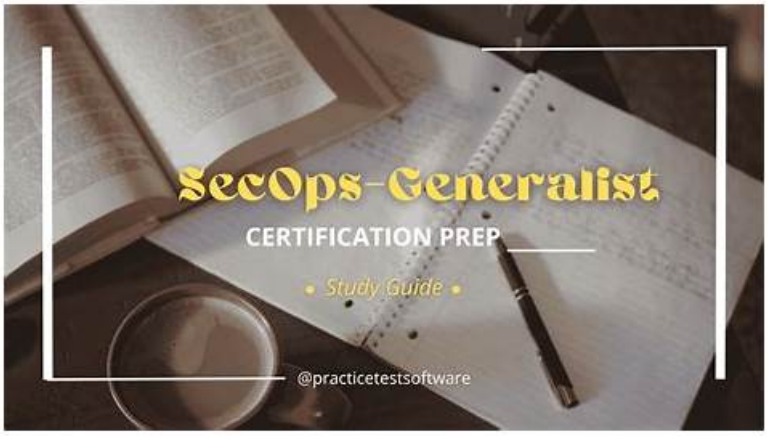
SecOps-Generalist Excellect Pass Rate - Latest SecOps-Generalist Test Voucher



If you prepare for the SecOps-Generalist exam using our TrainingQuiz testing engine, it is easy and convenient to buy. Just two steps to complete your purchase, we will send the SecOps-Generalist product to your mailbox quickly. And you only need to download e-mail attachments to get your products.

Nowadays the test SecOps-Generalist certificate is more and more important because if you pass it you will improve your abilities and your stocks of knowledge in some certain area and find a good job with high pay. If you buy our SecOps-Generalist exam materials you can pass the exam easily and successfully. Our SecOps-Generalist Exam Materials boost high passing rate and if you are unfortunate to fail in exam we can refund you in full at one time immediately. The learning costs you little time and energy and you can commit yourself mainly to your jobs or other important things.

>> SecOps-Generalist Excellect Pass Rate <<

Latest SecOps-Generalist Test Voucher & Exam SecOps-Generalist Review

Our SecOps-Generalist study materials have won many people's strong support. And our SecOps-Generalist learning quiz is famous all over the world. Now, our loyal customers have gained wealth and respect with the guidance of our SecOps-Generalist learning materials. At the same time, the price is not so high. You totally can afford them. Do not make excuses for your laziness. Please take immediate actions. Our SecOps-Generalist Study Guide is extremely superior.

Palo Alto Networks Security Operations Generalist Sample Questions (Q37-Q42):

NEW QUESTION # 37
An organization uses Prisma Access for mobile users and logs to Cortex Data Lake. A user reports slow performance when accessing a SaaS application. The administrator suspects network latency between the user and the closest Prisma Access location or between Prisma Access and the SaaS provider, or potentially high load on the assigned Prisma Access node. Which log types or monitoring views in Cortex Data Lake or the Cloud Management Console could help diagnose these potential performance bottlenecks? (Select all that apply)

- A. Performance monitoring views in the Cloud Management Console showing metrics for the user's connected Prisma Access location (e.g., resource utilization, latency to internet/service connections).
- B. Traffic logs showing the session details for the SaaS application, including bytes transferred and session duration, correlated with timestamps.
- C. System logs on the Prisma Access service edge showing daemon restarts or critical errors.
- D. Application Performance Monitoring (APM) data (if applicable) showing latency and performance specific to the SaaS application over the Prisma Access path.
- E. GlobalProtect logs, specifically looking for login success/failure and gateway assignment.

Answer: A,B,C,D

Explanation:
Troubleshooting performance in a SASE environment involves looking at network path performance, application performance metrics, resource utilization, and session details. - Option A: GlobalProtect logs confirm connection status but don't show performance within the tunnel. - Option B (Correct): Monitoring views showing performance metrics for the Prisma Access location itself provide insight into potential bottlenecks at the cloud edge or connectivity issues from the edge to destinations. - Option C (Correct): Traffic logs, when analyzed for session duration relative to bytes transferred, can indicate slowness (e.g., long duration for small data transfer). While not showing latency directly, they provide session activity context. - Option D (Correct): APM data is specifically designed to measure application performance over the network, showing latency and other quality metrics from the user to the application. - Option E (Correct): System logs can indicate if the underlying Prisma Access node handling the user's traffic is experiencing issues (high CPU, memory pressure, restarts) that would impact performance.

NEW QUESTION # 38
Causality View in Cortex XDR provides analysts with:
Response:

- A. Automatic remediation capabilities for all detected threats
- B. The ability to ignore false positives without investigation
- C. A visual representation of how a security event evolved over time
- D. A simple list of alert logs without additional correlation

Answer: C

NEW QUESTION # 39
An organization is configuring Security Policy rules on a Palo Alto Networks VM-Series firewall in a public cloud environment (e.g., AWS VPC) to segment application tiers. They have zones for 'Web-Tier', 'App-Tier', and 'DB-Tier'. They need to allow HTTP/HTTPS traffic from 'Web-Tier' to 'App-Tier' but apply deep threat inspection. They also need to allow database traffic (MS-SQL, MySQL) from 'App-Tier' to 'DB-Tier' but only for specific application servers. Which policy elements and configurations are essential for implementing these requirements? (Select all that apply)

- A. Decryption Policy rule to decrypt HTTP/HTTPS traffic flowing from 'Web-Tier' to 'App-Tier'.
- B. User-ID configured to identify users accessing applications within the tiers.
- C. NAT policy rules configured for traffic between application tiers to translate private IP addresses.
- D. Security Policy rule: Source Zone 'Web-Tier', Destination Zone 'App-Tier', Application 'web-browsing' (or 'http', 'ssl'), Action 'allow', apply relevant Threat Prevention profile.
- E. Security Policy rule: Source Zone 'App-Tier', Destination Zone 'DB-Tier', Source Address 'Specific App Server Address Group', Application 'ms-sql', 'mysql', Action 'allow', apply relevant security profiles (optional but recommended).

Answer: A,D,E

Explanation:
Segmenting traffic between application tiers requires defining policies based on zones, applications, and sources, and applying inspection. - Option A (Correct): This defines the rule for Web-Tier to App-Tier traffic, using zones, common web applications, and applying a Threat Prevention profile for inspection. - Option B (Correct): This defines the rule for App-Tier to DB-Tier traffic, specifying the source zone, destination zone, using an Address Group for the specific allowed servers, and using App-IDs for the database protocols. Applying security profiles (like Threat Prevention) to database traffic is also a best practice for detecting potential exploits or C2 over these protocols. - Option C (Correct): Deep threat inspection on HTTPS traffic requires decryption. A Decryption policy rule matching traffic between 'Web-Tier' and 'App-Tier' for HTTPS (ssl service) is necessary to enable Content-ID inspection by profiles like Threat Prevention and WildFire. - Option D (Incorrect): NAT is generally not needed for internal segmentation traffic using private, routable IP addresses within the same VPC/network space, unless there's a specific requirement for address translation between segments (which is uncommon in simple tier egmentation). - Option E (Optional but not essential for the described policy): User-ID provides user context but is not strictly necessary for policies based on application tiers and server addresses, unless the requirement was to allow access based on user identity accessing resources within those tiers.

NEW QUESTION # 40
An organization uses numerous SaaS applications (e.g., Office 365, Salesforce, Slack). They want to gain granular visibility into which specific functions within these applications users are accessing (e.g., posting a message in Slack, uploading a file to OneDrive, viewing a record in Salesforce) and enforce policies based on these actions. Which Palo Alto Networks feature, extended by

CDSS, provides the capability to identify these specific activities within a SaaS application?

- A. Threat Prevention signatures
- B. Service ports and protocols
- C. URL Filtering categories
- D. Data Filtering patterns
- E. App-ID and Application Function Control

Answer: E

Explanation:
Palo Alto Networks App-ID goes beyond identifying the base application (like 'slack'). It can identify specific functions or activities within many applications, known as application functions (e.g., 'slack-post', 'onedrive-upload', 'salesforce-view'). The Application Function Control feature in security policy allows administrators to permit or deny these specific actions. Option A categorizes websites but doesn't see actions within. Option B looks for data patterns. Option D is basic L4 control. Option E detects threats, not specific application activities.

NEW QUESTION # 41
An administrator is reviewing Data Filtering logs and observes a large number of 'alert' actions triggered for sensitive data patterns being detected in traffic to a sanctioned cloud storage service. They want to understand if the sensitive data was actually uploaded successfully despite the alert. Which other log type is essential to correlate with the Data Filtering logs to confirm if the upload session was allowed by the security policy?

- A. System logs
- B. Threat logs
- C. Traffic logs
- D. URL Filtering logs
- E. Decryption logs

Answer: C

Explanation:
Data Filtering logs show that a sensitive data match occurred and the action taken by the Data Filtering profile (alert or block). To know if the overall session that carried this data was allowed or denied by the firewall's security policy, you need to check the Traffic logs. - Option A: Threat logs are for malware/exploits. - Option B: System logs are for firewall health. - Option C (Correct): Traffic logs record every session and the action taken by the Security Policy rule (allow, deny, drop, reset). Correlating the session ID from the Data Filtering log with the Traffic log entry for the same session will show if the session was ultimately allowed to complete, indicating a successful upload despite the DLP alert. - Option D: Decryption logs confirm if the session was decrypted, necessary for DLP, but not whether the session was allowed by security policy. - Option E: URL Filtering logs track web access actions.

NEW QUESTION # 42
.....

Free PDF Palo Alto Networks - Newest SecOps-Generalist Excellect Pass Rate

Save time and money most people choose to join the training institution to struggle for SecOps-Generalist actual test, you can learn the key knowledge of SecOps-Generalist exam collection directly and intensively.

As the development of the technology, many companies SecOps-Generalist have higher requirement and the demand for the employee with skills and technology, You are ready to get highest score in SecOps-Generalist actual test if you are using our latest Palo Alto Networks pass test guaranteed pass test guaranteed for your assistance.

- SecOps-Generalist Reliable Exam Tutorial □ Interactive SecOps-Generalist Practice Exam □ Reliable SecOps-Generalist Test Dumps □ Easily obtain free download of " SecOps-Generalist " by searching on ➥ www.prepawaypdf.com □ □New SecOps-Generalist Exam Practice
- Pdf SecOps-Generalist Torrent □ SecOps-Generalist Instant Discount □ SecOps-Generalist Online Test □ Immediately open 【 www.pdfvce.com 】 and search for 《 SecOps-Generalist 》 to obtain a free download □SecOps-Generalist Instant Discount
- Valid SecOps-Generalist Study Notes □ Free SecOps-Generalist Test Questions □ SecOps-Generalist Latest Exam Book ☀ Download ➥ SecOps-Generalist □ for free by simply searching on ➤ www.prep4sures.top □ □SecOps-Generalist Instant Discount
- Valid SecOps-Generalist Test Simulator □ New SecOps-Generalist Exam Practice □ SecOps-Generalist Certification Questions □ Search on ⇛ www.pdfvce.com ⇚ for （ SecOps-Generalist ） to obtain exam materials for free download □ □SecOps-Generalist Reliable Exam Tutorial
- New SecOps-Generalist Exam Practice □ Reliable SecOps-Generalist Test Objectives □ Valid SecOps-Generalist Test Simulator □ Search for ➥ SecOps-Generalist □ and obtain a free download on ⇛ www.examcollectionpass.com ⇚ □ □Reliable SecOps-Generalist Test Objectives
- Tips to Crack the SecOps-Generalist Exam □ Search for 《 SecOps-Generalist 》 and obtain a free download on ☀ www.pdfvce.com □☀□ □SecOps-Generalist Valid Test Vce Free
- SecOps-Generalist Online Test □ SecOps-Generalist Exam Voucher □ SecOps-Generalist Reliable Exam Tutorial □ Copy URL ▹ www.pdfdumps.com ◃ open and search for ⇛ SecOps-Generalist ⇚ to download for free □SecOps-Generalist Latest Test Dumps
- Pdf SecOps-Generalist Torrent □ Pass SecOps-Generalist Guarantee □ SecOps-Generalist Latest Exam Book □ Search for （ SecOps-Generalist ） and obtain a free download on ➤ www.pdfvce.com □ □Reliable SecOps-Generalist Test Dumps
- SecOps-Generalist Valid Test Vce Free □ Unlimited SecOps-Generalist Exam Practice ◂ Pdf SecOps-Generalist Torrent □ Download □ SecOps-Generalist □ for free by simply searching on （ www.validtorrent.com ） □Unlimited SecOps-Generalist Exam Practice
- SecOps-Generalist Certification Questions □ SecOps-Generalist Exam Voucher □ Pdf SecOps-Generalist Torrent □ Simply search for ⇛ SecOps-Generalist ⇚ for free download on □ www.pdfvce.com □ □SecOps-Generalist Instant Discount
- SecOps-Generalist Instant Discount □ Free SecOps-Generalist Test Questions □ Free SecOps-Generalist Test Questions □ Download [SecOps-Generalist] for free by simply searching on ☀ www.prepawayete.com □☀□ □Pdf SecOps-Generalist Torrent
- 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, 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, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, bbs.t-firefly.com, Disposable vapes