Hot Current Cybersecurity-Practitioner Exam Content– High-quality Reliable Study Questions Providers for Palo Alto Networks Cybersecurity-Practitioner

BONUS!!! Download part of TestBraindump Cybersecurity-Practitioner dumps for free: https://drive.google.com/open?id=1kCOBE0Fpr_jq5brMVuXLAJ5Hn2rsrrG2

The software keeps track of the previous Palo Alto Networks Cybersecurity Practitioner (Cybersecurity-Practitioner) practice exam attempts and shows the changes of each attempt. You don't need to wait days or weeks to get your performance report. The software displays the result of the Palo Alto Networks Cybersecurity-Practitioner Practice Test immediately, which is an excellent way to understand which area needs more attention.

The company is preparing for the test candidates to prepare the Cybersecurity-Practitioner Study Materials professional brand, designed to be the most effective and easiest way to help users through their want to get the test Cybersecurity-Practitioner certification and obtain the relevant certification. In comparison with similar educational products, our training materials are of superior quality and reasonable price, so our company has become the top enterprise in the international market.

>> Current Cybersecurity-Practitioner Exam Content <<

Become Proficient to Pass the Exam with Updated Cybersecurity-Practitioner Exam Dumps

Even the fierce competition cannot stop demanding needs from exam candidates. To get more specific information about our Cybersecurity-Practitioner learning quiz, we are here to satisfy your wish with following details. So you can get detailed information with traits and information about our Cybersecurity-Practitioner Real Exam requested on the website. You can free download the demos of our Cybersecurity-Practitioner exam questions and click on every detail that you are interested.

Palo Alto Networks Cybersecurity-Practitioner Exam Syllabus Topics:

Topic	Details
Topic 1	• Secure Access: This domain examines SASE and SSE architectures, security challenges for data and applications including AI tools, and technologies like Secure Web Gateway, CASB, DLP, Remote Browser Isolation, SD-WAN, and Prisma SASE solutions.
Topic 2	• Security Operations: This domain focuses on security operations including threat hunting, incident response, SIEM and SOAR platforms, Attack Surface Management, and Cortex solutions including XSOAR, Xpanse, and XSIAM.
Topic 3	• Network Security: This domain addresses network protection through Zero Trust Network Access, firewalls, microsegmentation, and security technologies like IPS, URL filtering, DNS security, VPN, and SSL • TLS decryption, plus OT • IoT concerns, NGFW deployments, Cloud-Delivered Security Services, and Precision AI.
Topic 4	• Endpoint Security: This domain addresses endpoint protection including indicators of compromise, limitations of signature-based anti-malware, UEBA, EDR • XDR, Behavioral Threat Prevention, endpoint security technologies like host firewalls and disk encryption, and Cortex XDR features.
Topic 5	• Cybersecurity: This domain covers foundational security concepts including AAA framework, MITRE ATT&CK techniques, Zero Trust principles, advanced persistent threats, and common security technologies like IAM, MFA, mobile device management, and secure email gateways.

Palo Alto Networks Cybersecurity Practitioner Sample Questions (Q38-Q43):

NEW QUESTION # 38
In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

- A. reconnaissance
- B. delivery
- C. exploitation
- D. weaponization

Answer: D

Explanation:
"Weaponization: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message."

NEW QUESTION # 39
Which two statements describe the Jasager attack? (Choose two.)

- A. The victim must manually choose the attacker s access point
- B. It actively responds to beacon reguests.
- C. It tries to get victims to conned at random.
- D. The attacker needs to be wilhin close proximity of the victim.

Answer: B,D

Explanation:
A Jasager attack is a type of wireless man-in-the-middle attack that exploits the way mobile devices search for known wireless networks. A Jasager device will respond to any beacon request from a mobile device by saying "Yes, I'm here", pretending to be one of the preferred networks. This way, the Jasager device can trick the mobile device into connecting to it, without the user's knowledge or consent. The Jasager device can then intercept, modify, or redirect the traffic of the victim. For this attack to work, the attacker needs to be within close proximity of the victim, and the victim must have at least one known network in their preferred list. The victim does not need to manually choose the attacker's access point, nor does the attacker try to get victims to connect at random. Reference: Wireless Man in the Middle - Palo Alto Networks, Man-in-the-middle attacks with malicious & rogue Wi-Fi access points - Privacy Guides

NEW QUESTION # 40
Which action must Secunty Operations take when dealing with a known attack?

- A. Disclose details of lhe attack in accordance with regulatory standards.
- B. Increase the granularity of the application firewall.
- C. Limit the scope of who knows about the incident.
- D. Document, monitor, and track the incident.

Answer: D

Explanation:
Security Operations (SecOps) is the process of coordinating and aligning security teams and IT teams to improve the security posture of an organization. SecOps involves implementing and maintaining security controls, technologies, policies, and procedures to protect the organization from cyber threats and incidents. When dealing with a known attack, SecOps must take the following action: document, monitor, and track the incident. This action is important because it helps SecOps to:
* Record the details of the attack, such as the source, target, impact, timeline, and response actions.
* Monitor the status and progress of the incident response and recovery efforts, as well as the ongoing threat activity and indicators of compromise.
* Track the performance and effectiveness of the security controls and technologies, as well as the lessons learned and improvement opportunities. Reference:
* Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)
* 6 Incident Response Steps to Take After a Security Event - Exabeam
* Dealing with Cyber Attacks-Steps You Need to Know | NIST

NEW QUESTION # 41
What differentiates SOAR from SIEM?

- A. SOAR platforms collect data and send alerts.
- B. SOAR platforms focus on analyzing network traffic.
- C. SOAR platforms filter alerts with their broader coverage of security incidents.
- D. SOAR platforms integrate automated response into the investigation process.

Answer: D

Explanation:
SOAR (Security Orchestration, Automation, and Response) differs from SIEM by adding automated incident response and workflow orchestration to the detection and alerting capabilities found in SIEM. This enables faster and more efficient handling of security incidents.

NEW QUESTION # 42
Which technique changes protocols at random during a session?

- A. use of non-standard ports
- B. hiding within SSL encryption
- C. tunneling within commonly used services
- D. port hopping

Answer: D

Explanation:
Port hopping is a technique that changes protocols at random during a session to evade detection and analysis by security devices. Port hopping can be used by malware or attackers to communicate with command and control servers or to exfiltrate data. Port hopping makes it difficult to identify and block malicious traffic based on port numbers or signatures. Reference: Port Hopping, Ports Used for Management Functions, Adding a Custom Application/Ports to Security Policy

NEW QUESTION # 43
.....

Through years of marketing, our Cybersecurity-Practitioner latest certification guide has won the support of many customers. The most obvious data is that our products are gradually increasing each year, and it is a great effort to achieve such a huge success thanks to our product development. First of all, we have done a very good job in studying the updating of materials. In addition, the quality of our Cybersecurity-Practitioner real study braindumps is strictly controlled by teachers. So, believe that we are the right choice, if you have any questions about our study materials, you can consult us.

BTW, DOWNLOAD part of TestBraindump Cybersecurity-Practitioner dumps from Cloud Storage: https://drive.google.com/open?id=1kCOBE0Fpr_jq5brMVuXLAJ5Hn2rsrrG2