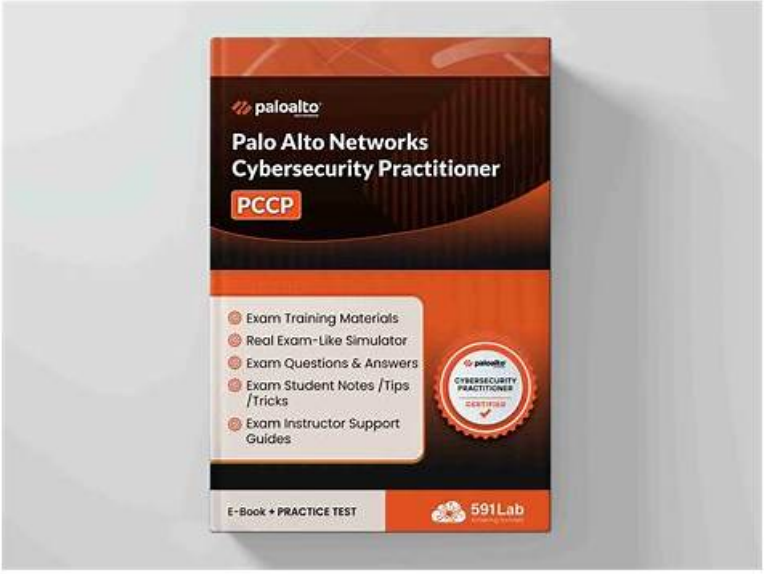
TOP Cybersecurity-Practitioner Latest Exam Online - Valid Palo Alto Networks Test Cybersecurity-Practitioner Simulator Free: Palo Alto Networks Cybersecurity Practitioner



Through our investigation and analysis of the real problem over the years, our Cybersecurity-Practitioner prepare questions can accurately predict the annual Cybersecurity-Practitioner exams. And the Cybersecurity-Practitioner quiz guide's experts still have the ability to master propositional trends. Believe that such a high hit rate can better help users in the review process to build confidence, and finally help users through the qualification examination to obtain a certificate. All in all, we want you to have the courage to challenge yourself, and our Cybersecurity-Practitioner Exam Prep will do the best for the user's expectations.

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	• 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.
Topic 5	• 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.

>> Cybersecurity-Practitioner Latest Exam Online <<

Palo Alto Networks Cybersecurity-Practitioner Pdf Questions - Outstanding Practice To your Palo Alto Networks Cybersecurity Practitioner Exam

The content system of Cybersecurity-Practitioner exam simulation is constructed by experts. After-sales service of our study materials is also provided by professionals. If you encounter some problems when using our Cybersecurity-Practitioner study materials, you can also get them at any time. After you choose Cybersecurity-Practitioner Preparation questions, professional services will enable you to use it in the way that suits you best, truly making the best use of it, and bringing you the best learning results.

Palo Alto Networks Cybersecurity Practitioner Sample Questions (Q191-Q196):

NEW QUESTION # 191
Which type of malware replicates itself to spread rapidly through a computer network?

- A. ransomware
- B. virus
- C. worm
- D. Trojan horse

Answer: C

Explanation:
A worm is a type of malware that replicates itself to spread rapidly through a computer network. Unlike a virus, a worm does not need a host program or human interaction to infect other devices. A worm can consume network bandwidth, slow down the system performance, or deliver a malicious payload, such as ransomware or a backdoor123. Reference: Types of Malware & Malware Examples - Kaspersky, 10 types of malware + how to prevent malware from the start, Computer worm - Wikipedia A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

NEW QUESTION # 192
Which tool automates remediation of a confirmed cybersecurity breach?

- A. SOAR
- B. EDR
- C. SIEM
- D. ISIM

Answer: A

Explanation:
Security Orchestration, Automation, and Response (SOAR) platforms are designed to automate the remediation of confirmed cybersecurity breaches by executing predefined response playbooks, reducing response time and manual effort during incidents.

NEW QUESTION # 193
Which feature of the VM-Series firewalls allows them to fully integrate into the DevOps workflows and CI/CD pipelines without slowing the pace of business?

- A. Log export
- B. External dynamic lists
- C. 5G
- D. Elastic scalability

Answer: D

Explanation:
Elastic scalability is the feature of the VM-Series firewalls that allows them to fully integrate into the DevOps workflows and CI/CD pipelines without slowing the pace of business. Elastic scalability means that the VM-Series firewalls can automatically adjust their capacity and performance based on the changing demand and workload of the applications they protect. This enables the VM-Series firewalls to provide consistent and optimal security across multiple cloud environments, while also reducing operational costs and complexity. Elastic scalability also allows the VM-Series firewalls to seamlessly integrate with automation and orchestration tools, such as Terraform, Ansible, and AWS CloudFormation, that are commonly used in DevOps processes. This way, the VM-Series firewalls can be deployed and managed as part of the application development lifecycle and CI/CD pipelines, ensuring that security is always aligned with the business needs and objectives. Reference: VM-Series Virtual Next-Generation Firewall - Palo Alto Networks, Securing Multi-Cloud Environments with VM-Series Virtual Firewalls, Terraform Modules for Palo Alto Networks VM-Series on AWS.

NEW QUESTION # 194
With regard to cloud-native security in layers, what is the correct order of the four C's from the top (surface) layer to the bottom (base) layer?

- A. container, code, cluster, cloud
- B. code, container, cloud, cluster
- C. container, code, cloud, cluster
- D. code, container, cluster, cloud

Answer: D

Explanation:
Cloud-native security is the integration of security strategies into applications and systems designed to be deployed and to run in cloud environments. It involves a layered approach that considers security at every level of the cloud-native application architecture. The four C's of cloud-native security are123:
Code: This layer refers to the application code and its dependencies. Security at this layer involves ensuring the code is free of vulnerabilities, using secure coding practices, and implementing encryption, authentication, and authorization mechanisms.
Container: This layer refers to the lightweight, isolated units that encapsulate the application and its dependencies. Security at this layer involves scanning and verifying the container images, enforcing policies and rules for container deployment and runtime, and isolating and protecting the containers from unauthorized access.
Cluster: This layer refers to the group of nodes that host the containers and provide orchestration and management capabilities. Security at this layer involves securing the communication between the nodes and the containers, monitoring and auditing the cluster activity, and applying security patches and updates to the cluster components.
Cloud: This layer refers to the underlying infrastructure and services that support the cloud-native applications. Security at this layer involves configuring and hardening the cloud resources, implementing identity and access management, and complying with the cloud provider's security standards and best practices.
The correct order of the four C's from the top (surface) layer to the bottom (base) layer is code, container, cluster, cloud, as each layer depends on the security of the next outermost layer. Reference: What Is Cloud-Native Security? - Palo Alto Networks, What is Cloud-Native Security? An Introduction | Splunk, The 4C's of Cloud Native Kubernetes security - Medium

NEW QUESTION # 195
Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

- A. MAC
- B. NFS
- C. SNMP
- D. UDP

Answer: C

Explanation:
* Application (Layer 7 or L7): This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication.
* Presentation (Layer 6 or L6): This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system.
* Session (Layer 5 or L5): This layer manages communication sessions (service requests and service responses) between networked

systems, including connection establishment, data transfer, and connection release.
* Transport (Layer 4 or L4): This layer provides transparent, reliable data transport and end-to-end transmission control.

NEW QUESTION # 196
.....

The versions of our Cybersecurity-Practitioner study guide includes the PDF version, PC version, APP online version. Each version's using method and functions are different and the client can choose the most convenient version to learn our Cybersecurity-Practitioner exam materials. For example, the PDF version is convenient for you to download and print our Cybersecurity-Practitioner Test Questions and is suitable for browsing learning. If you use the PDF version you can print our Cybersecurity-Practitioner test torrent on the papers and it is convenient for you to take notes. You can learn our Cybersecurity-Practitioner test questions at any time and place.