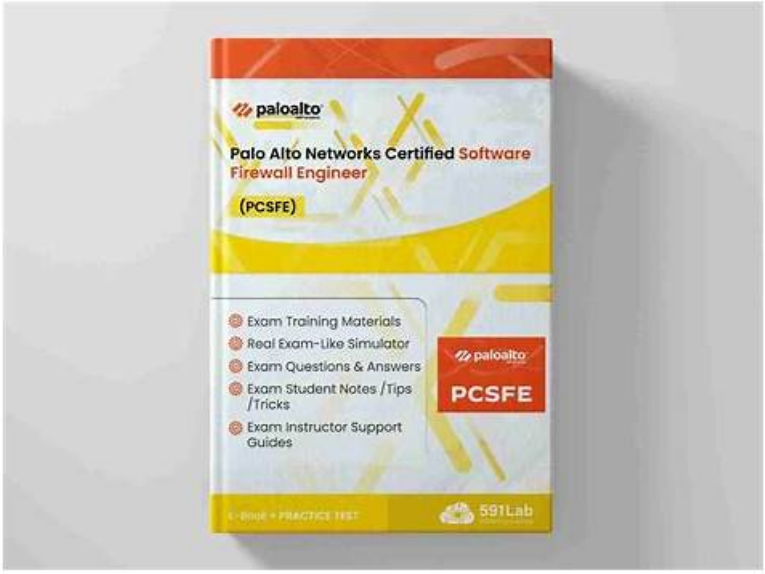
Palo Alto Networks PCCP Exam | PCCP Dump - Try Valid PCCP Exam Pdf Free and Buy Easily



P.S. Free & New PCCP dumps are available on Google Drive shared by Pass4Leader: https://drive.google.com/open?id=142LKjDVns4VC41-qUBPeNuWgamSqbRWk

The real and updated Palo Alto Networks Palo Alto Networks PCCP exam dumps file, desktop practice test software, and web-based practice test software are ready for download. Take the best decision of your professional career and enroll in the Palo Alto Networks Certified Cybersecurity Practitioner (PCCP) certification exam and download Palo Alto Networks Certified Cybersecurity Practitioner (PCCP) exam questions and starts preparing today.

Palo Alto Networks PCCP Exam Syllabus Topics:

Topic	Details
Topic 1	• Cybersecurity:This section of the exam measures skills of a Cybersecurity Practitioner and covers fundamental concepts of cybersecurity, including the components of the authentication, authorization, and accounting (AAA) framework, attacker techniques as defined by the MITRE ATT&CK framework, and key principles of Zero Trust such as continuous monitoring and least privilege access. It also addresses understanding advanced persistent threats (APT) and common security technologies like identity and access management (IAM), multi-factor authentication (MFA), mobile device and application management, and email security.
Topic 2	• Secure Access: This part of the exam measures skills of a Secure Access Engineer and focuses on defining and differentiating Secure Access Service Edge (SASE) and Secure Service Edge (SSE). It covers challenges related to confidentiality, integrity, and availability of data and applications across data, private apps, SaaS, and AI tools. It examines security technologies including secure web gateways, enterprise browsers, remote browser isolation, data loss prevention (DLP), and cloud access security brokers (CASB). The section also describes Software-Defined Wide Area Network (SD-WAN) and Prisma SASE solutions such as Prisma Access, SD-WAN, AI Access, and enterprise DLP.
Topic 3	• Security Operations: This final section measures skills of a Security Operations Analyst and covers key characteristics and practices of threat hunting and incident response processes. It explains functions and benefits of security information and event management (SIEM) platforms, security orchestration, automation, and response (SOAR) tools, and attack surface management (ASM) platforms. It also highlights the functionalities of Cortex solutions, including XSOAR, Xpanse, and XSIAM, and describes services offered by Palo Alto Networks' Unit 42.

>> PCCP Dump <<

Valid PCCP Exam Pdf - New PCCP Exam Fee

In the course of your study, the test engine of PCCP actual exam will be convenient to strengthen the weaknesses in the learning process. This can be used as an alternative to the process of sorting out the wrong questions of PCCP learning torrent in peacetime learning, which not only help you save time, but also makes you more focused in the follow-up learning process with our PCCP Learning Materials. Choose our PCCP guide materials and you will be grateful for your right decision.

Palo Alto Networks Certified Cybersecurity Practitioner Sample Questions (Q98-Q103):

NEW QUESTION # 98
What is a purpose of workload security on a Cloud Native Security Platform (CNSP)?

- A. To provide comprehensive logging of potential threat vectors
- B. To provide automation for application creation in the cloud
- C. To secure public cloud infrastructures only
- D. To secure serverless functions across the application

Answer: D

Explanation:
Workload security in a Cloud Native Security Platform (CNSP) is designed to secure containers, VMs, and serverless functions throughout the entire application lifecycle - from development to runtime - by detecting and blocking vulnerabilities, misconfigurations, and runtime threats.

NEW QUESTION # 99
Which pillar of Prisma Cloud application security does vulnerability management fall under?

- A. dynamic computing
- B. identity security
- C. network protection
- D. compute security

Answer: D

Explanation:
Prisma Cloud comprises four pillars:
Visibility, governance, and compliance. Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.
Compute security. Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your integrated development environment (IDE), software configuration management (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.
Network protection. Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.
Identity security. Monitor and leverage user and entity behavior analytics (UEBA) across your environments to detect and block malicious actions. Gain visibility into and enforce governance p

NEW QUESTION # 100
Which methodology does Identity Threat Detection and Response (ITDR) use?

- A. Rule-based activity prioritization
- B. Manual inspection of user activities

- C. Comparison of alerts to signatures
- D. Behavior analysis

Answer: D

Explanation:
Identity Threat Detection and Response (ITDR) leverages behavior analysis to identify suspicious or anomalous activities associated with user identities. This methodology involves continuously monitoring user authentication patterns, access events, and privilege escalations to build a baseline of "normal" behavior. By detecting deviations-such as unusual login locations, timeframes, or excessive access attempts-ITDR can flag potential identity compromises or insider threats that traditional signature or rule-based systems often miss. Palo Alto Networks' ITDR integrates behavioral analytics with threat intelligence to deliver real-time alerts and automated response capabilities, essential in mitigating credential abuse and lateral movement within networks. This behavioral approach is crucial for adapting to sophisticated identity attacks that evolve constantly.

NEW QUESTION # 101
Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and include panic?

- A. cyberterrorists
- B. state-affiliated groups
- C. cybercriminals
- D. hacktivists

Answer: A

Explanation:
Cyberterrorists are attackers who use the internet to recruit members to an ideology, to train them, and to spread fear and induce panic. Cyberterrorists may target critical infrastructure, government systems, or public services to cause disruption, damage, or harm. Cyberterrorists may also use the internet to disseminate propaganda, incite violence, or coordinate attacks. Cyberterrorists differ from other attacker profiles in their motivation, which is usually political, religious, or ideological, rather than financial or personal. References: Cyberterrorism, Cyber Threats, Cybersecurity Threat Landscape

NEW QUESTION # 102
What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

- A. run a static analysis
- B. send the executable to WildFire
- C. check its execution policy
- D. run a dynamic analysis

Answer: B

Explanation:
Palo Alto Networks Cortex XDR is an extended detection and response platform that provides endpoint protection, threat detection, and incident response capabilities. When an endpoint is asked to run an executable, Cortex XDR does the following steps1:
* First, it sends the executable to WildFire, a cloud-based malware analysis and prevention service, to determine if it is malicious or benign. WildFire uses static and dynamic analysis, machine learning, and threat intelligence to analyze the executable and provide a verdict in seconds2.
* Next, it checks the execution policy, which is a set of rules that define what actions are allowed or blocked on the endpoint. The execution policy can be configured by the administrator to enforce granular control over the endpoint behavior3.
* Then, it runs a static analysis, which is a technique that examines the executable without executing it. Static analysis can identify malicious indicators, such as file signatures, hashes, strings, and embedded resources4.
* Finally, it runs a dynamic analysis, which is a technique that executes the executable in a sandboxed environment and monitors its behavior. Dynamic analysis can detect malicious activities, such as network connections, registry changes, file modifications, and process injections4.
Cortex XDR Endpoint Protection Overview
WildFire Overview
[Execution Policy]
[Static and Dynamic Analysis]

NEW QUESTION # 103

......

Market is a dynamic place because a number of variables keep changing, so is the practice materials field of the PCCP practice exam. Our PCCP exam dumps are indispensable tool to pass it with high quality and low price. By focusing on how to help you effectively, we encourage exam candidates to buy our PCCP practice test with high passing rate up to 98 to 100 percent all these years. Our Palo Alto Networks exam dumps almost cover everything you need to know about the exam. As long as you practice our PCCP Test Question, you can pass exam quickly and successfully. By using them, you can not only save your time and money, but also pass PCCP practice exam without any stress.

Valid PCCP Exam Pdf: https://www.pass4leader.com/Palo-Alto-Networks/PCCP-exam.html

DOWNLOAD the newest Pass4Leader PCCP PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=142LKjDVns4VC41-qUBPeNuWgamSqbRWk