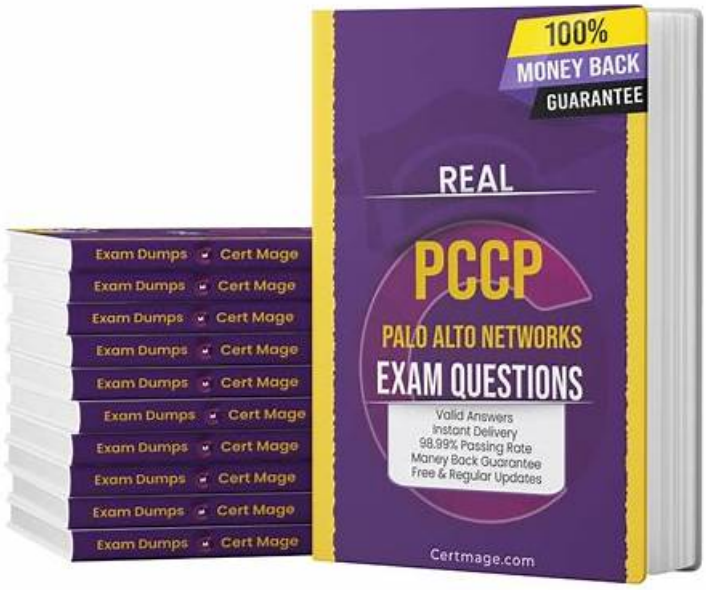
# PCCP Valid Exam Review, PCCP Latest Exam Cram




BONUS!!! Download part of Exams-boost PCCP dumps for free: https://drive.google.com/open?id=1DI_y8HVDDYiV2kDhS9eYHMLKAkMGCTZ-

Are you an exam jittering? Are you like a cat on hot bricks before your driving test? Do you have put a test anxiety disorder? If your answer is yes, we think that it is high time for you to use our PCCP exam question. Our PCCP study materials have confidence to help you Pass PCCP Exam successfully and get related certification that you long for. The PCCP guide torrent from our company must be a good choice for you, and then we will help you understand our PCCP test questions in detail.

## Palo Alto Networks PCCP Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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. |
| Topic 2 | • Cloud Security: This section targets a Cloud Security Specialist and addresses major cloud architectures and topologies. It discusses security challenges like application security, cloud posture, and runtime security. Candidates will learn about technologies securing cloud environments such as Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP), as well as the functions of a Cloud Native Application Protection Platform (CNAPP) and features of Cortex Cloud. |
| Topic 3 | • Endpoint Security: This domain is aimed at an Endpoint Security Analyst and covers identifying indicators of compromise (IOCs) and understanding the limits of signature-based anti-malware. It includes concepts like User and Entity Behavior Analytics (UEBA), endpoint detection and response (EDR), and extended detection and response (XDR). It also describes behavioral threat prevention and endpoint security technologies such as host-based firewalls, intrusion prevention systems, device control, application control, disk encryption, patch management, and features of Cortex XDR. |

**>> PCCP Valid Exam Review <<**

# PCCP Latest Exam Cram, Exam PCCP Tips

The marketplace is competitive, especially for securing a well-paid job. Moving your career one step ahead with PCCP certification will be a necessary and important thing. How to get the PCCP exam dumps with 100% pass is also important. PCCP training topics will ensure you pass at first time. The experts who involved in the edition of PCCP questions & answers all have rich hands-on experience, which guarantee you the high quality and high pass rate.

# Palo Alto Networks Certified Cybersecurity Practitioner Sample Questions (Q174-Q179):

**NEW QUESTION # 174**
Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

- A. Anomaly-based
- B. Behavior-based
- C. Statistical-based
- D. Knowledge-based

**Answer: D**

Explanation:
A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective.
# A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt.
These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge-based systems.

**NEW QUESTION # 175**
Which of the Cloud-Delivered Security Services (CDSS) will detect zero-day malware by using inline cloud machine learning (ML) and sandboxing?

- A. DNS security
- B. Advanced WildFire
- C. loT security
- D. Advanced Threat Prevention

**Answer: B**

Explanation:
Advanced WildFire is a Cloud-Delivered Security Service (CDSS) that detects zero-day malware using inline cloud machine learning (ML) and sandboxing techniques. It analyzes unknown files in real-time to identify and block new threats before they can cause harm.

**NEW QUESTION # 176**
In which type of Wi-Fi attack does the attacker intercept and redirect the victim's web traffic to serve content from a web server it controls?

- A. Evil Twin
- B. Emotet
- C. Jasager
- D. Meddler-in-the-middle

**Answer: D**

Explanation:
A meddler-in-the-middle (MITM) attack is a type of Wi-Fi attack where the attacker intercepts and redirects the victim's web traffic to serve content from a web server it controls. The attacker can use various techniques, such as ARP spoofing, DNS spoofing, or SSL stripping, to trick the victim into connecting to a rogue access point or a proxy server that acts as a middleman between the victim and the legitimate website.
The attacker can then modify, inject, or drop the packets that are exchanged between the victim and the website, and perform malicious actions, such as stealing credentials, injecting malware, or displaying fake or misleading content. A MITM attack can compromise the confidentiality, integrity, and availability of the victim's web traffic and expose them to various risks and threats.
References:
* What is a man-in-the-middle attack?
* The 5 most dangerous Wi-Fi attacks, and how to fight them
* What Are Sniffing Attacks, and How Can You Protect Yourself?

**NEW QUESTION # 177**
Which subnet does the host 192.168.19.36/27 belong?

- A. 192.168.19.32
- B. 192.168.19.0
- C. 192.168.19.64
- D. 192.168.19.16

**Answer: D**

Explanation:
To find the subnet that the host 192.168.19.36/27 belongs to, we need to convert the IP address and the subnet mask to binary form and perform a logical AND operation.
The /27 notation means that the subnet mask has 27 bits of ones and 5 bits of zeros.
In decimal form, the subnet mask is 255.255.255.224. The binary form of the IP address and the subnet mask are:
IP address: 11000000.10101000.00010011.00100100 Subnet mask: 11111111.11111111.11111111.11100000
The logical AND operation gives us the network prefix:
Network prefix: 11000000.10101000.00010011.00100000
To get the subnet address, we convert the network prefix back to decimal form:
Subnet address: 192.168.19.32
The subnet address is the first address in the subnet range. To find the last address in the subnet range, we flip the bits of the subnet mask and perform a logical OR operation with the network prefix:
Flipped subnet mask: 00000000.00000000.00000000.00011111 Logical OR: 11000000.10101000.00010011.00111111
The last address in the subnet range is:
Last address: 192.168.19.63
The subnet range is from 192.168.19.32 to 192.168.19.63. The host 192.168.19.36 belongs to this subnet.
Therefore, the correct answer is B. 192.168.19.16, which is the second address in the subnet range.
IP Subnet Calculator
Subnet Calculator - IP and CIDR
Which subnet does the host 192.168.19.36/27 belong? - VCEguide.com

**NEW QUESTION # 178**
Which endpoint tool or agent can enact behavior-based protection?

- A. MineMeld
- B. DNS Security
- C. Cortex XDR
- D. AutoFocus

**Answer: C**

Explanation:
Cortex XDR is an endpoint tool or agent that can enact behavior-based protection. Behavior-based protection is a method of detecting and blocking malicious activities based on the actions or potential actions of an object, such as a file, a process, or a

network connection. Behavior-based protection can identify and stop threats that are unknown or evade traditional signature-based detection, by analyzing the object's behavior for suspicious or abnormal patterns. Cortex XDR is a comprehensive solution that provides behavior-based protection for endpoints, networks, and cloud environments. Cortex XDR uses artificial intelligence and machine learning to continuously monitor and analyze data from multiple sources, such as logs, events, alerts, and telemetry. Cortex XDR can detect and prevent advanced attacks, such as ransomware, fileless malware, zero-day exploits, and lateral movement, by applying behavioral blocking and containment rules. Cortex XDR can also perform root cause analysis, threat hunting, and incident response, to help organizations reduce the impact and duration of security incidents. References:
* Cortex XDR - Palo Alto Networks
* Behavioral blocking and containment | Microsoft Learn
* Behaviour Based Endpoint Protection | Signature-Based Security - Xcitium
* The 12 Best Endpoint Security Software Solutions and Tools [2024]

**NEW QUESTION # 179**
.....

Everyone has their roles in society, and they are busy with their jobs and family. So the time and energy are very precious for the preparation of PCCP actual test. While, now you are lucky. PCCP cert guide will give you some instructions and help you do study plan for your coming test. If you are a fresh men in this industry, do not worry, Palo Alto Networks PCCP PDF training will help you. The questions and knowledge points are very simple and easy to get. You can download the PCCP test engine and install it on your phone. When you take the subway, you can open it and do test practice. To take full use of the spare time by PCCP test engine, you will enjoy a high efficiency study experience.