

# Paloalto-Networks

## Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician



#### NEW QUESTION 1

Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

- A. SaaS
- B. DaaS
- C. PaaS
- D. IaaS

**Answer:** D

#### NEW QUESTION 2

Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

- A. endpoint antivirus software
- B. strong endpoint passwords
- C. endpoint disk encryption
- D. endpoint NIC ACLs

**Answer:** A

#### NEW QUESTION 3

In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across the internet so that they can modify their attack objectives and methods?

- A. exploitation
- B. actions on the objective
- C. command and control
- D. installation

**Answer:** C

#### Explanation:

Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

#### NEW QUESTION 4

Which statement describes DevOps?

- A. DevOps is its own separate team
- B. DevOps is a set of tools that assists the Development and Operations teams throughout the software delivery process
- C. DevOps is a combination of the Development and Operations teams
- D. DevOps is a culture that unites the Development and Operations teams throughout the software delivery process

**Answer:** D

#### Explanation:

DevOps is not:

A combination of the Dev and Ops teams: There still are two teams; they just operate in a communicative, collaborative way.

Its own separate team: There is no such thing as a “DevOps engineer.” Although some companies may appoint a “DevOps team” as a pilot when trying to transition to a DevOps culture, DevOps refers to a culture where developers, testers, and operations personnel cooperate throughout the entire software delivery lifecycle.

A tool or set of tools: Although there are tools that work well with a DevOps model or help promote DevOps culture, DevOps ultimately is a strategy, not a tool.

Automation: Although automation is very important for a DevOps culture, it alone does not define DevOps.

#### NEW QUESTION 5

Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

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

**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 6

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

- A. Credit card number
- B. Trade secret
- C. National security information
- D. A symmetric encryption key

**Answer:** A

#### NEW QUESTION 7

Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

- A. Expedition
- B. AutoFocus
- C. MineMeld
- D. Cortex XDR

**Answer:** D

#### Explanation:

From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes.

#### NEW QUESTION 8

Which endpoint product from Palo Alto Networks can help with SOC visibility?

- A. STIX
- B. Cortex XDR
- C. WildFire
- D. AutoFocus

**Answer:** B

#### Explanation:

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can:

Identify hidden, stealthy, and sophisticated threats proactively and quickly  
Track threats across any source or location within the organization  
Increase the productivity of the people operating the technology  
Get more out of their security investments  
Conclude investigations more efficiently

#### NEW QUESTION 9

How does Prisma SaaS provide protection for Sanctioned SaaS applications?

- A. Prisma SaaS connects to an organizations internal print and file sharing services to provide protection and sharing visibility
- B. Prisma SaaS does not provide protection for Sanctioned SaaS applications because they are secure
- C. Prisma access uses Uniform Resource Locator (URL) Web categorization to provide protection and sharing visibility
- D. Prisma SaaS connects directly to sanctioned external service providers SaaS application service to provide protection and sharing visibility

**Answer:** D

#### Explanation:

Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

#### NEW QUESTION 10

In SecOps, what are two of the components included in the identify stage? (Choose two.)

- A. Initial Research
- B. Change Control
- C. Content Engineering
- D. Breach Response

**Answer:** AC

#### NEW QUESTION 10

Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

- A. Cortex XSOAR
- B. Prisma Cloud
- C. AutoFocus
- D. Cortex XDR

**Answer:** A

#### Explanation:

SOAR tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

<https://www.paloaltonetworks.com/cortex/security-operations-automation>

#### NEW QUESTION 15

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

- A. Network
- B. Management
- C. Cloud
- D. Security

**Answer:** D

#### Explanation:

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following:

Networking

Software-defined wide-area networks (SD-WANs) Virtual private networks (VPNs)

Zero Trust network access (ZTNA) Quality of Service (QoS)

Security

Firewall as a service (FWaaS) Domain Name System (DNS) security Threat prevention

Secure web gateway (SWG) Data loss prevention (DLP)

Cloud access security broker (CASB)

#### NEW QUESTION 17

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

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

**Answer:** D

#### NEW QUESTION 19

Which three services are part of Prisma SaaS? (Choose three.)

- A. Data Loss Prevention
- B. DevOps
- C. Denial of Service
- D. Data Exposure Control
- E. Threat Prevention

**Answer:** ADE

#### NEW QUESTION 24

What is a characteristic of the National Institute Standards and Technology (NIST) defined cloud computing model?

- A. requires the use of only one cloud service provider
- B. enables on-demand network services
- C. requires the use of two or more cloud service providers
- D. defines any network service

**Answer:** B

#### Explanation:

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner.

#### NEW QUESTION 25

In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

- A. SaaS
- B. PaaS
- C. On-premises
- D. IaaS

**Answer:** AB

#### NEW QUESTION 27

Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

- A. NetOps
- B. SecOps
- C. SecDevOps
- D. DevOps

**Answer:** B

**Explanation:**

Security operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast-evolving threats. SecOps needs to arm security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

**NEW QUESTION 32**

Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

- A. MineMeld
- B. AutoFocus
- C. WildFire
- D. Cortex XDR

**Answer:** B

**Explanation:**

"Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team's existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources."

**NEW QUESTION 35**

What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

- A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
- B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
- C. control and protect inter-host traffic by using IPv4 addressing
- D. control and protect inter-host traffic using physical network security appliances

**Answer:** D

**Explanation:**

page 211 "Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment: ... .. This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus."

**NEW QUESTION 38**

Which pillar of Prisma Cloud application security addresses ensuring that your cloud resources and SaaS applications are correctly configured?

- A. visibility, governance, and compliance
- B. network protection
- C. dynamic computing
- D. compute security

**Answer:** A

**Explanation:**

Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

**NEW QUESTION 43**

Which type of Wi-Fi attack depends on the victim initiating the connection?

- A. Evil twin
- B. Jasager
- C. Parager
- D. Mirai

**Answer:** A

**Explanation:**

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with "free Wi-Fi access." The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection.  
<https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/>

**NEW QUESTION 47**

In an IDS/IPS, which type of alarm occurs when legitimate traffic is improperly identified as malicious traffic?

- A. False-positive
- B. True-negative
- C. False-negative
- D. True-positive

**Answer:** A

**Explanation:**

In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative incorrectly identifies a threat as legitimate traffic.

**NEW QUESTION 50**

What are two key characteristics of a Type 1 hypervisor? (Choose two.)

- A. is hardened against cyber attacks
- B. runs without any vulnerability issues
- C. runs within an operating system
- D. allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer

**Answer:** CD

**NEW QUESTION 53**

Which NGFW feature is used to provide continuous identification, categorization, and control of known and previously unknown SaaS applications?

- A. User-ID
- B. Device-ID
- C. App-ID
- D. Content-ID

**Answer:** C

**Explanation:**

App-ID™ technology leverages the power of the broad global community to provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

**NEW QUESTION 56**

Which IoT connectivity technology is provided by satellites?

- A. 4G/LTE
- B. VLF
- C. L-band
- D. 2G/2.5G

**Answer:** C

**Explanation:**

2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications.

3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to

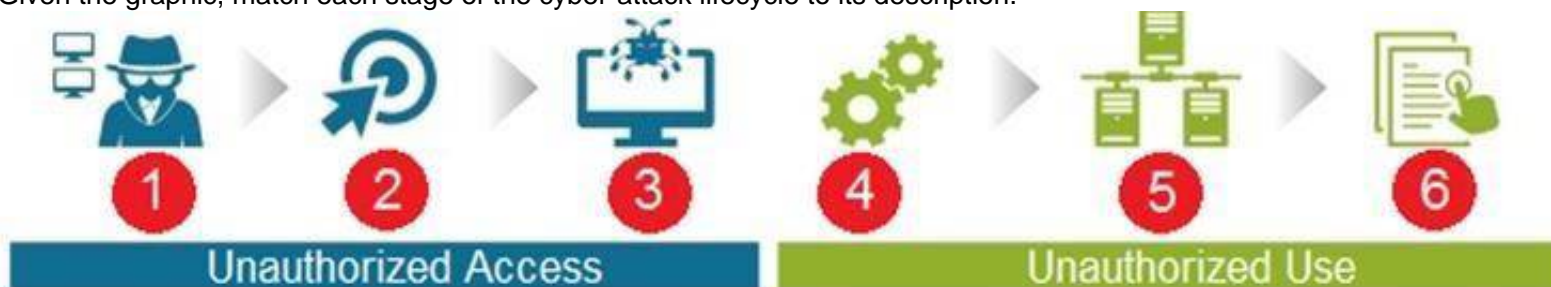
achieve data transfer rates of 384Kbps to 168Mbps.

4G/Long-Term Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.

5G: 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

**NEW QUESTION 60**

Given the graphic, match each stage of the cyber-attack lifecycle to its description.





reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

NEW QUESTION 65

In a traditional data center what is one result of sequential traffic analysis?

- A. simplifies security policy management
- B. reduces network latency
- C. causes security policies to be complex
- D. improves security policy application ID enforcement

Answer: C

Explanation:

Multiple policies, no policy reconciliation tools: Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying

**NEW QUESTION 70**

.....



## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

### PCCET Practice Exam Features:

- \* PCCET Questions and Answers Updated Frequently
- \* PCCET Practice Questions Verified by Expert Senior Certified Staff
- \* PCCET Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* PCCET Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PCCET Practice Test Here](#)**