



Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

NEW QUESTION 1

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

- A. Dynamic
- B. Pre-exploit protection
- C. Bare-metal
- D. Static

Answer: A

NEW QUESTION 2

What is required for a SIEM to operate correctly to ensure a translated flow from the system of interest to the SIEM data lake?


- A. connectors and interfaces
- B. infrastructure and containers
- C. containers and developers
- D. data center and UPS

Answer: A

NEW QUESTION 3

DRAG DROP

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



Unauthorized Access		Unauthorized Use
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 4

On an endpoint, which method should you use to secure applications against exploits?

- A. endpoint-based firewall
- B. strong user passwords
- C. full-disk encryption
- D. software patches

Answer: A

NEW QUESTION 5

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: D

NEW QUESTION 6

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

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

Answer: B

NEW QUESTION 7

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 syslog 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

NEW QUESTION 8

Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

- A. Global Protect
- B. WildFire
- C. AutoFocus
- D. STIX

Answer: C

NEW QUESTION 9

DRAG DROP

Match the description with the VPN technology.

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.		Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.		Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.		Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection		Secure Socket Tunneling Protocol

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.	Supported by most operating systems and provides no encryption by itself.	Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	Secure Socket Tunneling Protocol

NEW QUESTION 10

A native hypervisor runs:

- A. with extreme demands on network throughput
- B. only on certain platforms
- C. within an operating system's environment
- D. directly on the host computer's hardware

Answer: D

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

NEW QUESTION 12

Which activities do local organization security policies cover for a SaaS application?

- A. how the data is backed up in one or more locations
- B. how the application can be used

- C. how the application processes the data
- D. how the application can transit the Internet

Answer: B

NEW QUESTION 13

Which network analysis tool can be used to record packet captures?

- A. Smart IP Scanner
- B. Wireshark
- C. Angry IP Scanner
- D. Netman

Answer: B

NEW QUESTION 16

Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?

- A. Expedition
- B. Cortex XDR
- C. AutoFocus
- D. App-ID

Answer: B

NEW QUESTION 20

Which option describes the “selective network security virtualization” phase of incrementally transforming data centers?

- A. during the selective network security virtualization phase, all intra-host communication paths are strictly controlled
- B. during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server
- C. during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol
- D. during the selective network security virtualization phase, all intra-host traffic is load balanced

Answer: A

NEW QUESTION 25

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

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

Answer: C

NEW QUESTION 29

Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability?

- A. an intranet-accessed contractor’s system that was compromised
- B. exploitation of an unpatched security vulnerability
- C. access by using a third-party vendor’s password
- D. a phishing scheme that captured a database administrator’s password

Answer: D

NEW QUESTION 30

Why is it important to protect East-West traffic within a private cloud?

- A. All traffic contains threats, so enterprises must protect against threats across the entire network
- B. East-West traffic contains more session-oriented traffic than other traffic
- C. East-West traffic contains more threats than other traffic
- D. East-West traffic uses IPv6 which is less secure than IPv4

Answer: A

NEW QUESTION 33

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 37

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

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

Answer: D

NEW QUESTION 41

Which tool supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security?

- A. Prisma SAAS
- B. WildFire
- C. Cortex XDR
- D. Cortex XSOAR

Answer: D

NEW QUESTION 42

In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?

- A. Cortex XDR
- B. AutoFocus
- C. MineMild
- D. Cortex XSOAR

Answer: A

NEW QUESTION 43

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

- A. operating system patches
- B. full-disk encryption
- C. periodic data backups
- D. endpoint-based firewall

Answer: B

NEW QUESTION 47

Why have software developers widely embraced the use of containers?

- A. Containers require separate development and production environments to promote authentic code.
- B. Containers share application dependencies with other containers and with their host computer.
- C. Containers simplify the building and deploying of cloud native applications.
- D. Containers are host specific and are not portable across different virtual machine hosts.

Answer: C

NEW QUESTION 48

Which item accurately describes a security weakness that is caused by implementing a "ports first" data security solution in a traditional data center?

- A. You may have to use port numbers greater than 1024 for your business-critical applications.
- B. You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.
- C. You may not be able to assign the correct port to your business-critical applications.
- D. You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

Answer: B

NEW QUESTION 49

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: B

NEW QUESTION 50

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

NEW QUESTION 53

Which subnet does the host 192.168.19.36/27 belong?

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

Answer: D

NEW QUESTION 56

How does adopting a serverless model impact application development?

- A. costs more to develop application code because it uses more compute resources
- B. slows down the deployment of application code, but it improves the quality of code development
- C. reduces the operational overhead necessary to deploy application code
- D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code

Answer: C

NEW QUESTION 59

In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?

- A. Computer
- B. Switch
- C. Infrastructure
- D. Cloud

Answer: C

NEW QUESTION 64

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 66

SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

- A. People
- B. Accessibility
- C. Processes
- D. Understanding
- E. Business

Answer: ACE

NEW QUESTION 68

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

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

Answer: B

NEW QUESTION 69

What is the key to “taking down” a botnet?

- A. prevent bots from communicating with the C2
- B. install openvas software on endpoints

- C. use LDAP as a directory service
- D. block Docker engine software on endpoints

Answer: A

NEW QUESTION 71

Which type of Software as a Service (SaaS) application provides business benefits, is fast to deploy, requires minimal cost and is infinitely scalable?

- A. Benign
- B. Tolerated
- C. Sanctioned
- D. Secure

Answer: C

NEW QUESTION 72

An Administrator wants to maximize the use of a network address. The network is 192.168.6.0/24 and there are three subnets that need to be created that can not overlap. Which subnet would you use for the network with 120 hosts?

Requirements for the three subnets:

Subnet 1: 3 host addresses

Subnet 2: 25 host addresses

Subnet 3: 120 host addresses

- A. 192.168.6.168/30
- B. 192.168.6.0/25
- C. 192.168.6.160/29
- D. 192.168.6.128/27

Answer: B

NEW QUESTION 77

.....

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](#)