

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

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

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

Answer: B

NEW QUESTION 3

DRAG DROP

Match the Identity and Access Management (IAM) security control with the appropriate definition.

IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

IAM security	IAM security	Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity	User Entity Behavior Analytics	Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics	Access Management	Securing and managing the relationships between users and cloud resources
Access Management	Machine Identity	Decoupling workload identity from IP addresses

NEW QUESTION 4

Which not-for-profit organization maintains the common vulnerability exposure catalog that is available through their public website?

- A. Department of Homeland Security
- B. MITRE
- C. Office of Cyber Security and Information Assurance
- D. Cybersecurity Vulnerability Research Center

Answer: B

NEW QUESTION 5

Which technique changes protocols at random during a session?

- A. use of non-standard ports
- B. port hopping
- C. hiding within SSL encryption
- D. tunneling within commonly used services

Answer: B

NEW QUESTION 6

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 7

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 8

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 9

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 10

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 10

Systems that allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows are known as what?

- A. XDR
- B. STEP
- C. SOAR
- D. SIEM

Answer: C

NEW QUESTION 13

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 16

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 18

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 19

Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?

- A. Shortest Path
- B. Hop Count
- C. Split Horizon
- D. Path Vector

Answer: B

NEW QUESTION 20

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 23

The customer is responsible only for which type of security when using a SaaS application?

- A. physical
- B. platform
- C. data
- D. infrastructure

Answer: C

NEW QUESTION 27

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 30

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 34

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 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

NEW QUESTION 40

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 42

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 45

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 48

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 52

Which IoT connectivity technology is provided by satellites?

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

Answer: C

NEW QUESTION 57

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 61

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 64

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 67

How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline?

- A. DevSecOps improves pipeline security by assigning the security team as the lead team for continuous deployment
- B. DevSecOps ensures the pipeline has horizontal intersections for application code deployment
- C. DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline
- D. DevSecOps does security checking after the application code has been processed through the CI/CD pipeline

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 75

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 77

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)