



Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

NEW QUESTION 1

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 2

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 3

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 4

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 5

Which characteristic of serverless computing enables developers to quickly deploy application code?

- A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand
- B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components
- C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code
- D. Using Container as a Service (CaaS) to deploy application containers to run their code.

Answer: A

NEW QUESTION 6

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 7

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 8

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 9

What does SIEM stand for?

- A. Security Infosec and Event Management
- B. Security Information and Event Management
- C. Standard Installation and Event Media
- D. Secure Infrastructure and Event Monitoring

Answer: B

NEW QUESTION 10

DRAG DROP

Match the IoT connectivity description with the technology.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10

Which aspect of a SaaS application requires compliance with local organizational security policies?

- A. Types of physical storage media used
- B. Data-at-rest encryption standards
- C. Acceptable use of the SaaS application
- D. Vulnerability scanning and management

Answer: C

NEW QUESTION 14

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 17

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 19

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 20

Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?

- A. DNS Security
- B. URL Filtering
- C. WildFire
- D. Threat Prevention

Answer: C

NEW QUESTION 24

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 26

During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?

- A. Frame
- B. Segment
- C. Packet
- D. Data

Answer: C

NEW QUESTION 30

Which core component is used to implement a Zero Trust architecture?

- A. VPN Concentrator
- B. Content Identification
- C. Segmentation Platform
- D. Web Application Zone

Answer: C

NEW QUESTION 31

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 36

DRAG DROP

Match each description to a Security Operating Platform key capability.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 39

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 40

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 45

DRAG DROP

Order the OSI model with Layer7 at the top and Layer1 at the bottom.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 50

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 55

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 56

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

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

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 66

Which type of LAN technology is being displayed in the diagram?

- A. Star Topology
- B. Spine Leaf Topology
- C. Mesh Topology
- D. Bus Topology

Answer: C

NEW QUESTION 71

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 72

What is a key advantage and key risk in using a public cloud environment?

- A. Multi-tenancy
- B. Dedicated Networks
- C. Dedicated Hosts
- D. Multiplexing

Answer: A

NEW QUESTION 75

.....

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](#)