Paloalto Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

NEW QUESTION 1
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 2
Under which category does an application that is approved by the IT department, such as Office 365, fall?

A. unsanctioned
B. prohibited
C. tolerated
D. sanctioned

Answer: D

NEW QUESTION 3
Which of the following is an AWS serverless service?

A. Beta
B. Kappa
C. Delta
D. Lambda

Answer: D

Explanation:
Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

NEW QUESTION 4
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 5
Which type of IDS/IPS uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt?

A. Knowledge-based
B. Signature-based
C. Behavior-based
D. Database-based

Answer: C

Explanation:
IDSs and IPSs also can be classified as knowledge-based (or signature-based) or behavior-based (or statistical anomaly-based) systems:
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 6
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 7
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 8
Which network device breaks networks into separate broadcast domains?

A. Hub
B. Layer 2 switch
C. Router
D. Wireless access point

Answer: C

Explanation:
A layer 2 switch will break up collision domains but not broadcast domains. To break up broadcast domains you need a Layer 3 switch with vlan capabilities.

NEW QUESTION 9
Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

A. North-South traffic
B. Intrazone traffic
C. East-West traffic
D. Interzone traffic

Answer: A

NEW QUESTION 10
Which key component is used to configure a static route?

A. router ID
B. enable setting
C. routing protocol
D. next hop IP address

Answer: D

NEW QUESTION 11
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: D

Explanation:
New software vulnerabilities and exploits are discovered all the time and thus diligent software patch management is required by system and security administrators in every organization.

NEW QUESTION 12
Which method is used to exploit vulnerabilities, services, and applications?

A. encryption
B. port scanning
C. DNS tunneling
D. port evasion

Answer: D

Explanation:
Attack communication traffic is usually hidden with various techniques and tools, including:
Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. Port evasion using network anonymizers or port hopping to traverse over any available open ports
Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult
DNS tunneling is used for C2 communications and data infiltration

NEW QUESTION 13
Which type of malware replicates itself to spread rapidly through a computer network?

A. ransomware
B. Trojan horse
C. virus
D. worm

Answer: D

Explanation:
A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

NEW QUESTION 14
Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

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

Answer: B

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 15
Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

A. Session, Transport, Network
B. Application, Presentation, and Session
C. Physical, Data Link, Network
D. Data Link, Session, Transport

Answer: B

Explanation:
Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model. Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.
Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.
Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

NEW QUESTION 16
When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.)

A. decrypt the infected file using base64
B. alert system administrators
C. quarantine the infected file
D. delete the infected file
E. remove the infected file’s extension

Answer: CDE

NEW QUESTION 17
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:

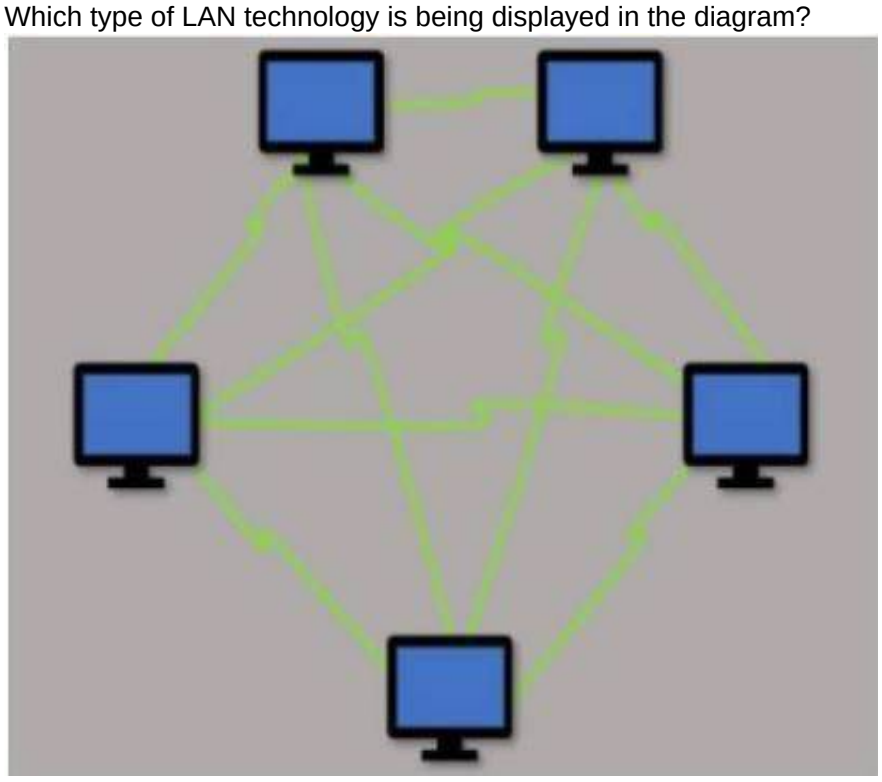
In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative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

NEW QUESTION 18
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 19
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: A

NEW QUESTION 20
Which IPsec feature allows device traffic to go directly to the Internet?

A. Split tunneling
B. Diffie-Hellman groups
C. d.Authentication Header (AH)
D. IKE Security Association

Answer: A

Explanation:
"Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less
performance degradation."

NEW QUESTION 21
.....

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