Vendor: Palo Alto Networks

Exam Code: PCCP

Exam Name: Palo Alto Networks Certified Cybersecurity Practitioner

Version: DEMO

QUESTION 1
Which technology helps Security Operations Center (SOC) teams identify heap spray attacks on company-owned laptops?

A. CSPM
B. ASM
C. EDR
D. CVVP

Answer: C
Explanation:
Heap spray attacks exploit memory management vulnerabilities by injecting malicious code into a program's heap to manipulate execution flow. Endpoint Detection and Response (EDR) platforms monitor memory and process behavior on endpoints, enabling the detection of such memory-based exploits through anomaly and behavior analysis. Palo Alto Networks' Cortex XDR equips SOC teams with the tools to detect, analyze, and respond to heap spray and other in-memory attacks on company laptops in real time. EDR's endpoint-centric visibility is crucial since heap spray attacks operate below network layers and often bypass traditional perimeter defenses.

QUESTION 2
What are two common lifecycle stages for an advanced persistent threat (APT) that is infiltrating a network? (Choose two.)

A. Lateral movement
B. Communication with covert channels
C. Deletion of critical data
D. Privilege escalation

Answer: AD
Explanation:
Lateral movement is a key stage where the attacker moves across the network to find valuable targets.
Privilege escalation involves gaining higher access rights to expand control within the compromised environment.
Communication with covert channels is a tactic used during persistence or exfiltration, while deletion of critical data is not a standard APT lifecycle stage -- it's more characteristic of destructive attacks.

QUESTION 3
A high-profile company executive receives an urgent email containing a malicious link. The sender appears to be from the IT department of the company, and the email requests an update of the executive's login credentials for a system update.
Which type of phishing attack does this represent?

A. Whaling
B. Vishing
C. Pharming
D. Angler phishing

Answer: A
Explanation:
Whaling is a targeted phishing attack aimed at high-profile individuals, such as executives. The

attacker impersonates a trusted entity (e.g., IT department) to trick the executive into revealing sensitive credentials. This is a form of spear phishing specifically focused on "big fish" targets.

QUESTION 4
Which next-generation firewall (NGFW) deployment option provides full application visibility into Kubernetes environments?

A. Virtual
B. Container
C. Physical
D. SASE

Answer: B
Explanation:
A container-based NGFW is specifically designed to integrate with Kubernetes environments, providing full application visibility and control within containerized workloads. It operates at the pod level, making it ideal for securing dynamic microservices architectures.

QUESTION 5
Which type of firewall should be implemented when a company headquarters is required to have redundant power and high processing power?

A. Cloud
B. Physical
C. Virtual
D. Containerized

Answer: B
Explanation:
A physical firewall is ideal for environments like a company headquarters that require redundant power, high throughput, and dedicated hardware for maximum reliability and performance. It supports more robust failover and scalability compared to virtual or containerized options.

QUESTION 6
Which statement describes the process of application allow listing?

A. It allows only trusted files, applications, and processes to run.
B. It creates a set of specific applications that do not run on the system.
C. It encrypts application data to protect the system from external threats.
D. It allows safe use of applications by scanning files for malware.

Answer: A
Explanation:
Application allow listing is a security practice that permits only pre-approved (trusted) applications, files, and processes to run on a system. This approach helps prevent unauthorized or malicious software from executing, thereby reducing the attack surface.

QUESTION 7
Which component of the AAA framework verifies user identities so they may access the network?

A. Allowance
B. Authorization
C. Accounting
D. Authentication

Answer: D
Explanation:
Authentication is the component of the AAA (Authentication, Authorization, and Accounting) framework that verifies user identities (e.g., via passwords, certificates, or biometrics) before granting access to network resources.

QUESTION 8
Which capability does Cloud Security Posture Management (CSPM) provide for threat detection within Prisma Cloud?

A. Real-time protection from threats
B. Alerts for new code introduction
C. Integration with threat feeds
D. Continuous monitoring of resources

Answer: D
Explanation:
Cloud Security Posture Management (CSPM), includingPrisma Cloud's offering, continuously monitors all cloud resources -- such as compute instances, storage, network configurations, and identities -- to detect misconfigurations, vulnerabilities, and potential threats in near real time.

QUESTION 9
Which type of system collects data and uses correlation rules to trigger alarms?

A. SIM
B. SIEM
C. UEBA
D. SOAR

Answer: B
Explanation:
A Security Information and Event Management (SIEM) system collects data from various sources (logs, events, etc.) and uses correlation rules to analyze this data and trigger alarms when suspicious or predefined patterns are detected.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**