Palo Alto Networks

CYBERSECURITY-PRACTITIONER Exam

Palo Alto Networks Cybersecurity Practitioner

Questions & Answers
Demo

Version: 4.0

Question: 1

Which methodology does Identity Threat Detection and Response (ITDR) use?

A. Behavior analysis

B. Comparison of alerts to signatures

C. Manual inspection of user activities

D. Rule-based activity prioritization

Answer: A

Explanation:

Identity Threat Detection and Response (ITDR) leverages behavior analysis to identify suspicious or anomalous activities associated with user identities. This methodology involves continuously monitoring user authentication patterns, access events, and privilege escalations to build a baseline of “normal” behavior. By detecting deviations—such as unusual login locations, timeframes, or excessive access attempts—ITDR can flag potential identity compromises or insider threats that traditional signature or rule-based systems often miss. Palo Alto Networks’ ITDR integrates behavioral analytics with threat intelligence to deliver real-time alerts and automated response capabilities, essential in mitigating credential abuse and lateral movement within networks. This behavioral approach is crucial for adapting to sophisticated identity attacks that evolve constantly.

Question: 2

Which technology grants enhanced visibility and threat prevention locally on a device?

A. EDR

B. IDS

C. SIEM

D. DLP

Answer: A

Explanation:

Endpoint Detection and Response (EDR) technologies provide comprehensive visibility and real-time threat prevention directly on endpoint devices. EDR continuously monitors process activities, file executions, and system calls to detect malware, suspicious behaviors, and zero-day threats at the source. Palo Alto Networks' Cortex XDR platform exemplifies this by correlating endpoint telemetry with network and cloud data to provide a holistic defense against attacks. Operating locally on endpoints allows EDR to prevent lateral movement and respond to threats quickly, filling security gaps that network-centric tools alone cannot address. This endpoint-level insight is critical to identifying sophisticated threats that initiate or manifest on user devices.

Question: 3

What are two examples of an attacker using social engineering? (Choose two.)

A. Convincing an employee that they are also an employee

B. Leveraging open-source intelligence to gather information about a high-level executive

C. Acting as a company representative and asking for personal information not relevant to the reason for their call

D. Compromising a website and configuring it to automatically install malicious files onto systems that visit the page

Answer: A,C

Explanation:

Social engineering attacks manipulate human trust to gain unauthorized access or information. Convincing an employee that an attacker is also an employee builds rapport, lowering defenses for information disclosure or credential sharing. Similarly, impersonating a company representative and requesting unrelated personal data exploits authority bias to deceive victims. These tactics exploit psychological vulnerabilities rather than technical flaws and are prevalent initial steps in multi-stage attacks. Palo Alto Networks highlights the importance of training, multi-factor authentication, and behavior-based threat detection to mitigate social engineering risks effectively.

Question: 4

Which two services does a managed detection and response (MDR) solution provide? (Choose two.)

A. Improved application development

B. Incident impact analysis

C. Periodic firewall updates

D. Proactive threat hunting

Answer: B,D

Explanation:

Managed Detection and Response (MDR) services combine incident impact analysis and proactive threat hunting to enhance organizational security posture. Incident impact analysis assesses the severity, scope, and potential damage of identified threats, helping prioritize responses. Proactive threat hunting involves skilled analysts searching for hidden threats that automated detection may miss, leveraging threat intelligence and behavioral analytics. Palo Alto Networks' MDR integrates Cortex XDR and human expertise to detect, investigate, and remediate sophisticated threats early. Unlike routine firewall updates or development processes, MDR is focused on active threat discovery and comprehensive incident management.

Question: 5

What role do containers play in cloud migration and application management strategies?

A. They enable companies to use cloud-native tools and methodologies.

B. They are used for data storage in cloud environments.

C. They serve as a template manager for software applications and services.

D. They are used to orchestrate virtual machines (VMs) in cloud environments.

Answer: A

Explanation:

Containers encapsulate applications and their dependencies into lightweight, portable units that can run consistently across multiple environments. This abstraction supports cloud-native development by enabling microservices architectures, rapid deployment, and scaling within orchestration platforms like Kubernetes. Containers accelerate cloud migration by decoupling applications from infrastructure, facilitating automation, and continuous integration/continuous deployment (CI/CD) workflows. Palo Alto Networks addresses container security by integrating runtime protection, vulnerability scanning, and compliance enforcement within its Prisma Cloud platform, ensuring safe adoption of cloud-native tools and methodologies.