Palo Alto Networks

PCCET Exam

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Questions & Answers
Demo

Version: 6.0

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

Explanation:

The WildFire cloud-based malware analysis environment is a cyber threat prevention service that identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment.

Question: 2

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

Explanation:

Question: 3

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

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

Answer: A

Explanation:

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with "free Wi-Fi access." The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection.
https://www.paloaltonetworks.com/blog/2013/11/wireless-man-middle/

Question: 4

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

Explanation:

Question: 5

Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

A. NetOps
B. SecOps
C. SecDevOps
D. DevOps

Answer: B

Explanation:

Security operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast-evolving threats. SecOps needs to arm security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.