Exam : **PCCET**

Title : Palo Alto Networks Certified Cybersecurity Entry-level Technician

Version : DEMO

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:
Dynamic analysis is a method of malware analysis that executes the malware in a controlled environment and observes its behavior and effects. Dynamic analysis can reveal the malware's network activity, file system changes, registry modifications, and other indicators of compromise. Dynamic analysis is performed by Palo Alto Networks WildFire, a cloud-based service that analyzes unknown files and links from various sources, such as email attachments, web downloads, and firewall traffic. WildFire uses a custom-built, evasion-resistant virtual environment to detonate the submissions and generate detailed reports and verdicts. WildFire can also share the threat intelligence with other Palo Alto Networks products and partners to prevent future attacks.
Reference: WildFire Overview, WildFire Features, WildFire Dynamic Analysis

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:
Connectors and interfaces are the components that enable a SIEM to collect, process, and analyze data from various sources, such as Microsoft 365 services and applications1, cloud platforms, network devices, and security solutions. Connectors are responsible for extracting and transforming data from the source systems, while interfaces are responsible for sending and receiving data to and from the SIEM server. Without connectors and interfaces, a SIEM cannot operate correctly and ensure a translated flow from the system of interest to the SIEM data lake.
Reference: SIEM server integration with Microsoft 365 services and applications
What Is SIEM Integration? 2024 Comprehensive Guide - SelectHub
SIEM Connector - docs.metallic.io
SIEM Connector

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:

An evil twin is a type of Wi-Fi attack that involves setting up a fake malicious Wi-Fi hotspot with the same name as a legitimate network to trick users into connecting to it. The attacker can then intercept the user's data, such as passwords, credit card numbers, or personal information. The victim initiates the connection by choosing the fake network from the list of available Wi-Fi networks, thinking it is the real one. The attacker can also use a deauthentication attack to disconnect the user from the legitimate network and force them to reconnect to the fake one.
Reference: Types of Wi-Fi Attacks You Need to Guard Your Business Against - TechGenix Types of Wireless and Mobile Device Attacks - GeeksforGeeks
The 5 most dangerous Wi-Fi attacks, and how to fight them What are Wi-Fi Attacks & How to Fight - Tech Resider

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:
North-South traffic refers to the data packets that move between the virtualized environment and the external network, such as the internet or a traditional data center. This traffic typically involves requests from clients to access applications or services hosted on virtual machines (VMs) or containers, or responses from those VMs or containers to the clients. North-South traffic can also include management or monitoring traffic from external devices to the virtualized environment.
Reference: Fundamentals of Cloud Security, East-West and North-South Traffic Security, What is the meaning / origin of the terms north-south and east-west traffic?

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:
SecOps is the organizational function that is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues. SecOps is a collaboration between security and operations teams that aims to align their goals, processes, and tools to improve security posture and efficiency. SecOps can leverage automation to simplify and accelerate security tasks, such as threat detection, incident response, vulnerability management, compliance enforcement, and more. Security automation can also reduce human errors, enhance scalability, and free up resources for more strategic initiatives.
Reference: SecOps from Palo Alto Networks
What is security automation? from Red Hat

What is Security Automation? from Check Point Software