Palo Alto Networks
Cybersecurity-Apprentice
Palo Alto Networks Certified Cybersecurity Apprentice

Latest Version: 6.0

Question: 1

What are two endpoint security implementation methods? (Choose two.)

A. Installing an anti-malware agent onto a user device
B. Deploying a firewall to prevent traffic from reaching an end user
C. Enforcing security policies on north-south traffic between users and the internet
D. Downloading software onto a laptop to prevent spyware

Answer: A, D

Explanation:
Endpoint security focuses on protecting the individual device where users work, such as laptops, desktops, mobile devices, and other endpoint systems. Installing an anti-malware agent onto a user device is a direct endpoint security implementation method because the security control resides on the host and inspects files, processes, and system behavior for malicious activity. Downloading software onto a laptop to prevent spyware is also an endpoint-focused control because it protects the local device against malicious code designed to monitor activity, steal data, or weaken the operating environment. By contrast, deploying a firewall to prevent traffic from reaching an end user is primarily a network security control when placed at the network boundary. Enforcing north-south traffic policies is also network security because it governs traffic moving between internal users and the internet. Palo Alto Networks identifies endpoint security objectives and components such as security updates, antivirus, and host-based firewalls under the Endpoint Security domain. Cybersecurity Apprentice Datasheet, Endpoint Security 4.2 and 4.3.

Question: 2

Which tool resides on a host to identify malicious activity?

A. Instruction Detection System (IDS)
B. Unified threat detection device
C. Endpoint protection agent
D. Next-generation firewall appliance

Answer: C

Explanation:

An endpoint protection agent is software installed directly on a host, such as a workstation, laptop, or server, to monitor local activity and identify malicious behavior. Because it resides on the endpoint, it can observe processes, files, registry changes, network connections, and user activity that may not be visible to a perimeter security device. This makes it especially useful for detecting malware execution, suspicious scripts, privilege abuse, and post-compromise activity. An IDS may detect suspicious patterns, but the answer is not precise because IDS can be network-based or host-based and is not necessarily an agent. A next-generation firewall appliance is typically deployed inline at a network control point, not directly on the host. “Unified threat detection device” is not the standard course term for a host-resident control. The Palo Alto Networks Cybersecurity Apprentice blueprint places endpoint protection components under Endpoint Security and also recognizes host-based detection concepts under cybersecurity threat detection systems. Cybersecurity Apprentice Datasheet, Endpoint Security 4.3 and Cybersecurity 1.4.

Question: 3

Which type of device does a Host-Based Intrusion Detection System (HIDS) monitor?

A. Appliance
B. Computer
C. Switch
D. Router

Answer: B

Explanation:
A Host-Based Intrusion Detection System monitors an individual host, which is typically a computer, server, or endpoint device. Its purpose is to inspect activity occurring on that system rather than traffic across an entire network segment. A HIDS can evaluate system logs, file integrity, configuration changes, authentication events, and suspicious local behavior. This distinguishes it from a Network-Based Intrusion Detection System, which observes packets traversing a network link or segment. A switch and router are network infrastructure devices, and while they may generate logs or support monitoring, they are not the primary monitored object of a HIDS. The term “appliance” is too broad and usually refers to a dedicated hardware or virtual security device. Palo Alto Networks lists IDS, HIDS, and NIDS as common threat detection systems in the Cybersecurity Apprentice Cybersecurity domain, requiring candidates to distinguish where each system operates and what it observes. Cybersecurity Apprentice Datasheet, Cybersecurity 1.4.

Question: 4

What is the primary goal of the Weaponization and Delivery stage in the cyber attack lifecycle?

A. Developing and testing malware for bypassing defenses
B. Ensuring compliance with Security policies
C. Distributing compromised hardware to targets
D. Creating a malicious payload by using vulnerabilities

Answer: D

Explanation:
The Weaponization and Delivery stage focuses on preparing and transmitting the attack mechanism that will be used against the target. In this phase, the attacker turns knowledge gathered during reconnaissance into a usable malicious payload. That payload may exploit a software vulnerability, embed malicious code into a document, or prepare a link, file, or package that can compromise the victim once executed or accessed. The correct answer is D because it combines the creation of a malicious payload with the use of vulnerabilities, which is the operational purpose of weaponization. Developing and testing malware is related, but it is narrower and does not fully capture delivery to the target. Compliance with security policies is a defensive governance activity, not an attacker lifecycle phase. Distributing compromised hardware can occur in some supply chain attacks, but it is not the primary definition of this lifecycle stage. Palo Alto Networks requires candidates to identify and describe stages of the cyber attack lifecycle under the Cybersecurity domain. Cybersecurity Apprentice Datasheet, Cybersecurity 1.2.

Question: 5

What is a cluster in relation to cloud-native security?

A. Portable and self-sufficient unit that packages an application with its dependencies
B. Set of system rules written in a particular programming language
C. Collection of nodes (bare-metal or virtualized machines) that will host application pods
D. Distributed collection of servers that hosts software and is accessible over the internet

Answer: C

Explanation:
In cloud-native security, a cluster is a collection of compute nodes that run containerized workloads. These nodes may be physical bare-metal systems or virtualized machines, and together they provide the execution environment for application pods. In Kubernetes-style architectures, a pod is the smallest deployable unit, and the cluster provides scheduling, networking, scaling, and orchestration capabilities. Answer A describes a container, not a cluster, because a container packages application code with the runtime and dependencies needed to execute consistently across environments. Answer B describes code or policy logic, not infrastructure. Answer D is a broad description of cloud-hosted services but lacks the specific cloud-native meaning of nodes hosting pods. Palo Alto Networks includes common

cloud terms such as virtualization, virtual machine, container, microservice, and API in the Cloud Security domain, and also includes cloud-native security platform concepts. Understanding clusters is essential because cloud-native security must protect the orchestration layer, workload runtime, identities, configurations, and network paths between services. Cybersecurity Apprentice Datasheet, Cloud Security 5.4 and 5.5.

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer