DUMPSARENA

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Palo Alto Networks PCCET

Version Demo

Total Demo Questions: 19

Total Premium Questions: 192

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cybersecurity Fundamentals	55
Topic 2, Network Fundamentals	46
Topic 3, Cloud Security Fundamentals	40
Topic 4, Security Operations Fundamentals	22
Topic 5, Palo Alto Networks Portfolio	29
Total	192

QUESTION NO: 1

Which two actions are commonly performed during the containment phase of incident response? (Choose two.)

A. Isolate an affected endpoint from the network

B. Block known malicious domains or IP addresses

C. Rebuild all affected systems from backups

D. Conduct a lessons-learned review

ANSWER: A B

Explanation:

Isolating an affected endpoint and **blocking malicious network indicators** are containment actions. Containment is intended to limit the scope and impact of an incident while preserving the ability to investigate and recover. Isolating a compromised endpoint can prevent it from communicating with other internal systems or attacker-controlled infrastructure.

Security teams can also block known malicious IP addresses, domains, URLs, or file hashes to interrupt additional malicious activity. Rebuilding systems and conducting a lessons-learned review are important activities, but they normally occur during recovery and post-incident activities rather than initial containment. See CISA incident response guidance and NIST SP 800-61, Computer Security Incident Handling Guide.

QUESTION NO: 2

Which key component is used to configure a static route?

A. router ID

B. enable setting

C. routing protocol

D. next hop IP address

ANSWER: D

Explanation:

A **next hop IP address** is a key component of a static route because it identifies the Layer 3 device to which the firewall should forward traffic destined for a specified network. Static routes are manually defined forwarding entries in a virtual router. Along with the destination prefix and an egress interface, the next-hop value tells the firewall where to send packets so they can continue toward the destination. For a normal unicast static route, the next hop is typically the IP address of the adjacent router reachable through the selected outgoing interface. This explicit forwarding instruction is what makes the route static: the firewall does not need to learn the path dynamically from a routing protocol. Palo Alto Networks documentation describes static-route configuration as including a destination, interface, and next-hop setting, with the next hop specifying the router or forwarding target used for traffic matching the route. See the Palo Alto Networks documentation on configuring static routes and the Virtual Routers documentation for the routing concepts and configuration context.

QUESTION NO: 3

What does SOAR technology use to automate and coordinate workflows?

A. algorithms

B. Cloud Access Security Broker

C. Security Incident and Event Management

D. playbooks

ANSWER: D

Explanation:

SOAR technology uses **playbooks** to automate and coordinate security workflows. A playbook is a structured, repeatable sequence of response steps that defines how the platform should handle a particular alert, incident type, or operational process. It can orchestrate actions across connected tools, such as gathering alert context, enriching indicators with threat-intelligence data, creating tickets, notifying analysts, blocking malicious indicators, and documenting the response.

Playbooks make response processes consistent because they translate an organization's approved incident-response procedures into executable workflows. They can include automated tasks, decision points, integrations with security products and IT systems, and manual analyst tasks where human review or approval is needed. This lets security teams reduce repetitive work while retaining appropriate control over higher-impact actions. Palo Alto Networks Cortex XSOAR describes playbooks as the mechanism used to model and automate incident-response processes, including actions performed through integrations and automations. See the Cortex XSOAR overview and the Cortex XSOAR playbooks documentation.

QUESTION NO: 4 - (DRAG DROP)

DRAG DROP

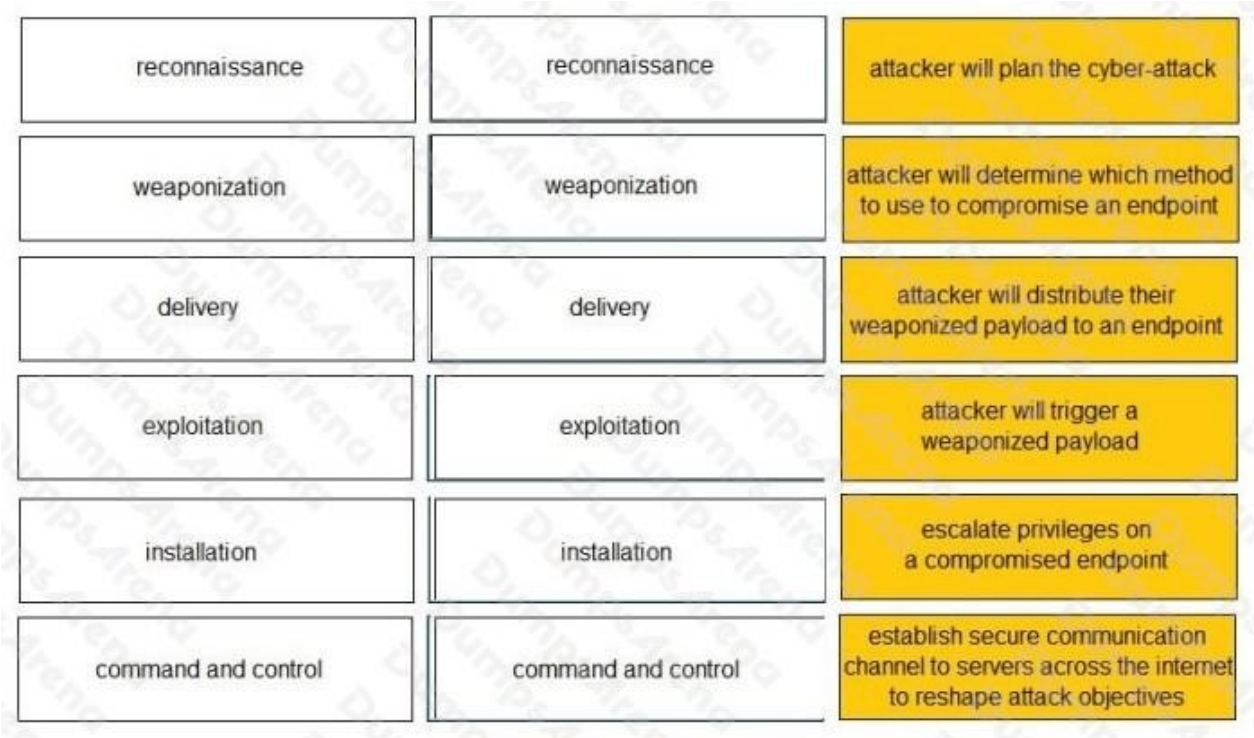
Given the graphic, match each stage of the cyber-attack lifecycle to its description.



Select and Place:



ANSWER:



Explanation:

The completed lifecycle correctly follows the sequence of activity an attacker performs while progressing from preparation to controlling a compromised system. Reconnaissance is the planning and information-gathering phase, where the attacker identifies a target and prepares the overall attack approach. Weaponization follows by selecting or preparing the technique and payload intended to compromise the target endpoint. Delivery is then the movement of that weaponized payload to the endpoint, such as through a message, download, or other transmission path. Exploitation occurs when the delivered payload is activated or triggered against the target. Installation represents the attacker establishing a stronger foothold on the compromised endpoint, including gaining elevated privileges where needed to continue operating successfully. Finally, command and control is the stage in which the compromised endpoint communicates with attacker-controlled servers through a channel that permits instructions, updates, and changes to attack objectives. This progression matches the cyber kill chain model's view of an intrusion as a connected set of stages, allowing defenders to detect and disrupt adversary activity before it reaches its later operational phases. Palo Alto Networks discusses the value of understanding the cyber kill chain for identifying where attacks can be prevented in its Cyber Kill Chain overview. The original model and its lifecycle concepts are also documented by Lockheed Martin's Cyber Kill Chain resource.

QUESTION NO: 5

What is the purpose of SIEM?

A. Securing cloud-based applications

B. Automating the security team's incident response

C. Real-time monitoring and analysis of security events

D. Filtering webpages employees are allowed to access

ANSWER: C

Explanation:

Real-time monitoring and analysis of security events is the core purpose of a Security Information and Event Management (SIEM) solution. A SIEM centrally collects and aggregates log data, alerts, and event records from security tools, endpoints, servers, network devices, and applications. It normalizes and correlates that data so security analysts can identify suspicious patterns, investigate potential threats, and maintain visibility across the organization's environment. SIEM capabilities commonly include continuous monitoring, event correlation, alerting, dashboards, reporting, and support for incident investigation and compliance activities. In a Palo Alto Networks security operations context, centralized visibility and

analytics help analysts prioritize meaningful security events and respond with appropriate investigation workflows. Although some security platforms can integrate SIEM with automation or other controls, SIEM's defining function is collecting, monitoring, correlating, and analyzing security-relevant telemetry. Palo Alto Networks describes Cortex XSIAM as building on SIEM capabilities by collecting and analyzing security data at scale, while the Cybersecurity and Infrastructure Security Agency identifies centralized logging and monitoring as essential practices for detecting and responding to cyber threats. See Palo Alto Networks Cortex XSIAM and CISA: Logging Made Easy.

QUESTION NO: 6

Which three statements describe advantages of using containers? (Choose three.)

A. Portability across compatible environments

B. Efficient use of host resources

C. Rapid application deployment

D. A separate guest operating system for every container

E. Elimination of application vulnerabilities

ANSWER: A B C

Explanation:

Portability, **efficient resource use**, and **rapid deployment** are common advantages of containers. A container packages an application with its required libraries and dependencies, allowing the workload to run consistently across compatible environments. This portability can reduce differences between development, testing, and production deployments.

Containers share the host operating-system kernel rather than requiring a complete guest operating system for every workload. This makes them relatively lightweight and can allow many workloads to run efficiently on the same host. Container images can also be built, distributed, and started quickly, supporting automated CI/CD workflows. Containers do not eliminate the need for operating-system, application, identity, image, and runtime security controls. See Docker Docs: What is a container? and Palo Alto Networks: What Is Container Security?.

QUESTION NO: 7

Which two statements are true about microsegmentation? (Choose two.)

A. It applies granular policy controls between workloads.

B. It can limit lateral movement after a workload is compromised.

C. It requires all internal systems to share one trusted security zone.

D. It eliminates the need for identity-based access controls.

ANSWER: A B

Explanation:

Microsegmentation divides an environment into smaller security zones and applies granular controls to communication between workloads. Instead of allowing broad access throughout a data center or cloud network, policies can limit a workload to only the applications, services, and destinations it requires.

Microsegmentation also helps reduce lateral movement. If an attacker compromises one workload, segmentation can restrict its ability to communicate with unrelated systems, reducing the potential scope of the incident. This approach supports zero trust by enforcing access controls close to the protected workload. See Palo Alto Networks: What Is Microsegmentation? and NIST SP 800-207: Zero Trust Architecture.

QUESTION NO: 8

What type of DNS record maps an IPV6 address to a domain or subdomain to another hostname?

A. SOA

B. NS

C. AAAA

D. MX

ANSWER: C

Explanation:

AAAA is the DNS resource record type used to associate a domain name or hostname with an IPv6 address. When a client needs to reach a service over IPv6, it queries DNS for the hostname's AAAA record and receives the corresponding 128-bit IPv6 address. This is the IPv6 equivalent of an A record, which provides an IPv4 address for a hostname. For example, an AAAA record can map `www.example.com` to an address such as `2001:db8::10`, allowing IPv6-capable clients to establish a connection using that address. DNS terminology can be confusing when discussing address-to-name lookups: standard forward DNS uses an AAAA record to map a name to an IPv6 address, while reverse DNS uses a PTR record under the `ip6.arpa` domain to map an IPv6 address back to a hostname. In the context of selecting the DNS record for IPv6 host addressing, AAAA is the appropriate record type. See the IETF definition of AAAA records in RFC 3596 and the DNS record overview in Cloudflare's AAAA record documentation.

QUESTION NO: 9

Which IoT connectivity technology is provided by satellites?

A. 4G/LTE

B. VLF

C. L-band

D. 2G/2.5G

ANSWER: C

Explanation:

L-band is correct because it is a radio-frequency band widely used by satellite communications services, including satellite IoT connectivity. L-band satellite systems can connect remote sensors, trackers, industrial equipment, and other IoT devices where terrestrial network coverage is unavailable, unreliable, or impractical. This makes the technology particularly useful for assets operating at sea, in remote agriculture and mining locations, across transport routes, or in emergency-response scenarios.

Satellite IoT devices transmit data to an orbiting satellite using L-band spectrum; the satellite then relays that data through its ground infrastructure to the intended application or cloud service. L-band is well suited to many low-data-rate IoT use cases because its propagation characteristics support broad geographic coverage and communications with relatively small, low-power terminals. Inmarsat describes its L-band network as providing reliable global mobile satellite connectivity and identifies it as a foundation for IoT and machine-to-machine services. The GSMA also describes satellite IoT as a means of extending IoT connectivity beyond the reach of terrestrial networks. See Inmarsat L-band services and GSMA Satellite IoT.

QUESTION NO: 10 - (SIMULATION)

Given the graphic, match each stage of the cyber-attack lifecycle to its description.



reconnaissance		attacker will plan the cyber-attack
weaponization		attacker will determine which method to use to compromise an endpoint
delivery		attacker will distribute their weaponized payload to an endpoint
exploitation		attacker will trigger a weaponized payload
installation		escalate privileges on a compromised endpoint
command and control		establish secure communication channel to servers across the internet to reshape attack objectives

ANSWER: See the explanation for the answer

Explanation:

Correct matches (in cyber-attack lifecycle order):

The first three stages are associated with gaining *unauthorized access*; the final three represent *unauthorized use* of the compromised endpoint.

QUESTION NO: 11

Which two network resources does a directory service database contain? (Choose two.)

A. Services

B. /etc/shadow files

C. Users

D. Terminal shell types on endpoints

ANSWER: A C

Explanation:

Directory services centrally store and organize information about network identities and resources so that administrators and applications can locate, authenticate, authorize, and manage them consistently. **Users** are a fundamental directory object: their records commonly include identity attributes, credentials or authentication associations, group membership, and

access-related properties. This centralized user information supports account management and access control across the organization.

Services are also represented in directory environments. A directory can publish service-related objects and attributes that allow clients to discover available network services and enable services to authenticate or operate under managed identities. For example, Microsoft Active Directory Domain Services stores directory objects and provides the identity and directory infrastructure used to manage users, computers, groups, and related network resources. Palo Alto Networks likewise describes directory integration as a way to obtain user and group information for policy use through User-ID.

Keeping users and services in a directory database provides a shared, searchable source of identity and resource information rather than requiring each endpoint or application to maintain separate records. See Microsoft's Active Directory Domain Services overview and Palo Alto Networks User-ID documentation.

QUESTION NO: 12

What are three benefits of the cloud native security platform? (Choose three.)

A. Increased throughput

B. Exclusivity

C. Agility

D. Digital transformation

E. Flexibility

ANSWER: C D E

Explanation:

Agility, **Digital transformation**, and **Flexibility** are benefits of a cloud-native security platform. Cloud-native security is designed to protect applications, workloads, identities, and data across the cloud-development lifecycle while supporting the rapid pace of cloud development and deployment. This enables teams to innovate and release services more quickly, which is the practical value of agility. A unified cloud-native security platform also helps organizations adopt cloud services and modern application architectures with appropriate security controls, visibility, and governance, supporting secure digital transformation rather than treating security as a separate late-stage activity.

Flexibility results from using security capabilities that can operate across cloud environments, cloud accounts, containers, hosts, and application-development workflows. This allows organizations to apply protection consistently as infrastructure and applications change. Palo Alto Networks describes Prisma Cloud as a cloud-native application protection platform that secures cloud-native applications throughout their lifecycle and across clouds. Its platform approach helps teams build, deploy, and run applications securely while maintaining the speed and adaptability expected in cloud environments. See Palo Alto Networks Prisma Cloud and What Is Cloud-Native Security?.

QUESTION NO: 13

Which of the following is a CI/CD platform?

A. Github

B. Jira

C. Atom.io

D. Jenkins

ANSWER: D

Explanation:

Jenkins is a CI/CD automation platform used to build, test, and deliver software through repeatable pipelines. It can be connected to source-code repositories, triggered when developers commit changes, and configured to execute stages such as compiling code, running automated tests, performing security checks, creating artifacts, and deploying applications. Jenkins pipelines are defined as code, commonly in a `Jenkinsfile`, which makes the build and release process version-controlled, consistent, and reproducible across teams and environments.

In a DevOps workflow, this automation supports continuous integration by validating changes frequently and supports continuous delivery or deployment by moving validated builds through release stages. Jenkins has a broad plugin ecosystem that enables integrations with version-control systems, cloud platforms, container tooling, ticketing systems, and security tools. Palo Alto Networks CI/CD guidance similarly describes integrating security checks into automated development and delivery pipelines so that security is incorporated throughout the software lifecycle rather than added only at the end. See the Jenkins documentation and Palo Alto Networks' shift-left security overview.

QUESTION NO: 14

Which two statements are true about servers in a demilitarized zone (DMZ)? (Choose two.)

A. They can be accessed by traffic from the internet.

B. They are located in the internal network.

C. They can expose servers in the internal network to attacks.

D. They are isolated from the internal network.

ANSWER: A D

Explanation:

"They can be accessed by traffic from the internet." is true because a DMZ is commonly used to host public-facing services, such as web, email, DNS, or application servers. Security policy can permit only the required inbound connections from untrusted internet sources to those published services, rather than allowing unrestricted access. "They are isolated from the internal network." is also true because the core purpose of a DMZ is network segmentation: systems that must be reachable externally are placed in a separate zone from trusted internal resources. A next-generation firewall enforces explicit policy between the internet, the DMZ, and internal zones, inspecting and limiting each permitted flow. This architecture reduces the opportunity for an incident involving a public-facing server to directly affect internal systems and supports least-privilege access design. Palo Alto Networks describes security policy as controlling traffic between zones and recommends segmenting networks to apply appropriate protections based on trust level and exposure. See the Palo Alto Networks zone-based firewall documentation and the Palo Alto Networks DMZ overview.

QUESTION NO: 15

From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

A. Unit 52

B. PAN-DB

C. BrightCloud

D. MineMeld

ANSWER: B

Explanation:

PAN-DB is correct because it is Palo Alto Networks' cloud-based URL categorization and URL-filtering intelligence database. It classifies URLs and domains into predefined categories, allowing security products and analysts to associate web destinations with their reputation, content type, and potential risk. AutoFocus uses this URL intelligence as contextual enrichment when investigating threats, helping analysts correlate indicators observed in malware samples, WildFire analysis,

and broader threat data with the websites or domains involved. This context can reveal relevant behaviors such as connections to known malicious infrastructure, phishing destinations, command-and-control locations, or other suspicious web activity. PAN-DB intelligence is continuously maintained by Palo Alto Networks and is also the database used by URL Filtering to determine a site's category for policy enforcement. Using the same trusted URL intelligence across prevention and investigation supports faster, more informed analysis of an indicator's web-based relationships. Palo Alto Networks describes PAN-DB and URL categorization in its URL Filtering overview; additional AutoFocus product context is available on the AutoFocus product page.

QUESTION NO: 16

What are the two most prominent characteristics of the malware type rootkit? (Choose two.)

A. It encrypts user data.

B. It uses masking techniques to evade or hinder detection by antivirus.

C. It takes control of the operating system.

D. It steals personal information.

ANSWER: B C

Explanation:

Rootkits are distinguished by their ability to obtain highly privileged control of a compromised system and conceal their presence. "It uses masking techniques to evade or hinder detection by antivirus" is correct because rootkits can hide malicious files, processes, network connections, and registry entries from ordinary operating-system and security-tool views. Some rootkits operate at the kernel, boot, or firmware level, which enables them to interfere with the mechanisms security products use to inspect the device. Detection is not impossible, but it can be substantially more difficult than for conventional malware.

"It takes control of the operating system" is also correct because a rootkit is designed to provide an attacker with persistent, privileged access. By embedding itself deeply within the operating system or startup chain, it can control or manipulate system behavior while maintaining covert access. This level of control can support additional attacker activity, including executing other payloads, monitoring activity, or maintaining remote access. Palo Alto Networks describes rootkits as malware that provides unauthorized, privileged access while hiding its presence; Microsoft similarly notes that rootkits can conceal malware and enable persistent control of a device. See Palo Alto Networks Cyberpedia: What Is a Rootkit? and Microsoft Security: What is a rootkit?.

QUESTION NO: 17

Which type of malware replicates itself to spread rapidly through a computer network?

A. ransomware

B. Trojan horse

C. virus

D. worm

ANSWER: D

Explanation:

A worm is malware designed to self-replicate and propagate across networks, often without requiring a user to open a malicious file or otherwise take action. After reaching a vulnerable device, a worm can scan for other reachable systems and exploit security weaknesses or use available network paths to copy itself further. This autonomous, network-oriented propagation can cause infections to expand very quickly, consume bandwidth, and disrupt systems. Worms may also carry a payload, such as data theft tools, ransomware, or components that allow attackers to remotely control infected devices, but

their defining characteristic is their ability to reproduce and spread independently. The U.S. Cybersecurity and Infrastructure Security Agency describes worms as self-replicating programs that spread through networks, and Palo Alto Networks similarly identifies self-propagation as a key worm behavior. See CISA: Virus vs. Worm and Palo Alto Networks: What Is a Computer Worm?.

QUESTION NO: 18

Which three services are part of Prisma SaaS? (Choose three.)

A. Data Loss Prevention

B. DevOps

C. Denial of Service

D. Data Exposure Control

E. Threat Prevention

ANSWER: A D E

Explanation:

Prisma SaaS includes Data Loss Prevention, Data Exposure Control, and Threat Prevention as complementary services for protecting software-as-a-service applications and the information stored in them. Data Loss Prevention identifies sensitive information using predefined and customizable data patterns, then helps organizations apply policy controls to prevent inappropriate sharing or exposure. This gives security teams visibility into sensitive data across sanctioned SaaS applications.

Data Exposure Control focuses on discovering and remediating risky configurations and sharing settings that could expose data, such as publicly accessible files, overly permissive links, or external sharing. It continuously evaluates SaaS content and permissions so that access risks can be identified and addressed. Threat Prevention adds inspection for malicious content and threats within SaaS environments, helping detect malware and compromised or suspicious activity associated with cloud-hosted files and collaboration services. Together, these services address the core needs of SaaS security: protecting sensitive data, reducing exposure created by configuration and sharing, and detecting threats. Palo Alto Networks describes these SaaS security capabilities in its SaaS Security overview and its SaaS Security documentation.

QUESTION NO: 19

Which characteristic of serverless computing enables developers to quickly deploy application code?

A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand

B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components

C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code

D. Using Container as a Service (CaaS) to deploy application containers to run their code.

ANSWER: B

Explanation:

Uploading the application code itself, without having to provision a full container image or any OS virtual machine components is correct because serverless computing abstracts the underlying infrastructure from the developer. In the common function-as-a-service model, a developer supplies a function or application code, configures its trigger and any required settings, and the cloud provider handles server provisioning, operating-system maintenance, runtime availability, scaling, and execution. This substantially shortens the path from code to a deployed workload: developers do not need to build, patch, configure, or operate virtual-machine images, nor do they need to manage the infrastructure capacity that will

host the code. The platform can instantiate execution environments when events or requests arrive and scale them according to demand. This deployment model lets teams focus on application logic and integrations while the provider manages the operational components beneath the service. AWS describes Lambda as a serverless compute service that runs code without requiring servers or clusters to be provisioned or managed, and Azure similarly describes Functions as enabling event-driven code execution without managing infrastructure. See AWS Lambda Developer Guide and Azure Functions overview.