Download Palo Alto Networks Cybersecurity-Practitioner Exam Dumps Free

Shared by Payne on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two pieces of information are considered personally identifiable information (PII)? (Choose two.)

Options:

A- Birthplace
B- Login 10
C- Profession
D- Name

Answer:

A, D

Explanation:

Personally identifiable information (PII) is any data that can be used to identify someone.All information that directly or indirectly links to a person is considered PII1. Among PII, some pieces of information are more sensitive than others.Sensitive PII is sensitive information that directly identifies an individual and could cause significant harm if leaked or stolen2.Birthplace and name are examples of sensitive PII, as they can be used to distinguish or trace an individual's identity, either alone or when combined with other information3. Login 10 and profession are not considered sensitive PII, as they are not unique to a person and do not reveal their identity.Login 10 is a non-sensitive PII that is easily accessible from public sources, while profession is not a PII at all, as it does not link to a specific individual4.Reference:

1: What is PII (personally identifiable information)? - Cloudflare

2: What is Personally Identifiable Information (PII)? | IBM

3: personally identifiable information - Glossary | CSRC

4: What Is Personally Identifiable Information (PII)? Types and Examples

Question 2

Question Type: MultipleChoice

In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

Options:

A- SaaS
B- PaaS
C- On-premises
D- IaaS

Answer:

A, B

Explanation:

In cloud computing, there are three main service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Each model defines the level of responsibility and control that the cloud provider and the cloud customer have over the cloud resources and services. The cloud provider is responsible for vulnerability and patch management of the underlying operating system in SaaS and PaaS models, while the cloud customer is responsible for it in IaaS model. In SaaS, the cloud provider delivers software applications over the internet and manages all aspects of the cloud infrastructure, platform, and application. The cloud customer only needs to access the software through a web browser or an API. In PaaS, the cloud provider offers a platform for developing, testing, and deploying applications and manages the cloud infrastructure and operating system. The cloud customer can use the platform tools and services to create and run their own applications. In IaaS, the cloud provider supplies the basic cloud infrastructure, such as servers, storage, and networking, and the cloud customer can provision and configure their own operating system, middleware, and applications.Reference:Cloud Computing Service Models,Cloud Security Fundamentals - Module 2: Cloud Computing Models,Palo Alto Networks Certified Cybersecurity Entry-level Technician (PCCET)

Question 3

Question Type: MultipleChoice

Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

Options:

A- Expedition
B- AutoFocus
C- MineMeld
D- Cortex XDR

Answer:

D

Explanation:

From a business perspective, XDR platforms enable organizations to prevent successful cyberattacks as well as simplify and strengthen security processes.

Question 4

Question Type: MultipleChoice

What would allow a security team to inspect TLS encapsulated traffic?

Options:

A- DHCP markings
B- Decryption
C- Port translation
D- Traffic shaping

Answer:

B

Explanation:

Decryption is required to inspect TLS-encrypted traffic, allowing security tools (such as firewalls or intrusion prevention systems) to analyze the contents of the traffic for threats that would otherwise remain hidden within encrypted sessions.

Question 5

Question Type: MultipleChoice

What is an event-driven snippet of code that runs on managed infrastructure?

Options:

A- API
B- Serverless function
C- Hypervisor
D- Docker container

Answer:

B

Explanation:

A serverless function is an event-driven snippet of code that runs on managed infrastructure, typically as part of a Function as a Service (FaaS) model. It is executed in response to events such as HTTP requests or database changes, and the cloud provider handles the underlying infrastructure.

Question 6

Question Type: MultipleChoice

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

Options:

A- Increased throughput
B- Exclusivity
C- Agility
D- Digital transformation
E- Flexibility

Answer:

C, D, E

Explanation:

A cloud native security platform (CNSP) is a set of security practices and technologies designed specifically for applications built and deployed in cloud environments. It involves a shift in mindset from traditional security approaches, which often rely on network-based protections, to a more application-focused approach that emphasizes identity and access management, container security and workload security, and continuous monitoring and response. A CNSP offers three main benefits for cloud native applications:

Agility: A CNSP enables faster and more frequent delivery of software updates, as security is built into the application and infrastructure from the ground up, rather than added on as an afterthought. This allows for seamless integration of security controls into the continuous integration/continuous delivery (CI/CD) pipeline, reducing the risk of security gaps or delays. A CNSP also leverages automation and orchestration to simplify and streamline security operations, such as configuration, patching, scanning, and remediation.

Digital transformation: A CNSP supports the adoption of cloud native technologies, such as microservices, containers, serverless, and platform as a service (PaaS), which enable greater scalability, deployability, manageability, and performance of cloud applications. These technologies also allow for more innovation and experimentation, as developers can easily create, test, and deploy new features and functionalities. A CNSP helps to protect these cloud native architectures from threats and vulnerabilities, while also ensuring compliance with regulations and standards.

Flexibility: A CNSP provides consistent and comprehensive security across different cloud environments, such as public, private, and multi-cloud. It also allows for customization and adaptation of security policies and controls to suit the specific needs and pReference of each application and organization. A CNSP can also integrate with other security tools and platforms, such as firewalls, endpoint protection, threat intelligence, and security information and event management (SIEM), to provide a holistic and unified view of the security posture and risk level of cloud applications.

:

What Is a Cloud Native Security Platform?

What Is Cloud-Native Security?

All You Need to Know About Cloud Native Security

Top Five Benefits of Cloud Native Application Security