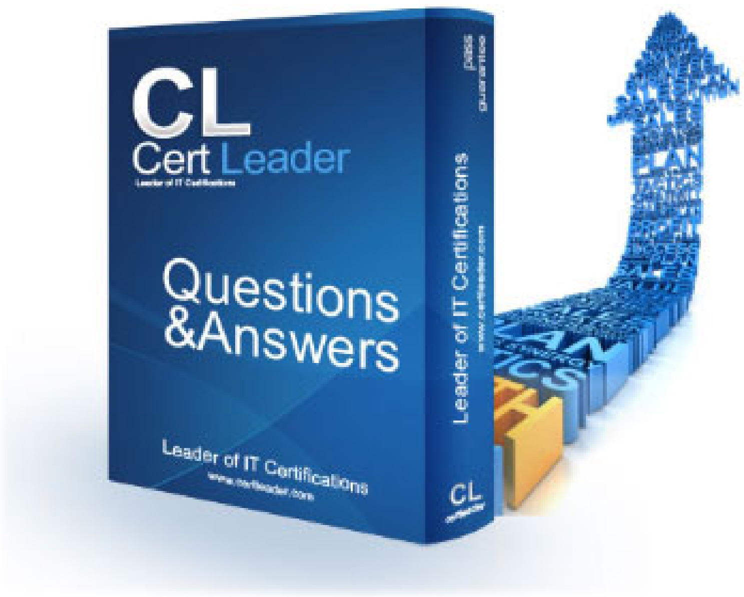
PCCET Dumps

Palo Alto Networks Certified Cybersecurity Entry-level Technician

https://www.certleader.com/PCCET-dumps.html



NEW QUESTION 1
Which model would a customer choose if they want full control over the operating system(s) running on their cloud computing platform?

A. SaaS
B. DaaS
C. PaaS
D. IaaS

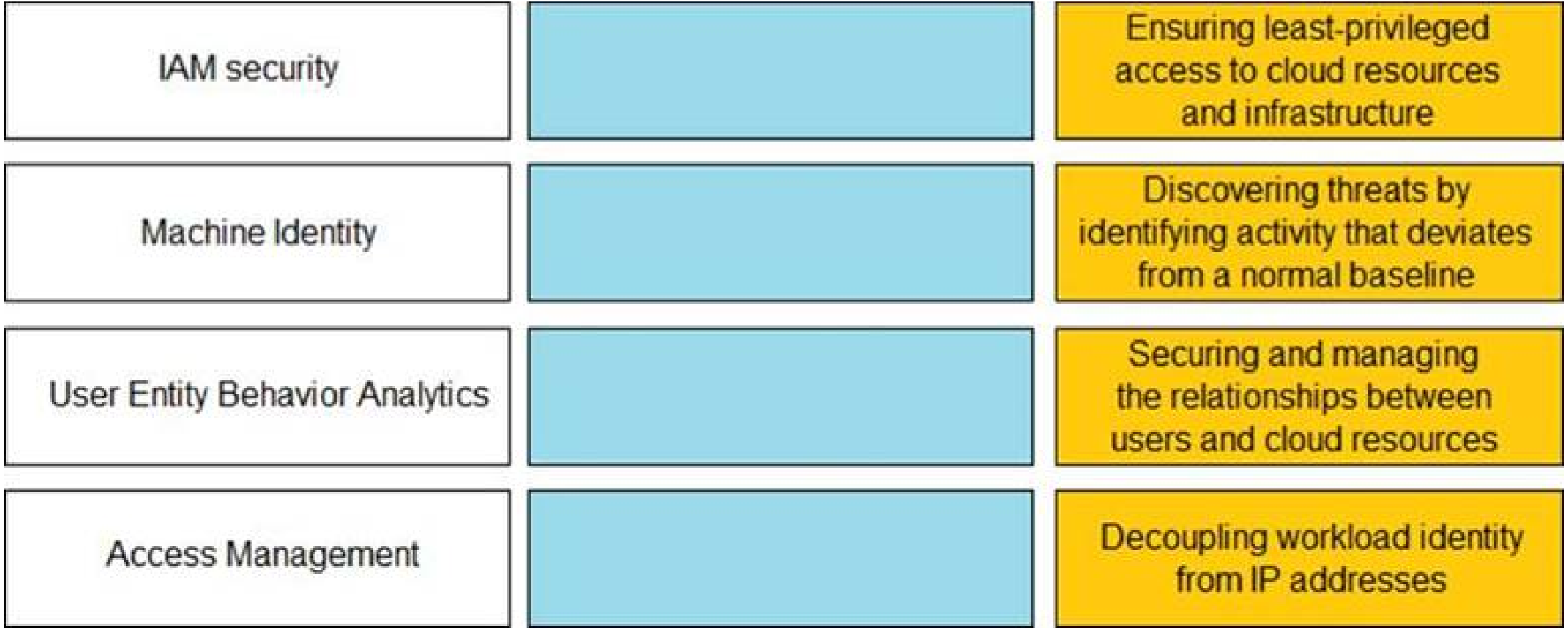
Answer: D

NEW QUESTION 2
Which security component should you configure to block viruses not seen and blocked by the perimeter firewall?

A. endpoint antivirus software
B. strong endpoint passwords
C. endpoint disk encryption
D. endpoint NIC ACLs

Answer: A

NEW QUESTION 3
Match the Identity and Access Management (IAM) security control with the appropriate definition.

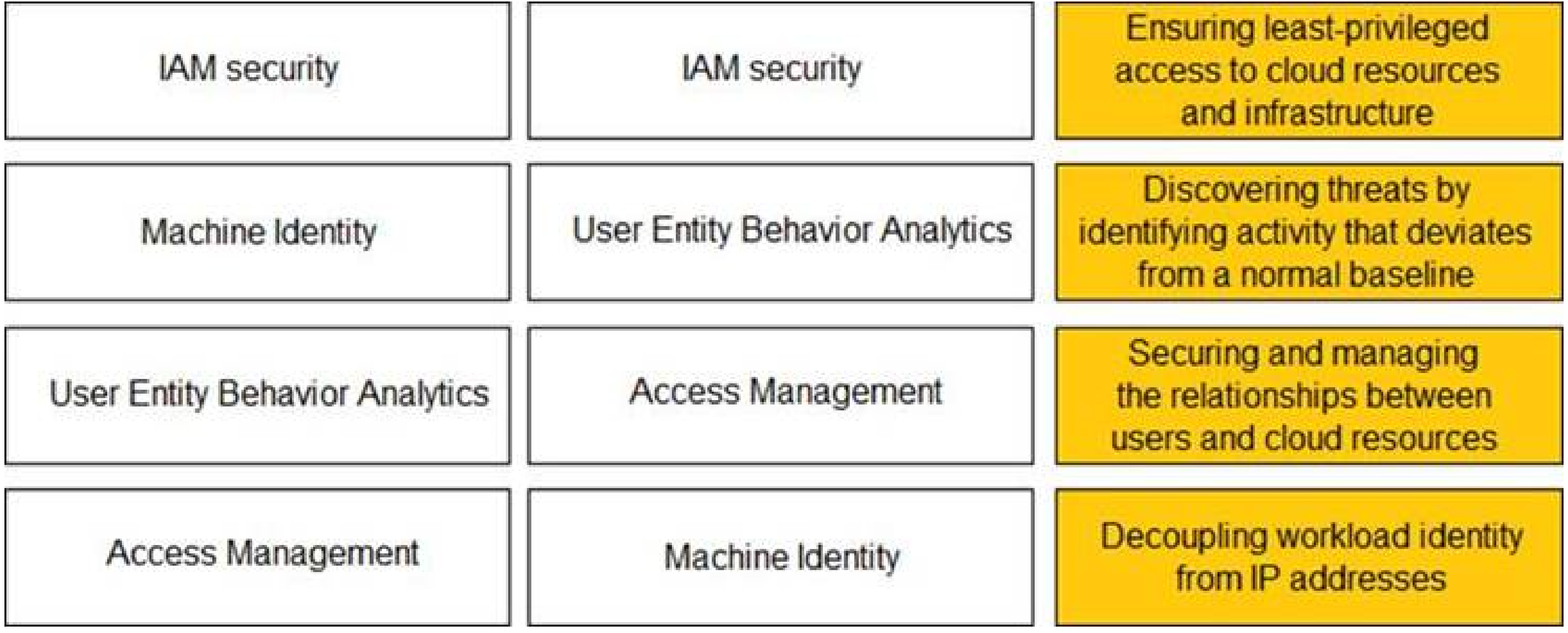


IAM security		Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity		Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics		Securing and managing the relationships between users and cloud resources
Access Management		Decoupling workload identity from IP addresses

A. Mastered
B. Not Mastered

Answer: A

Explanation:



IAM security	IAM security	Ensuring least-privileged access to cloud resources and infrastructure
Machine Identity	User Entity Behavior Analytics	Discovering threats by identifying activity that deviates from a normal baseline
User Entity Behavior Analytics	Access Management	Securing and managing the relationships between users and cloud resources
Access Management	Machine Identity	Decoupling workload identity from IP addresses

NEW QUESTION 4
A native hypervisor runs:

A. with extreme demands on network throughput
B. only on certain platforms
C. within an operating system's environment
D. directly on the host computer's hardware

Answer: D

Explanation:
Type 1 (native or bare metal). Runs directly on the host computer's hardware Type 2 (hosted). Runs within an operating system environment

NEW QUESTION 5
Which of the following is an AWS serverless service?

A. Beta
B. Kappa
C. Delta
D. Lambda

Answer: D

Explanation:
Examples of serverless environments include Amazon Lambda and Azure Functions. Many PaaS offerings, such as Pivotal Cloud Foundry, also are effectively serverless even if they have not historically been marketed as such. Although serverless may appear to lack the container-specific, cloud native attribute, containers are extensively used in the underlying implementations, even if those implementations are not exposed to end users directly.

NEW QUESTION 6
How does Prisma SaaS provide protection for Sanctioned SaaS applications?

A. Prisma SaaS connects to an organizations internal print and file sharing services to provide protection and sharing visibility
B. Prisma SaaS does not provide protection for Sanctioned SaaS applications because they are secure
C. Prisma access uses Uniform Resource Locator (URL) Web categorization to provide protection and sharing visibility
D. Prisma SaaS connects directly to sanctioned external service providers SaaS application service to provide protection and sharing visibility

Answer: D

Explanation:
Prisma SaaS connects directly to the applications themselves, therefore providing continuous silent monitoring of the risks within the sanctioned SaaS applications, with detailed visibility that is not possible with traditional security solutions.

NEW QUESTION 7
Which type of Software as a Service (SaaS) application provides business benefits, is fast to deploy, requires minimal cost and is infinitely scalable?

A. Benign
B. Tolerated
C. Sanctioned
D. Secure

Answer: C

NEW QUESTION 8
What does Palo Alto Networks Cortex XDR do first when an endpoint is asked to run an executable?

A. run a static analysis
B. check its execution policy
C. send the executable to WildFire
D. run a dynamic analysis

Answer: B

NEW QUESTION 9
Which attacker profile uses the internet to recruit members to an ideology, to train them, and to spread fear and include panic?

A. cybercriminals
B. state-affiliated groups
C. hacktivists
D. cyberterrorists

Answer: D

NEW QUESTION 10
Which network device breaks networks into separate broadcast domains?

A. Hub
B. Layer 2 switch
C. Router
D. Wireless access point

Answer: C

Explanation:
A layer 2 switch will break up collision domains but not broadcast domains. To break up broadcast domains you need a Layer 3 switch with vlan capabilities.

NEW QUESTION 10
Which Palo Alto subscription service identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs) through static and dynamic analysis in a scalable, virtual environment?

A. DNS Security
B. URL Filtering
C. WildFire
D. Threat Prevention

Answer: C

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. WildFire automatically disseminates updated protections in near-real time to immediately prevent threats from spreading; this occurs without manual intervention"

NEW QUESTION 12
In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?

A. Computer
B. Switch
C. Infrastructure
D. Cloud

Answer: D

Explanation:
Cortex XDR breaks the silos of traditional detection and response by natively integrating network, endpoint, and cloud data to stop sophisticated attacks

NEW QUESTION 14
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 tools ingest aggregated alerts from detection sources (such as SIEMs, network security tools, and mailboxes) before executing automatable, process-driven playbooks to enrich and respond to these alerts.

NEW QUESTION 18
On an endpoint, which method should you use to secure applications against exploits?

A. endpoint-based firewall
B. strong user passwords
C. full-disk encryption
D. software patches

Answer: D

Explanation:
New software vulnerabilities and exploits are discovered all the time and thus diligent software patch management is required by system and security administrators in every organization.

NEW QUESTION 23
Which Palo Alto Networks tools enable a proactive, prevention-based approach to network automation that accelerates security analysis?

A. MineMeld
B. AutoFocus
C. WildFire
D. Cortex XDR

Answer: B

Explanation:
"Palo Alto Networks AutoFocus enables a proactive, prevention-based approach to network security that puts automation to work for security professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS software and Panorama. AutoFocus speeds the security team’s existing workflows, which allows for in-depth investigation into suspicious activity, without additional specialized resources."

NEW QUESTION 27
In addition to local analysis, what can send unknown files to WildFire for discovery and deeper analysis to rapidly detect potentially unknown malware?

A. Cortex XDR

B. AutoFocus
C. MineMild
D. Cortex XSOAR

Answer: A

Explanation:
In addition to local analysis, Cortex XDR can send unknown files to WildFire for discovery and deeper analysis to rapidly detect.

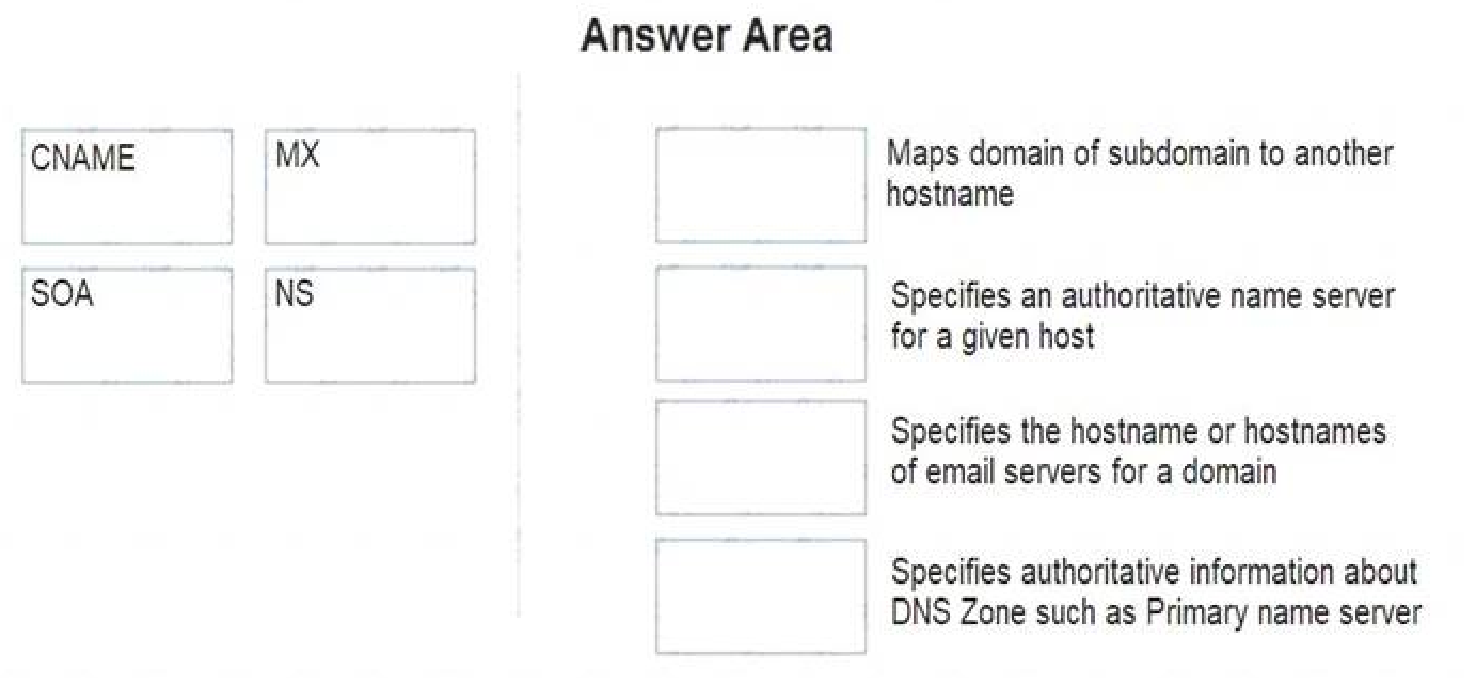
NEW QUESTION 29
In an IDS/IPS, which type of alarm occurs when legitimate traffic is improperly identified as malicious traffic?

A. False-positive
B. True-negative
C. False-negative
D. True-positive

Answer: A

Explanation:
In anti-malware, a false positive incorrectly identifies a legitimate file or application as malware. A false negative incorrectly identifies malware as a legitimate file or application. In intrusion detection, a false positive incorrectly identifies legitimate traffic as a threat, and a false negative incorrectly identifies a threat as legitimate traffic.

NEW QUESTION 32
Match the DNS record type to its function within DNS.



Answer Area

CNAME
MX
SOA
NS

Maps domain of subdomain to another hostname

Specifies an authoritative name server for a given host

Specifies the hostname or hostnames of email servers for a domain

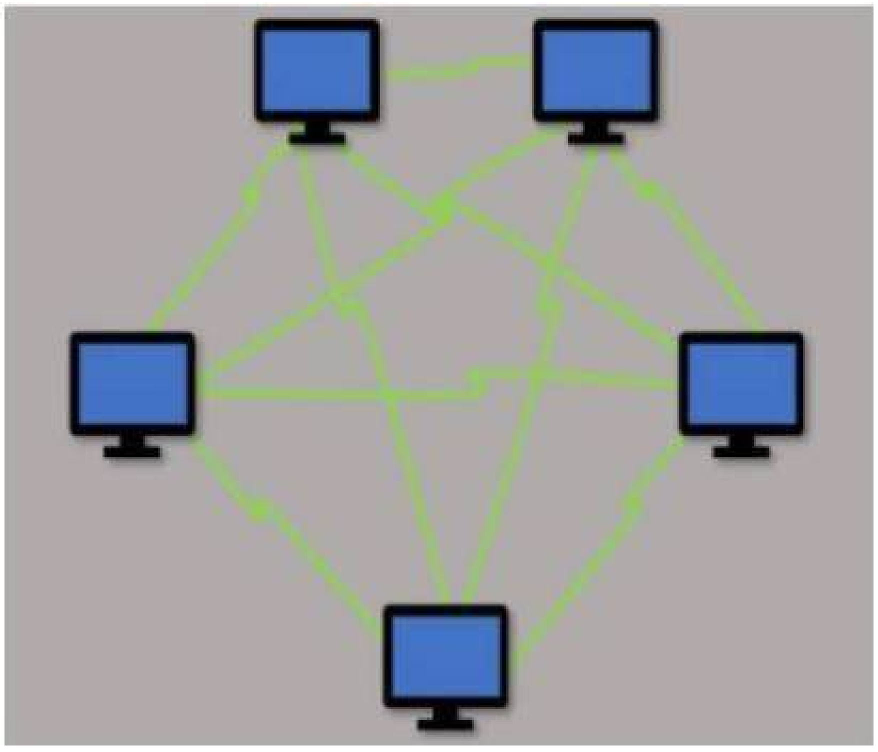
Specifies authoritative information about DNS Zone such as Primary name server

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The basic DNS record types are as follows:
A (IPv4) or AAAA (IPv6) (Address): Maps a domain or subdomain to an IP address or multiple IP addresses
CNAME (Canonical Name): Maps a domain or subdomain to another hostname
MX (Mail Exchanger): Specifies the hostname or hostnames of email servers for a domain PTR (Pointer): Points to a CNAME; commonly used for reverse DNS lookups that map an IP address to a host in a domain or subdomain
SOA (Start of Authority): Specifies authoritative information about a DNS zone such as primary name server, email address of the domain administrator, and domain serial number
NS (Name Server): The NS record specifies aan authoritative name server for a given host. TXT (Text): Stores text-based information

NEW QUESTION 33
Which type of LAN technology is being displayed in the diagram?



A. Star Topology
B. Spine Leaf Topology
C. Mesh Topology
D. Bus Topology

Answer: A

NEW QUESTION 38
Which Palo Alto Networks subscription service complements App-ID by enabling you to configure the next- generation firewall to identify and control access to websites and to protect your organization from websites hosting malware and phishing pages?

A. Threat Prevention
B. DNS Security
C. WildFire
D. URL Filtering

Answer: D

Explanation:
The URL Filtering service complements App-ID by enabling you to configure the next-generation firewall to identify and control access to websites and to protect your organization from websites that host malware and phishing pages.

NEW QUESTION 40
Anthem server breaches disclosed Personally Identifiable Information (PII) from a number of its servers. The infiltration by hackers was attributed to which type of vulnerability?

A. an intranet-accessed contractor’s system that was compromised
B. exploitation of an unpatched security vulnerability
C. access by using a third-party vendor’s password
D. a phishing scheme that captured a database administrator’s password

Answer: D

NEW QUESTION 45
How does DevSecOps improve the Continuous Integration/Continuous Deployment (CI/CD) pipeline?

A. DevSecOps improves pipeline security by assigning the security team as the lead team for continuousdeployment
B. DevSecOps ensures the pipeline has horizontal intersections for application code deployment
C. DevSecOps unites the Security team with the Development and Operations teams to integrate security into the CI/CD pipeline
D. DevSecOps does security checking after the application code has been processed through the CI/CD pipeline

Answer: C

Explanation:
DevSecOps takes the concept behind DevOps that developers and IT teams should work together closely, instead of separately, throughout software delivery and extends it to include security and integrate automated checks into the full CI/CD pipeline. The integration of the CI/CD pipeline takes care of the problem of security seeming like an outside force and instead allows developers to maintain their usual speed without compromising data security

NEW QUESTION 47
In a traditional data center what is one result of sequential traffic analysis?

A. simplifies security policy management
B. reduces network latency
C. causes security policies to be complex
D. improves security policy application ID enforcement

Answer: C

Explanation:
Multiple policies, no policy reconciliation tools: Sequential traffic analysis (stateful inspection, application control, intrusion prevention system (IPS), anti-malware, etc.) in traditional data center security solutions requires a corresponding security policy or profile, often using multiple management tools. The result is that your security policies become convoluted as you build and manage a firewall policy with source, destination, user, port, and action; an application control policy with similar rules; and any other threat prevention rules required. Multiple security policies that mix positive (firewall) and negative (application control, IPS, and anti-malware) control models can cause security holes by missing traffic and/or not identifying

NEW QUESTION 50
......

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PCCET Exam with Our Prep Materials Via below:

https://www.certleader.com/PCCET-dumps.html