Vendor: Palo Alto Networks

Exam Code:PCCET

Exam Name: Palo Alto Networks Certified
Cybersecurity Entry-level Technician

Version: Demo

QUESTION 1

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

Correct Answer: A

QUESTION 2

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

Correct Answer: D

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.

QUESTION 3

In which situation would a dynamic routing protocol be the quickest way to configure routes on a router?

A. the network is large

B. the network is small

C. the network has low bandwidth requirements

D. the network needs backup routes

Correct Answer: A

A static routing protocol requires that routes be created and updated manually on a router or other network device. If a static route is down, traffic can\\'t be automatically rerouted unless an alternate route has been configured. Also, if the route is congested, traffic can\\'t be automatically rerouted over the less congested alternate route. Static routing is

practical only in very small networks or for very limited, special-case routing scenarios (for example, a destination that\\'s used as a backup route or is reachable only via a single router). However, static routing has low bandwidth requirements (routing information isn\\'t broadcast across the network) and some built-in security (users can route only to destinations that are specified in statically defined routes).

QUESTION 4

Under which category does an application that is approved by the IT department, such as Office 365, fall?

A. unsanctioned

B. prohibited

C. tolerated

D. sanctioned

Correct Answer: D

QUESTION 5

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

Correct Answer: B

"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."

QUESTION 6

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 continuous deployment

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

Correct Answer: C

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

---

QUESTION 7

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

Correct Answer: D

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

---

QUESTION 8

How does adopting a serverless model impact application development?

A. costs more to develop application code because it uses more compute resources

B. slows down the deployment of application code, but it improves the quality of code development

C. reduces the operational overhead necessary to deploy application code

D. prevents developers from focusing on just the application code because you need to provision the underlying infrastructure to run the code

Correct Answer: C

List three advantages of serverless computing over CaaS: - Reduce costs - Increase agility - Reduce operational overhead

---

QUESTION 9

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

Correct Answer: A

QUESTION 10

During the OSI layer 3 step of the encapsulation process, what is the Protocol Data Unit (PDU) called when the IP stack adds source (sender) and destination (receiver) IP addresses?

A. Frame

B. Segment

C. Packet

D. Data

Correct Answer: C

The IP stack adds source (sender) and destination (receiver) IP addresses to the TCP segment (which now is called an IP packet) and notifies the server operating system that it has an outgoing message ready to be sent across the network.

QUESTION 11

DRAG DROP

Match the description with the VPN technology.

Select and Place:

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.		Generic Routing Encapsulation
Supported by most operating systems and provides no encryption by itself.		Layer 2 Tunneling Protocol
A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.		Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection		Secure Socket Tunneling Protocol

Correct Answer:

	A tunneling protocol developed by Cisco Systems that can various network layer protocols inside point-to-point links.	Generic Routing Encapsulation
	Supported by most operating systems and provides no encryption by itself.	Layer 2 Tunneling Protocol
	A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Internet Protocol Security
	Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	Secure Socket Tunneling Protocol

QUESTION 12

Which IPsec feature allows device traffic to go directly to the Internet?

A. Split tunneling

B. Diffie-Hellman groups

C. d.Authentication Header (AH)

D. IKE Security Association

Correct Answer: A

"Or split tunneling can be configured to allow internet traffic from the device to go directly to the internet, while other specific types of traffic route through the IPsec tunnel, for acceptable protection with much less performance degradation."