PCCET$^{Q\&As}$

Palo Alto Networks Certified Cybersecurity Entry-level Technician

Pass Palo Alto Networks PCCET Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/pccet.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

Which endpoint tool or agent can enact behavior-based protection?

A. AutoFocus

B. Cortex XDR

C. DNS Security

D. MineMeld

Correct Answer: B

QUESTION 2

Which item accurately describes a security weakness that is caused by implementing a "ports first" data security solution in a traditional data center?

A. You may have to use port numbers greater than 1024 for your business-critical applications.

B. You may have to open up multiple ports and these ports could also be used to gain unauthorized entry into your datacenter.

C. You may not be able to assign the correct port to your business-critical applications.

D. You may not be able to open up enough ports for your business-critical applications which will increase the attack surface area.

Correct Answer: B

QUESTION 3

Which option is an example of a North-South traffic flow?

A. Lateral movement within a cloud or data center

B. An internal three-tier application

C. Client-server interactions that cross the edge perimeter

D. Traffic between an internal server and internal user

Correct Answer: C

North-south refers to data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center. North-south traffic is secured by one or more physical form factor perimeter edge firewalls.

QUESTION 4

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

Correct Answer: A

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.

QUESTION 5

Which key component is used to configure a static route?

A. router ID

B. enable setting

C. routing protocol

D. next hop IP address

Correct Answer: D

QUESTION 6

Which core component is used to implement a Zero Trust architecture?

A. VPN Concentrator

B. Content Identification

C. Segmentation Platform

D. Web Application Zone

Correct Answer: C

"Remember that a trust zone is not intended to be a "pocket of trust" where systems (and therefore threats) within the zone can communicate freely and directly with each other. For a full Zero Trust implementation, the network would be configured to ensure that all communications traffic, including traffic between devices in the same zone, is intermediated by the corresponding Zero Trust Segmentation Platform."

QUESTION 7

Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) fall under which Prisma access service layer?

A. Network

B. Management

C. Cloud

D. Security

Correct Answer: D

A SASE solution converges networking and security services into one unified, cloud-delivered solution (see Figure 3-12) that includes the following:

Networking

Software-defined wide-area networks (SD-WANs)

Virtual private networks (VPNs)

Zero Trust network access (ZTNA)

Quality of Service (QoS)

Security

Firewall as a service (FWaaS)

Domain Name System (DNS) security

Threat prevention

Secure web gateway (SWG)

Data loss prevention (DLP)

Cloud access security broker (CASB)

QUESTION 8

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

Correct Answer: AC

A directory service is a database that contains information about users, resources, and services in a network.

QUESTION 9

What does SIEM stand for?

A. Security Infosec and Event Management

B. Security Information and Event Management

C. Standard Installation and Event Media

D. Secure Infrastructure and Event Monitoring

Correct Answer: B

Originally designed as a tool to assist organizations with compliance and industry-specific regulations, security information and event management (SIEM) is a technology that has been around for almost two decades

QUESTION 10

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

Correct Answer: ADE

QUESTION 11

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

Correct Answer: C

"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"

QUESTION 12

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 13

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 14

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 15

Which classification of IDS/IPS uses a database of known vulnerabilities and attack profiles to identify intrusion attempts?

A. Statistical-based

B. Knowledge-based

C. Behavior-based

D. Anomaly-based

Correct Answer: B

A knowledge-based system uses a database of known vulnerabilities and attack profiles to identify intrusion attempts. These types of systems have lower false-alarm rates than behavior-based systems but must be continually updated with new attack signatures to be effective. A behavior-based system uses a baseline of normal network activity to identify unusual patterns or levels of network activity that may be indicative of an intrusion attempt. These types of systems are more adaptive than knowledge-based systems and therefore may be more effective in detecting previously unknown vulnerabilities and attacks, but they have a much higher false-positive rate than knowledge- based systems.