

Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician



NEW QUESTION 1

Which of the following is a service that allows you to control permissions assigned to users in order for them to access and utilize cloud resources?

- A. User-ID
- B. Lightweight Directory Access Protocol (LDAP)
- C. User and Entity Behavior Analytics (UEBA)
- D. Identity and Access Management (IAM)

Answer: D

Explanation:

Identity and access management (IAM) is a software service or framework that allows organizations to define user or group identities within software environments, then associate permissions with them. The identities and permissions are usually spelled out in a text file, which is referred to as an IAM policy.

NEW QUESTION 2

In which phase of the cyberattack lifecycle do attackers establish encrypted communication channels back to servers across the internet so that they can modify their attack objectives and methods?

- A. exploitation
- B. actions on the objective
- C. command and control
- D. installation

Answer: C

Explanation:

Command and Control: Attackers establish encrypted communication channels back to command-and-control (C2) servers across the internet so that they can modify their attack objectives and methods as additional targets of opportunity are identified within the victim network, or to evade any new security countermeasures that the organization may attempt to deploy if attack artifacts are discovered.

NEW QUESTION 3

Why have software developers widely embraced the use of containers?

- A. Containers require separate development and production environments to promote authentic code.
- B. Containers share application dependencies with other containers and with their host computer.
- C. Containers simplify the building and deploying of cloud native applications.
- D. Containers are host specific and are not portable across different virtual machine hosts.

Answer: C

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 TCP/IP sub-protocol operates at the Layer7 of the OSI model?

- A. UDP
- B. MAC
- C. SNMP
- D. NFS

Answer: C

Explanation:

Application (Layer 7 or L7): This layer identifies and establishes availability of communication partners, determines resource availability, and synchronizes communication.

Presentation (Layer 6 or L6): This layer provides coding and conversion functions (such as data representation, character conversion, data compression, and data encryption) to ensure that data sent from the Application layer of one system is compatible with the Application layer of the receiving system.

Session (Layer 5 or L5): This layer manages communication sessions (service requests and service responses) between networked systems, including connection establishment, data transfer, and connection release.

Transport (Layer 4 or L4): This layer provides transparent, reliable data transport and end-to-end transmission control.

NEW QUESTION 6

Which Palo Alto Networks tool is used to prevent endpoint systems from running malware executables such as viruses, trojans, and rootkits?

- A. Expedition
- B. Cortex XDR
- C. AutoFocus
- D. App-ID

Answer: B

NEW QUESTION 7

Systems that allow for accelerated incident response through the execution of standardized and automated playbooks that work upon inputs from security technology and other data flows are known as what?

- A. XDR
- B. STEP
- C. SOAR
- D. SIEM

Answer: C

NEW QUESTION 8

Which endpoint product from Palo Alto Networks can help with SOC visibility?

- A. STIX
- B. Cortex XDR
- C. WildFire
- D. AutoFocus

Answer: B

Explanation:

XDR solutions bring a proactive approach to threat detection and response. It delivers visibility across all data, including endpoint, network, and cloud data, while applying analytics and automation to address today's increasingly sophisticated threats. With XDR, cybersecurity teams can:

- Identify hidden, stealthy, and sophisticated threats proactively and quickly
- Track threats across any source or location within the organization
- Increase the productivity of the people operating the technology
- Get more out of their security investments
- Conclude investigations more efficiently

NEW QUESTION 9

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 10

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 10

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 13

What are three benefits of SD-WAN infrastructure? (Choose three.)

- A. Improving performance of SaaS applications by requiring all traffic to be back-hauled through the corporate headquarters network
- B. Promoting simplicity through the utilization of a centralized management structure
- C. Utilizing zero-touch provisioning for automated deployments
- D. Leveraging remote site routing technical support by relying on MPLS

E. Improving performance by allowing efficient access to cloud-based resources without requiring back-haul traffic to a centralized location

Answer: BCE

Explanation:

Simplicity: Because each device is centrally managed, with routing based on application policies, WAN managers can create and update security rules in real time as network requirements change. Also, when SD-WAN is combined with zero-touch provisioning, a feature that helps automate the deployment and configuration processes, organizations can further reduce the complexity, resources, and operating expenses required to spin up new sites. **Improved performance:** By allowing efficient access to cloud-based resources without the need to backhaul traffic to centralized locations, organizations can provide a better user experience.

NEW QUESTION 14

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: ADE

NEW QUESTION 18

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

Answer: C

Explanation:

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.

NEW QUESTION 20

Which product from Palo Alto Networks extends the Security Operating Platform with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows?

- A. Global Protect
- B. WildFire
- C. AutoFocus
- D. STIX

Answer: C

Explanation:

page 173 "AutoFocus makes over a billion samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts. AutoFocus extends the product portfolio with the global threat intelligence and attack context needed to accelerate analysis, forensics, and hunting workflows. Together, the platform and AutoFocus move security teams away from legacy manual approaches that rely on aggregating a growing number of detectionbased alerts and post-event mitigation, to preventing sophisticated attacks and enabling proactive hunting activities."

NEW QUESTION 22

Which not-for-profit organization maintains the common vulnerability exposure catalog that is available through their public website?

- A. Department of Homeland Security
- B. MITRE
- C. Office of Cyber Security and Information Assurance
- D. Cybersecurity Vulnerability Research Center

Answer: B

NEW QUESTION 27

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 28

On an endpoint, which method is used to protect proprietary data stored on a laptop that has been stolen?

- A. operating system patches
- B. full-disk encryption
- C. periodic data backups
- D. endpoint-based firewall

Answer: B

NEW QUESTION 33

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.

Answer: B

NEW QUESTION 36

An Administrator wants to maximize the use of a network address. The network is 192.168.6.0/24 and there are three subnets that need to be created that can not overlap. Which subnet would you use for the network with 120 hosts?

Requirements for the three subnets: Subnet 1: 3 host addresses Subnet 2: 25 host addresses

Subnet 3: 120 host addresses

- A. 192.168.6.168/30
- B. 192.168.6.0/25
- C. 192.168.6.160/29
- D. 192.168.6.128/27

Answer: B

NEW QUESTION 39

Which element of the security operations process is concerned with using external functions to help achieve goals?

- A. interfaces
- B. business
- C. technology
- D. people

Answer: A

Explanation:

The six pillars include:

- * 1. Business (goals and outcomes)
- * 2. People (who will perform the work)
- * 3. Interfaces (external functions to help achieve goals)
- * 4. Visibility (information needed to accomplish goals)
- * 5. Technology (capabilities needed to provide visibility and enable people)
- * 6. Processes (tactical steps required to execute on goals)

NEW QUESTION 40

Which pillar of Prisma Cloud application security addresses ensuring that your cloud resources and SaaS applications are correctly configured?

- A. visibility, governance, and compliance
- B. network protection
- C. dynamic computing
- D. compute security

Answer: A

Explanation:

Ensuring that your cloud resources and SaaS applications are correctly configured and adhere to your organization's security standards from day one is essential to prevent successful attacks. Also, making sure that these applications, and the data they collect and store, are properly protected and compliant is critical to avoid costly fines, a tarnished image, and loss of customer trust. Meeting security standards and maintaining compliant environments at scale, and across SaaS applications, is the new expectation for security teams.

NEW QUESTION 43

Why is it important to protect East-West traffic within a private cloud?

- A. All traffic contains threats, so enterprises must protect against threats across the entire network
- B. East-West traffic contains more session-oriented traffic than other traffic
- C. East-West traffic contains more threats than other traffic
- D. East-West traffic uses IPv6 which is less secure than IPv4

Answer:

A

NEW QUESTION 47

Match the IoT connectivity description with the technology.

a proprietary multicast wireless sensor network technology primarily used in personal wearables		Bluetooth (BLE)
a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology		802.11
a wireless protocol defined by the Institute of Electrical and Electronics Engineers (IEEE)		Adaptive Network Technology (ANT+)
a low-energy wireless mesh network protocol primarily used for home automation applications		Z-Wave

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Short-range wireless:

Adaptive Network Technology+ (ANT+): ANT+ is a proprietary multicast wireless sensor network technology primarily used in personal wearables, such as sports and fitness sensors.

Bluetooth/Bluetooth Low-Energy (BLE): Bluetooth is a low-power, short-range communications technology primarily designed for point-to-point communications between wireless devices in a hub-and-spoke topology. BLE (also known as Bluetooth Smart or Bluetooth 4.0+) devices consume significantly less power than Bluetooth devices and can access the internet directly through 6LoWPAN connectivity.

Internet Protocol version 6 (IPv6) over Low-Power Wireless Personal Area Networks (6LoWPAN): 6LoWPAN allows IPv6 traffic to be carried over low-power wireless mesh networks. 6LoWPAN is designed for nodes and applications that require wireless internet connectivity at relatively low data rates in small form factors, such as smart light bulbs and smart meters.

Wi-Fi/802.11: The Institute of Electrical and Electronics Engineers (IEEE) defines the 802 LAN protocol standards. 802.11 is the set of standards used for Wi-Fi networks typically operating in the 2.4GHz and 5GHz frequency bands. The most common implementations today include:

* 802.11n (labeled Wi-Fi 4 by the Wi-Fi Alliance), which operates on both 2.4GHz and 5GHz bands at ranges from 54Mbps to 600Mbps

* 802.11ac (Wi-Fi 5), which operates on the 5GHz band at ranges from 433Mbps to 3.46 Gbps

* 802.11ax (Wi-Fi 6), which operates on the 2.4GHz and 5GHz bands (and all bands between 1 and 6GHz, when they become available for 802.11 use) at ranges up to 11Gbps

Z-Wave: Z-Wave is a low-energy wireless mesh network protocol primarily used for home automation applications such as smart appliances, lighting control, security systems, smart thermostats, windows and locks, and garage doors.

Zigbee/802.15.4: Zigbee is a low-cost, low-power wireless mesh network protocol based on the IEEE 802.15.4 standard. Zigbee is the dominant protocol in the low-power networking market, with a large installed base in industrial environments and smart home products.

NEW QUESTION 51

Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?

- A. Group policy
 B. Stateless
 C. Stateful
 D. Static packet-filter

Answer: C

Explanation:

Stateful packet inspection firewalls Second-generation stateful packet inspection (also known as dynamic packet filtering) firewalls have the following characteristics:

They operate up to Layer 4 (Transport layer) of the OSI model and maintain state information about the communication sessions that have been established between hosts on the trusted and untrusted networks.

They inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, and ICMP), and port number (during session establishment only) to determine whether the session should be allowed, blocked, or dropped based on configured firewall rules. After a permitted connection is established between two hosts, the firewall creates and deletes firewall rules for individual connections as needed, thus effectively creating a tunnel that allows traffic to flow between the two hosts without further inspection of individual packets during the session. This type of firewall is very fast, but it is port-based and it is highly dependent on the trustworthiness of the two hosts because individual packets aren't inspected after the connection is established.

NEW QUESTION 55

What are two key characteristics of a Type 1 hypervisor? (Choose two.)

- A. is hardened against cyber attacks
- B. runs without any vulnerability issues
- C. runs within an operating system
- D. allows multiple, virtual (or guest) operating systems to run concurrently on a single physical host computer

Answer: CD

NEW QUESTION 56

Match the DNS record type to its function within DNS.

Answer Area

CNAME	MX	<input type="text"/>	Maps domain of subdomain to another hostname
SOA	NS	<input type="text"/>	Specifies an authoritative name server for a given host
		<input type="text"/>	Specifies the hostname or hostnames of email servers for a domain
		<input type="text"/>	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 an authoritative name server for a given host. TXT (Text): Stores text-based information

NEW QUESTION 61

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 66

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

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 69

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

Answer: A

NEW QUESTION 74

Which tool supercharges security operations center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security?

- A. Prisma SAAS
- B. WildFire
- C. Cortex XDR
- D. Cortex XSOAR

Answer: D

Explanation:

Cortex XSOAR enhances Security Operations Center (SOC) efficiency with the world's most comprehensive operating platform for enterprise security. Cortex XSOAR unifies case management, automation, real-time collaboration, and native threat intel management in the industry's first extended security orchestration, automation, and response (SOAR) offering.

NEW QUESTION 78

Which aspect of a SaaS application requires compliance with local organizational security policies?

- A. Types of physical storage media used
- B. Data-at-rest encryption standards
- C. Acceptable use of the SaaS application
- D. Vulnerability scanning and management

Answer: C

NEW QUESTION 82

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 83

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

PCCET Practice Exam Features:

- * PCCET Questions and Answers Updated Frequently
- * PCCET Practice Questions Verified by Expert Senior Certified Staff
- * PCCET Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * PCCET Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PCCET Practice Test Here](#)