

Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician



NEW QUESTION 1

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 2

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 3

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 4

The customer is responsible only for which type of security when using a SaaS application?

- A. physical

- B. platform
- C. data
- D. infrastructure

Answer: C

NEW QUESTION 5

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

Answer: A

Explanation:

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).

NEW QUESTION 6

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 7

What is the key to "taking down" a botnet?

- A. prevent bots from communicating with the C2
- B. install openvas software on endpoints
- C. use LDAP as a directory service
- D. block Docker engine software on endpoints

Answer: A

NEW QUESTION 8

In which step of the cyber-attack lifecycle do hackers embed intruder code within seemingly innocuous files?

- A. weaponization
- B. reconnaissance
- C. exploitation
- D. delivery

Answer: A

Explanation:

"Weaponization: Next, attackers determine which methods to use to compromise a target endpoint. They may choose to embed intruder code within seemingly innocuous files such as a PDF or Microsoft Word document or email message."

NEW QUESTION 9

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

- A. VPN Concentrator
- B. Content Identification
- C. Segmentation Platform
- D. Web Application Zone

Answer: C

Explanation:

"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."

NEW QUESTION 10

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 10

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 13

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 14

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 18

In SecOps, what are two of the components included in the identify stage? (Choose two.)

- A. Initial Research
- B. Change Control
- C. Content Engineering
- D. Breach Response

Answer: AC

NEW QUESTION 23

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 26

Which technique changes protocols at random during a session?

- A. use of non-standard ports
- B. port hopping
- C. hiding within SSL encryption
- D. tunneling within commonly used services

Answer: B

Explanation:

Port hopping, in which ports and protocols are randomly changed during a session.

NEW QUESTION 29

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

Answer: D

Explanation:

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)

NEW QUESTION 33

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 38

What is a characteristic of the National Institute Standards and Technology (NIST) defined cloud computing model?

- A. requires the use of only one cloud service provider
- B. enables on-demand network services
- C. requires the use of two or more cloud service providers
- D. defines any network service

Answer: B

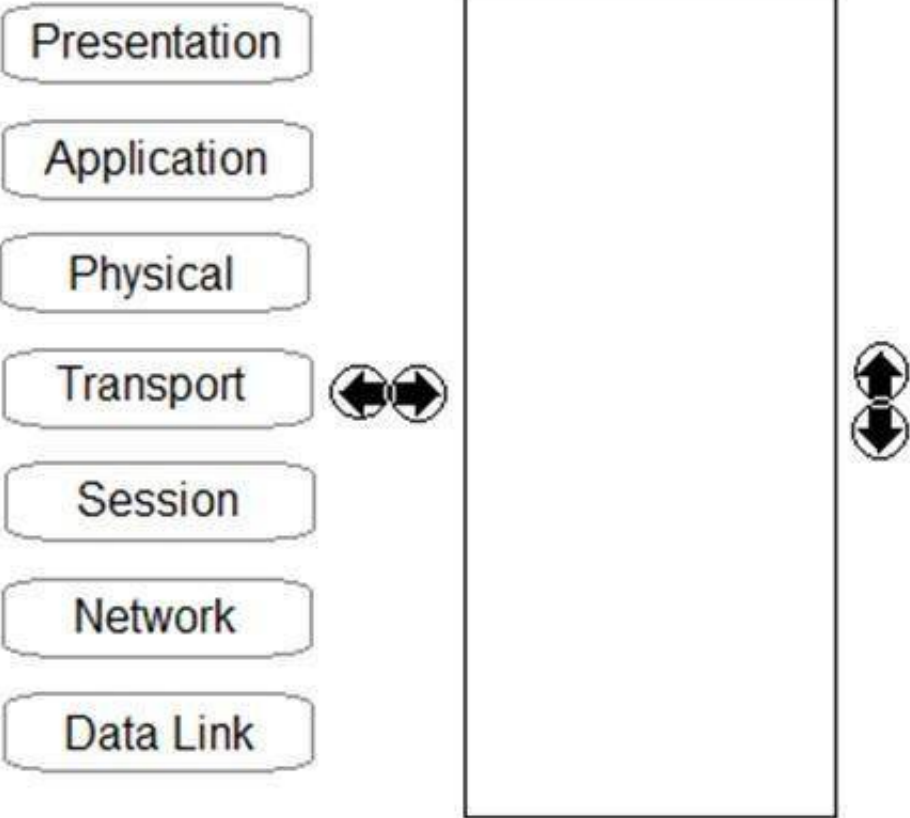
Explanation:

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner.

NEW QUESTION 43

Order the OSI model with Layer7 at the top and Layer1 at the bottom.

Unordered Options Ordered Options

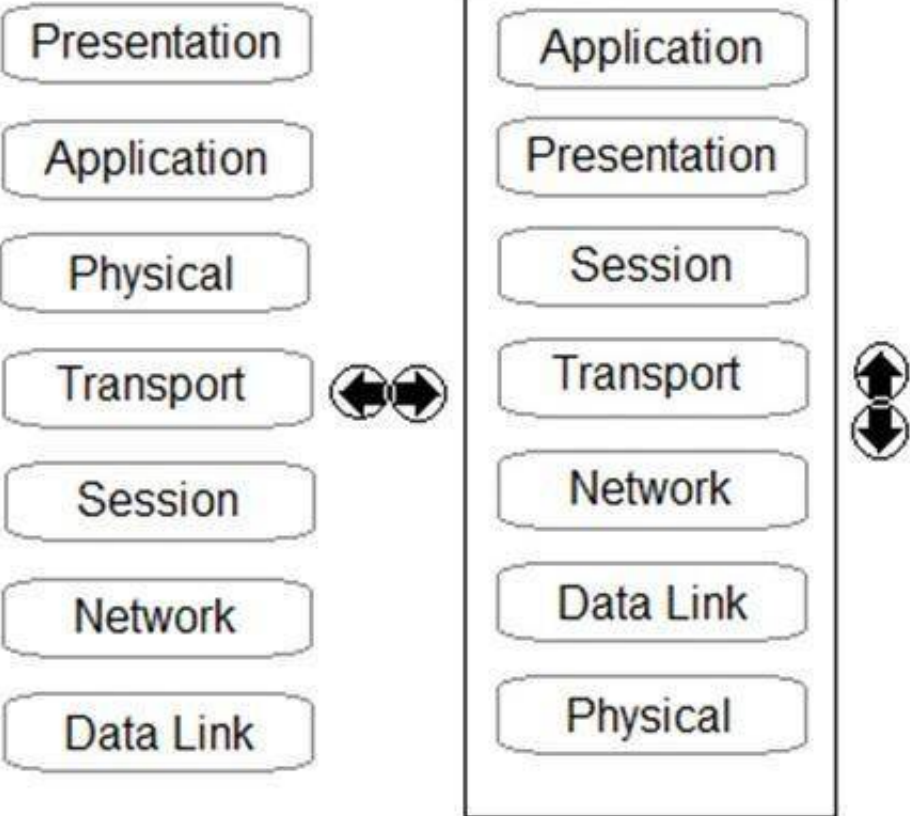


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Unordered Options Ordered Options



NEW QUESTION 48

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 53

Which option describes the “selective network security virtualization” phase of incrementally transforming data centers?

- A. during the selective network security virtualization phase, all intra-host communication paths are strictly controlled
- B. during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server
- C. during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol
- D. during the selective network security virtualization phase, all intra-host traffic is load balanced

Answer: A

Explanation:

Selective network security virtualization: Intra-host communications and live migrations are architected at this phase. All intra-host communication paths are strictly controlled to ensure that traffic between VMs at different trust levels is intermediated either by an on-box, virtual security appliance or by an off-box, physical security appliance.

NEW QUESTION 54

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 55

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 57

Which organizational function is responsible for security automation and eventual vetting of the solution to help ensure consistency through machine-driven responses to security issues?

- A. NetOps
- B. SecOps
- C. SecDevOps
- D. DevOps

Answer: B

Explanation:

Security operations (SecOps) is a necessary function for protecting the digital way of life, for global businesses and customers. SecOps requires continuous improvement in operations to handle fast-evolving threats. SecOps needs to arm security operations professionals with high-fidelity intelligence, contextual data, and automated prevention workflows to quickly identify and respond to these threats. SecOps must leverage automation to reduce strain on analysts and execute the Security Operation Center's (SOC) mission to identify, investigate, and mitigate threats.

NEW QUESTION 59

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 63

Which method is used to exploit vulnerabilities, services, and applications?

- A. encryption
- B. port scanning
- C. DNS tunneling

D. port evasion

Answer: D

Explanation:

Attack communication traffic is usually hidden with various techniques and tools, including:

Encryption with SSL, SSH (Secure Shell), or some other custom or proprietary encryption Circumvention via proxies, remote access tools, or tunneling. In some instances, use of cellular networks enables complete circumvention of the target network for attack C2 traffic. Port evasion using network anonymizers or port hopping to traverse over any available open ports

Fast Flux (or Dynamic DNS) to proxy through multiple infected endpoints or multiple, ever-changing C2 servers to reroute traffic and make determination of the true destination or attack source difficult

DNS tunneling is used for C2 communications and data infiltration

NEW QUESTION 66

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 67

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 71

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 74

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 75

What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

- A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
- B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
- C. control and protect inter-host traffic by using IPv4 addressing
- D. control and protect inter-host traffic using physical network security appliances

Answer: D

Explanation:

page 211 "Consolidating servers within trust levels: Organizations often consolidate servers within the same trust level into a single virtual computing environment:

... .. This virtual systems capability enables a single physical device to be used to simultaneously meet the unique requirements of multiple VMs or groups of VMs. Control and protection of inter-host traffic with physical network security appliances that are properly positioned and configured is the primary security focus."

NEW QUESTION 79

Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

- A. Dynamic
- B. Pre-exploit protection
- C. Bare-metal
- D. Static

Answer: A

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.

NEW QUESTION 83

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 86

Which characteristic of serverless computing enables developers to quickly deploy application code?

- A. Uploading cloud service autoscaling services to deploy more virtual machines to run their application code based on user demand
- B. Uploading the application code itself, without having to provision a full container image or any OS virtual machine components
- C. Using cloud service spot pricing to reduce the cost of using virtual machines to run their application code
- D. Using Container as a Service (CaaS) to deploy application containers to run their code.

Answer: B

Explanation:

"In serverless apps, the developer uploads only the app package itself, without a full container image or any OS components. The platform dynamically packages it into an image, runs the image in a container, and (if needed) instantiates the underlying host OS and VM and the hardware required to run them."

NEW QUESTION 91

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-W ave: 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/802.14: 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 96

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 97

Which NGFW feature is used to provide continuous identification, categorization, and control of known and previously unknown SaaS applications?

- A. User-ID
 B. Device-ID

- C. App-ID
- D. Content-ID

Answer: C

Explanation:

App-ID™ technology leverages the power of the broad global community to provide continuous identification, categorization, and granular risk-based control of known and previously unknown SaaS applications, ensuring new applications are discovered automatically as they become popular.

NEW QUESTION 100

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 101

Which IoT connectivity technology is provided by satellites?

- A. 4G/LTE
- B. VLF
- C. L-band
- D. 2G/2.5G

Answer: C

Explanation:

2G/2.5G: 2G connectivity remains a prevalent and viable IoT connectivity option due to the low cost of 2G modules, relatively long battery life, and large installed base of 2G sensors and M2M applications.

3G: IoT devices with 3G modules use either Wideband Code Division Multiple Access (W-CDMA) or Evolved High Speed Packet Access (HSPA+ and Advanced HSPA+) to

achieve data transfer rates of 384Kbps to 168Mbps.

4G/Long-Term Evolution (LTE): 4G/LTE networks enable real-time IoT use cases, such as autonomous vehicles, with 4G LTE Advanced Pro delivering speeds in excess of 3Gbps and less than 2 milliseconds of latency.

5G: 5G cellular technology provides significant enhancements compared to 4G/LTE networks and is backed by ultra-low latency, massive connectivity and scalability for IoT devices, more efficient use of the licensed spectrum, and network slicing for application traffic prioritization.

NEW QUESTION 106

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 111

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 112

.....

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](#)