



Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

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

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

Which statement describes DevOps?

- A. DevOps is its own separate team
- B. DevOps is a set of tools that assists the Development and Operations teams throughout the software delivery process
- C. DevOps is a combination of the Development and Operations teams
- D. DevOps is a culture that unites the Development and Operations teams throughout the software delivery process

Answer: D

Explanation:

DevOps is not:

A combination of the Dev and Ops teams: There still are two teams; they just operate in a communicative, collaborative way.

Its own separate team: There is no such thing as a “DevOps engineer.” Although some companies may appoint a “DevOps team” as a pilot when trying to transition to a DevOps culture, DevOps refers to a culture where developers, testers, and operations personnel cooperate throughout the entire software delivery lifecycle.

A tool or set of tools: Although there are tools that work well with a DevOps model or help promote DevOps culture, DevOps ultimately is a strategy, not a tool.

Automation: Although automation is very important for a DevOps culture, it alone does not define DevOps.

NEW QUESTION 6

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 7

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 8

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 9

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

Which option would be an example of PII that you need to prevent from leaving your enterprise network?

- A. Credit card number
- B. Trade secret
- C. National security information
- D. A symmetric encryption key

Answer: A

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 11

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 15

Which Palo Alto Networks product provides playbooks with 300+ multivendor integrations that help solve any security use case?

- A. Cortex XSOAR
- B. Prisma Cloud
- C. AutoFocus
- D. Cortex XDR

Answer: A

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.
<https://www.paloaltonetworks.com/cortex/security-operations-automation>

NEW QUESTION 17

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 22

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

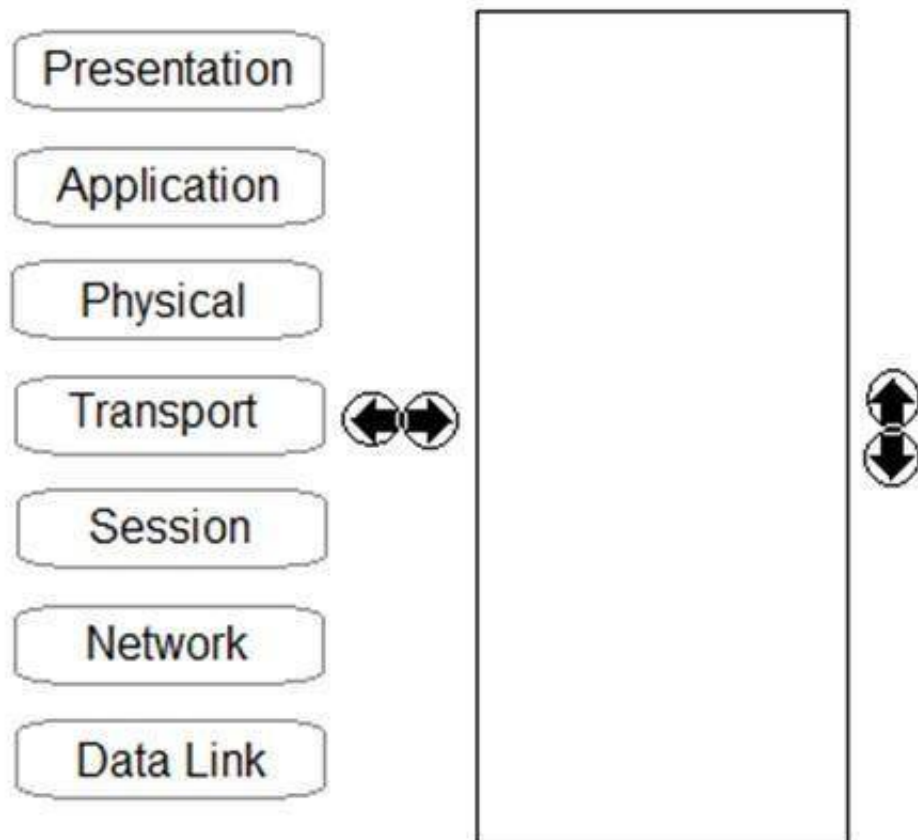
Explanation:

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

NEW QUESTION 26

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

Unordered Options Ordered Options

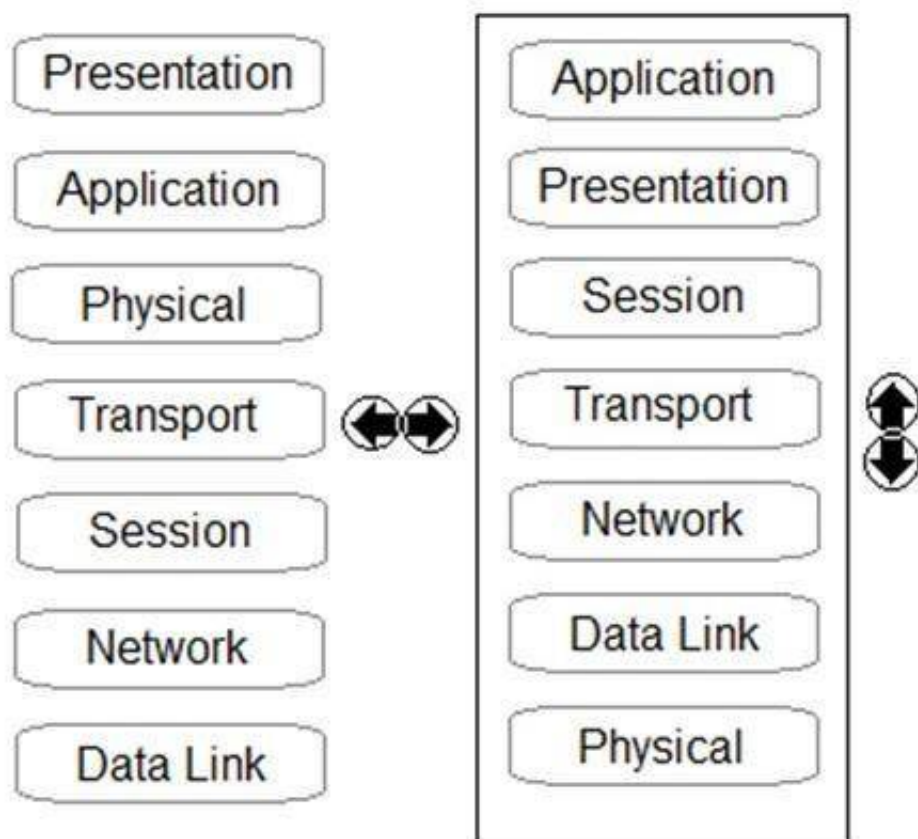


- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Unordered Options Ordered Options



NEW QUESTION 30

Which pillar of Prisma Cloud application security does vulnerability management fall under?

- A. dynamic computing
- B. identity security
- C. compute security
- D. network protection

Answer: C

Explanation:

Prisma Cloud comprises four pillars:

Visibility, governance, and compliance. Gain deep visibility into the security posture of multicloud environments. Track everything that gets deployed with an automated asset inventory, and maintain compliance with out-of-the-box governance policies that enforce good behavior across your environments.

Compute security. Secure hosts, containers, and serverless workloads throughout the application lifecycle. Detect and prevent risks by integrating vulnerability intelligence into your integrated development environment (IDE), software configuration management (SCM), and CI/CD workflows. Enforce machine learning-based runtime protection to protect applications and workloads in real time.

Network protection. Continuously monitor network activity for anomalous behavior, enforce microservice-aware micro-segmentation, and implement industry-leading firewall protection. Protect the network perimeter and the connectivity between containers and hosts.

Identity security. Monitor and leverage user and entity behavior analytics (UEBA) across your environments to detect and block malicious actions. Gain visibility into and enforce governance p

NEW QUESTION 34

In which two cloud computing service models are the vendors responsible for vulnerability and patch management of the underlying operating system? (Choose two.)

- A. SaaS
- B. PaaS
- C. On-premises
- D. IaaS

Answer: AB

NEW QUESTION 38

Which term describes data packets that move in and out of the virtualized environment from the host network or a corresponding traditional data center?

- A. North-South traffic
- B. Intrazone traffic
- C. East-West traffic
- D. Interzone traffic

Answer: A

NEW QUESTION 39

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 41

Match the description with the VPN technology.

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

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	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.	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.	A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Internet Protocol Security
A tunneling protocol that uses the Internet Key Exchange (IKE) to start a connection	Primarily used for secure remote client VPN rather than for site-to-site VPN tunnels.	Secure Socket Tunneling Protocol

NEW QUESTION 42

Which type of malware replicates itself to spread rapidly through a computer network?

- A. ransomware
 B. Trojan horse
 C. virus
 D. worm

Answer: D

Explanation:

A worm replicates through the network while a virus replicates, not necessarily to spread through the network.

NEW QUESTION 45

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 50

SecOps consists of interfaces, visibility, technology, and which other three elements? (Choose three.)

- A. People
 B. Accessibility
 C. Processes
 D. Understanding
 E. Business

Answer: ACE

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)

All elements must tie back to the business itself and the goals of the security operations

NEW QUESTION 54

Which three layers of the OSI model correspond to the Application Layer (L4) of the TCP/IP model?

- A. Session, Transport, Network
- B. Application, Presentation, and Session
- C. Physical, Data Link, Network
- D. Data Link, Session, Transport

Answer: B

Explanation:

Application (Layer 4 or L4): This layer loosely corresponds to Layers 5 through 7 of the OSI model. Transport (Layer 3 or L3): This layer corresponds to Layer 4 of the OSI model.

Internet (Layer 2 or L2): This layer corresponds to Layer 3 of the OSI model.

Network Access (Layer 1 or L1): This layer corresponds to Layers 1 and 2 of the OSI model

NEW QUESTION 56

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 57

Which subnet does the host 192.168.19.36/27 belong?

- A. 192.168.19.0
- B. 192.168.19.16
- C. 192.168.19.64
- D. 192.168.19.32

Answer: D

NEW QUESTION 59

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 61

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 63

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 66

Match the Palo Alto Networks WildFire analysis verdict with its definition.

Answer Area

Benign		malicious in intent and can pose a security threat
Grayware		does not pose a direct security threat
Malware		does not exhibit a malicious behavior

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Benign: Safe and does not exhibit malicious behavior

Grayware: No security risk but might display obtrusive behavior (for example, adware, spyware, and browser helper objects)

Malware: Malicious in nature and intent and can pose a security threat (for example, viruses, worms, trojans, root kits, botnets, and remote-access toolkits)

Phishing: Malicious attempt to trick the recipient into revealing sensitive data

NEW QUESTION 67

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

Answer: A

Explanation:

"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."

NEW QUESTION 72

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 73

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 77

Given the graphic, match each stage of the cyber-attack lifecycle to its description.



Unauthorized Access		Unauthorized Use	
reconnaissance		attacker will plan the cyber-attack	
weaponization		attacker will determine which method to use to compromise an endpoint	
delivery		attacker will distribute their weaponized payload to an endpoint	
exploitation		attacker will trigger a weaponized payload	
installation		escalate privileges on a compromised endpoint	
command and control		establish secure communication channel to servers across the internet to reshape attack objectives	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

reconnaissance	reconnaissance	attacker will plan the cyber-attack
weaponization	weaponization	attacker will determine which method to use to compromise an endpoint
delivery	delivery	attacker will distribute their weaponized payload to an endpoint
exploitation	exploitation	attacker will trigger a weaponized payload
installation	installation	escalate privileges on a compromised endpoint
command and control	command and control	establish secure communication channel to servers across the internet to reshape attack objectives

NEW QUESTION 79

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 83

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 85

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 90

Which option is a Prisma Access security service?

- A. Compute Security
- B. Firewall as a Service (FWaaS)
- C. Virtual Private Networks (VPNs)
- D. Software-defined wide-area networks (SD-WANs)

Answer:

B

Explanation:

Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

NEW QUESTION 94

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 98

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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](#)