Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

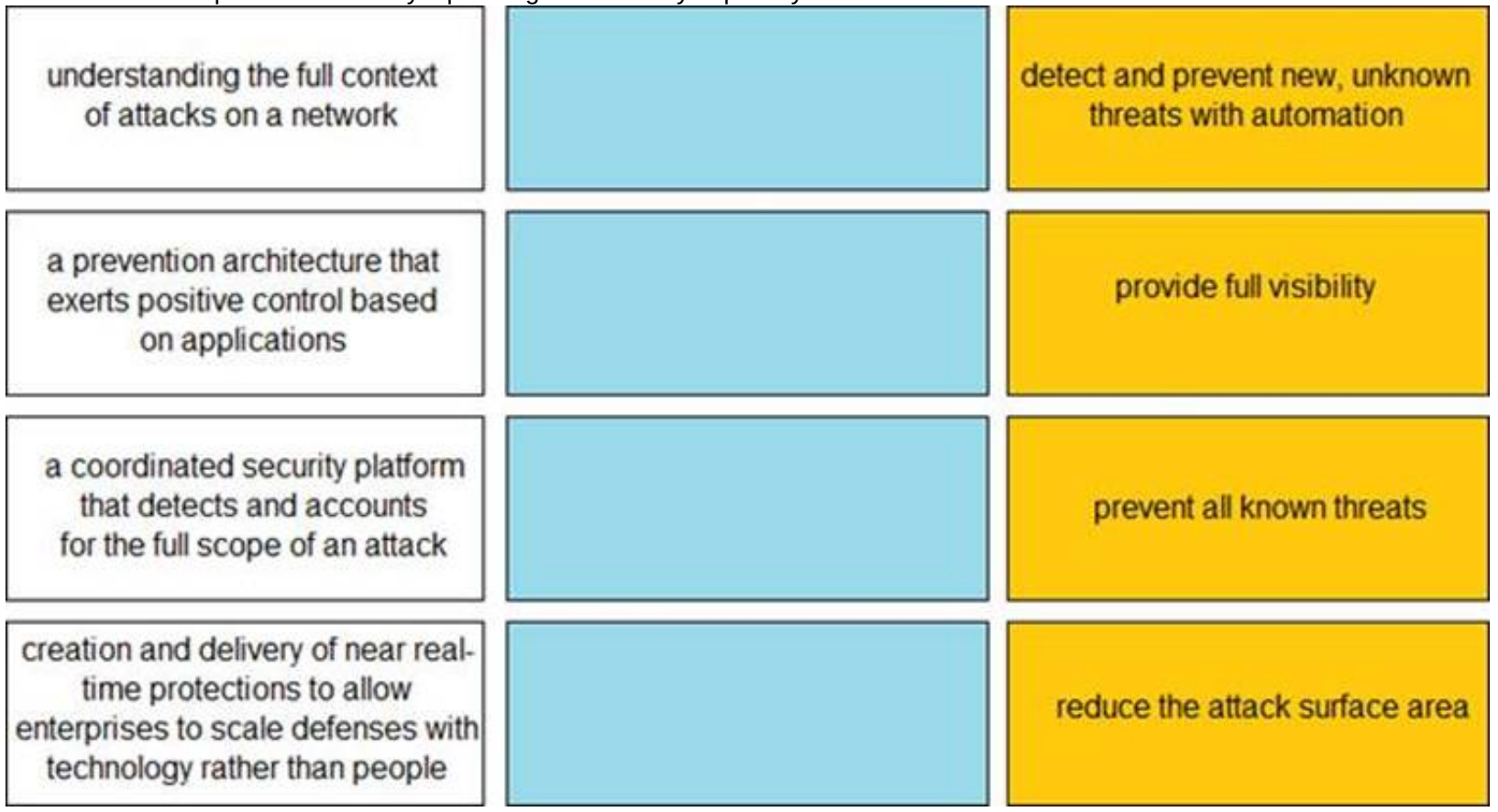
NEW QUESTION 1
Which statement describes DevOps?

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 2
Match each description to a Security Operating Platform key capability.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reduce the attack surface: Best-of-breed technologies that are natively integrated provide a prevention architecture that inherently reduces the attack surface. This type of architecture allows organizations to exert positive control based on applications, users, and content, with support for open communication, orchestration, and visibility.
Prevent all known threats, fast: A coordinated security platform accounts for the full scope of an attack across the various security controls that compose the security posture, thus enabling organizations to quickly identify and block known threats.
Detect and prevent new, unknown threats with automation: Security that simply detects threats and requires a manual response is too little, too late. Automated creation and
delivery of near-real-time protections against new threats to the various security solutions in the organization’s environments enable dynamic policy updates. These updates are
designed to allow enterprises to scale defenses with technology, rather than people.

NEW QUESTION 3
From which resource does Palo Alto Networks AutoFocus correlate and gain URL filtering intelligence?

A. Unit 52
B. PAN-DB
C. BrightCloud
D. MineMeld

Answer: B

Explanation:
When you enable URL Filtering, all web traffic is compared against the URL Filtering database, PAN-DB, which contains millions of URLs that have been grouped into about 65 categories.

NEW QUESTION 4
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 5
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 6
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 7
What is used to orchestrate, coordinate, and control clusters of containers?

A. Kubernetes
B. Prisma Saas
C. Docker
D. CN-Series

Answer: A

Explanation:
As containers grew in popularity and used diversified orchestrators such as Kubernetes (and its derivatives, such as OpenShift), Mesos, and Docker Swarm, it became increasingly important to deploy and operate containers at scale.
https://www.dynatrace.com/news/blog/kubernetes-vs-docker/

NEW QUESTION 8
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 9
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 10
Which network device breaks networks into separate broadcast domains?

A. Hub
B. Layer 2 switch
C. Router
D. Wireless access point

Answer: C

Explanation:
A layer 2 switch will break up collision domains but not broadcast domains. To break up broadcast domains you need a Layer 3 switch with vlan capabilities.

NEW QUESTION 10
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

Answer: C

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

NEW QUESTION 11
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 16
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 19
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 23
Which type of malware takes advantage of a vulnerability on an endpoint or server?

A. technique
B. patch
C. vulnerability
D. exploit

Answer: A

NEW QUESTION 28
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 29
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

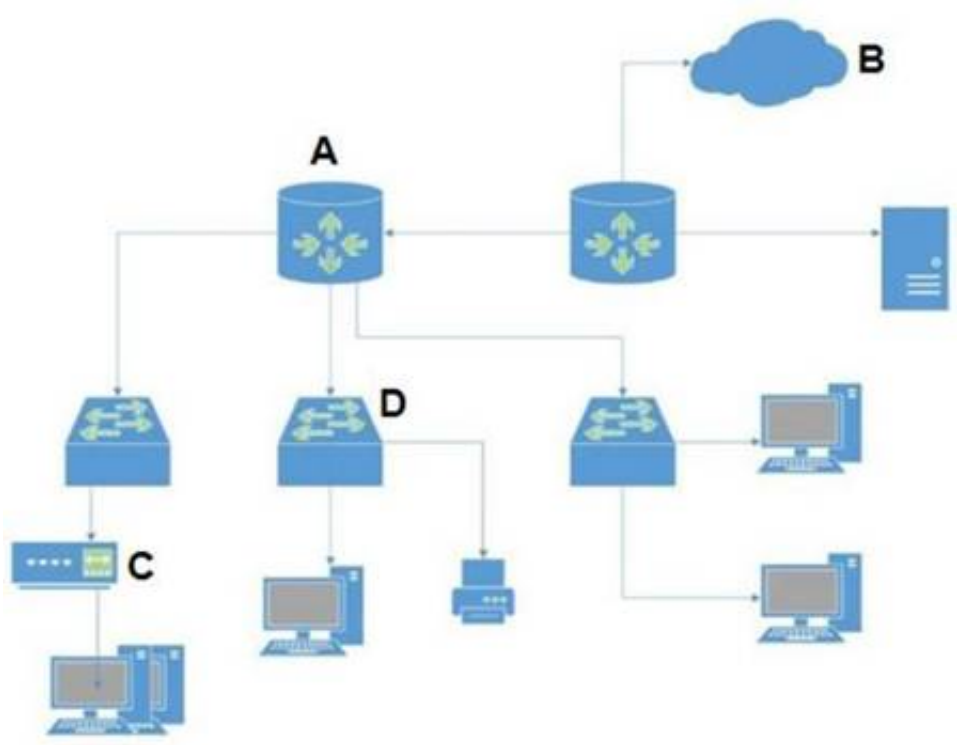
NEW QUESTION 32
Which network firewall operates up to Layer 4 (Transport layer) of the OSI model and maintains information about the communication sessions which have been established between hosts on trusted and untrusted networks?

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 34
In the attached network diagram, which device is the switch?



A. A
B. B
C. C
D. D

Answer: D

NEW QUESTION 38
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 39
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 42
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 44

.....

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