Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

https://www.2passeasy.com/dumps/PCCET/

NEW QUESTION 1
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

NEW QUESTION 2
DRAG DROP
Given the graphic, match each stage of the cyber-attack lifecycle to its description.:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

reconnaissance	reconnaissance	attacker will plan the cyber-attack
installation	exploitation	attacker will determine which method to use to compromise an endpoint
weaponization	weaponization	
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 3
DRAG DROP
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 4
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

Answer: D

NEW QUESTION 5
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: A

NEW QUESTION 6
Which key component is used to configure a static route?

A. router ID
B. enable setting
C. routing protocol
D. next hop IP address

Answer: D

NEW QUESTION 7
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

NEW QUESTION 8
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

NEW QUESTION 9
Which network analysis tool can be used to record packet captures?

A. Smart IP Scanner
B. Wireshark
C. Angry IP Scanner
D. Netman

Answer: B

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 10
DRAG DROP
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:

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

NEW QUESTION 13
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 17
Which TCP/IP sub-protocol operates at the Layer7 of the OSI model?

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

Answer: C

NEW QUESTION 22
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 23
Routing Information Protocol (RIP), uses what metric to determine how network traffic should flow?

A. Shortest Path
B. Hop Count
C. Split Horizon
D. Path Vector

Answer: B

NEW QUESTION 25
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 30
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

NEW QUESTION 33
Which endpoint tool or agent can enact behavior-based protection?

A. AutoFocus
B. Cortex XDR
C. DNS Security
D. MineMeld

Answer: B

NEW QUESTION 35
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

NEW QUESTION 39
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

NEW QUESTION 43
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

NEW QUESTION 48
DRAG DROP
Match each description to a Security Operating Platform key capability.

understanding the full context of attacks on a network		detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications		provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack		prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people		reduce the attack surface area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

understanding the full context of attacks on a network	creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people	detect and prevent new, unknown threats with automation
a prevention architecture that exerts positive control based on applications	understanding the full context of attacks on a network	provide full visibility
a coordinated security platform that detects and accounts for the full scope of an attack	a coordinated security platform that detects and accounts for the full scope of an attack	prevent all known threats
creation and delivery of near real-time protections to allow enterprises to scale defenses with technology rather than people	a prevention architecture that exerts positive control based on applications	reduce the attack surface area

NEW QUESTION 52
Which product from Palo Alto Networks enables organizations to prevent successful cyberattacks as well as simplify and strengthen security processes?

A. Expedition
B. AutoFocus
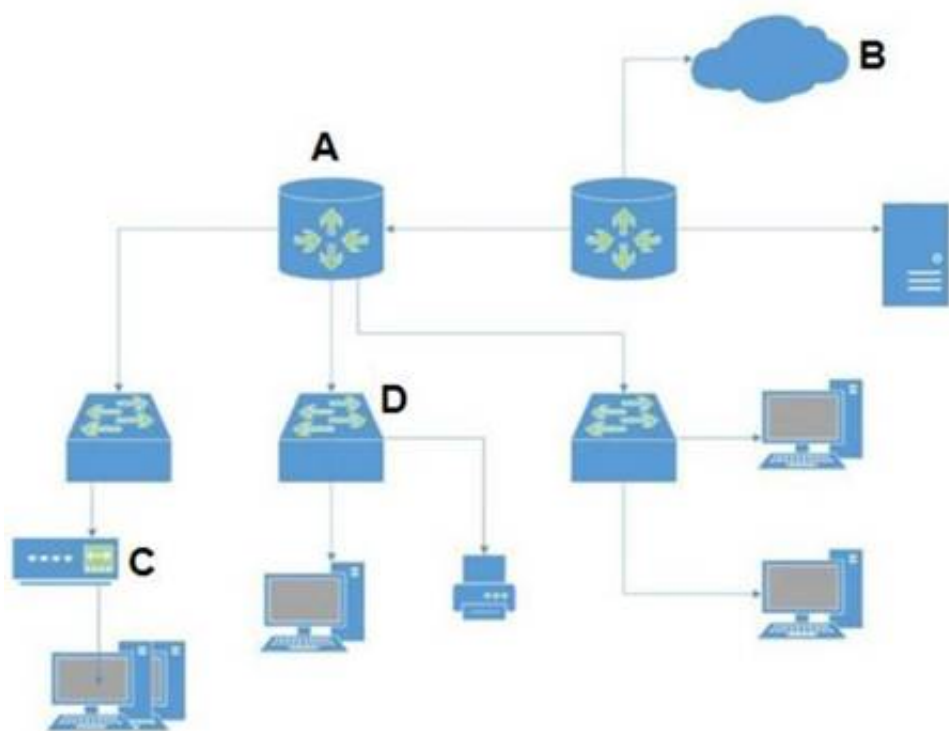C. MineMeld
D. Cortex XDR

Answer: D

NEW QUESTION 57
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

NEW QUESTION 60
In the attached network diagram, which device is the switch?

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

Answer: D

NEW QUESTION 65
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 67
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/CDpipeline

Answer: C

NEW QUESTION 72
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 74
......

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