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
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 3
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 4
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

NEW QUESTION 5
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: A

NEW QUESTION 6
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 7
Which endpoint product from Palo Alto Networks can help with SOC visibility?

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

Answer: B

NEW QUESTION 8
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

NEW QUESTION 9
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

NEW QUESTION 10
DRAG DROP
Match the description with the VPN technology.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10
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 12
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 16

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 17
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 20
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 24
Which option is an example of a North-South traffic flow?

A. Lateral movement within a cloud or data center
B. An internal three-tier application
C. Client-server interactions that cross the edge perimeter
D. Traffic between an internal server and internal user

Answer: C

NEW QUESTION 26
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 30
Which endpoint tool or agent can enact behavior-based protection?

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

Answer: B

NEW QUESTION 34
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 36
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

NEW QUESTION 41
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 43
When signature-based antivirus software detects malware, what three things does it do to provide protection? (Choose three.)

A. decrypt the infected file using base64
B. alert system administrators
C. quarantine the infected file
D. delete the infected file
E. remove the infected file’s extension

Answer: CDE

NEW QUESTION 45
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: B

NEW QUESTION 48
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

NEW QUESTION 53
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 55
In addition to integrating the network and endpoint components, what other component does Cortex integrate to speed up IoC investigations?

A. Computer
B. Switch
C. Infrastructure
D. Cloud

Answer: C

NEW QUESTION 56
In the attached network diagram, which device is the switch?

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

Answer: D

NEW QUESTION 58
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 60
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 64
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 68
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

NEW QUESTION 72
Which two network resources does a directory service database contain? (Choose two.)

A. Services
B. /etc/shadow files
C. Users
D. Terminal shell types on endpoints

Answer: AC

NEW QUESTION 75
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 76
......