PCCET Dumps

Palo Alto Networks Certified Cybersecurity Entry-level Technician

https://www.certleader.com/PCCET-dumps.html
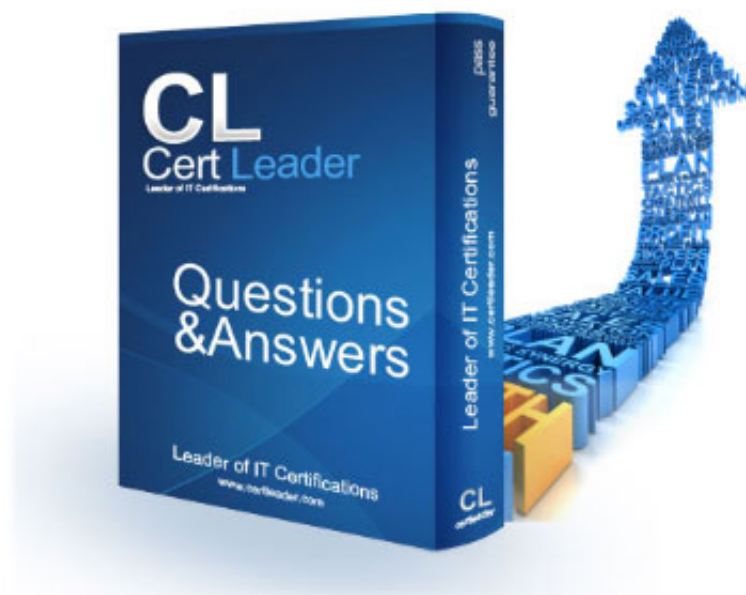
NEW QUESTION 1
Which analysis detonates previously unknown submissions in a custom-built, evasion-resistant virtual environment to determine real-world effects and behavior?

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

Answer: A

NEW QUESTION 2
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 3
DRAG DROP
Given the graphic, match each stage of the cyber-attack lifecycle to its description.:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 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 TCP/IP sub-protocol operates at the Layer7 of the OSI model?

A. UDP
B. MAC
C. SNMP

D. NFS

Answer: C

NEW QUESTION 13
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 17
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 21
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 22
Which endpoint tool or agent can enact behavior-based protection?

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

Answer: B

NEW QUESTION 26
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 28
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 33
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 34
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 38
DRAG DROP
Order the OSI model with Layer7 at the top and Layer1 at the bottom.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 42
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 46
In the attached network diagram, which device is the switch?

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

Answer: D

NEW QUESTION 48
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 49
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 53
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 56
An Administrator wants to maximize the use of a network address. The network is 192.168.6.0/24 and there are three subnets that need to be created that can not overlap. Which subnet would you use for the network with 120 hosts?
Requirements for the three subnets:
Subnet 1: 3 host addresses
Subnet 2: 25 host addresses
Subnet 3: 120 host addresses

A. 192.168.6.168/30
B. 192.168.6.0/25
C. 192.168.6.160/29
D. 192.168.6.128/27

Answer: B

NEW QUESTION 58
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 60
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your PCCET Exam with Our Prep Materials Via below:

https://www.certleader.com/PCCET-dumps.html