Paloalto-Networks

Exam Questions PCCET

Palo Alto Networks Certified Cybersecurity Entry-level Technician

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

    All examinations will be up to date.

* 24/7 Quality Support

    We will provide service round the clock.

* 100% Pass Rate

    Our guarantee that you will pass the exam.

* Unique Gurantee

    If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
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 4
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 5
What is the primary security focus after consolidating data center hypervisor hosts within trust levels?

A. control and protect inter-host traffic using routers configured to use the Border Gateway Protocol (BGP) dynamic routing protocol
B. control and protect inter-host traffic by exporting all your traffic logs to a sysvol log server using the User Datagram Protocol (UDP)
C. control and protect inter-host traffic by using IPv4 addressing
D. control and protect inter-host traffic using physical network security appliances

Answer: D

NEW QUESTION 6
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 7
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 8
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 9
Which option describes the "selective network security virtualization" phase of incrementally
transforming data centers?

A. during the selective network security virtualization phase, all intra-host communication paths are strictly controlled
B. during the selective network security virtualization phase, all intra-host traffic is forwarded to a Web proxy server
C. during the selective network security virtualization phase, all intra-host traffic is encapsulated and encrypted using the IPSEC protocol
D. during the selective network security virtualization phase, all intra-host traffic is load balanced

Answer: A

NEW QUESTION 10
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 10
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 11
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 15
Which endpoint tool or agent can enact behavior-based protection?

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

Answer: B

NEW QUESTION 19
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

NEW QUESTION 23
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 28
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 31
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 35
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 37
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
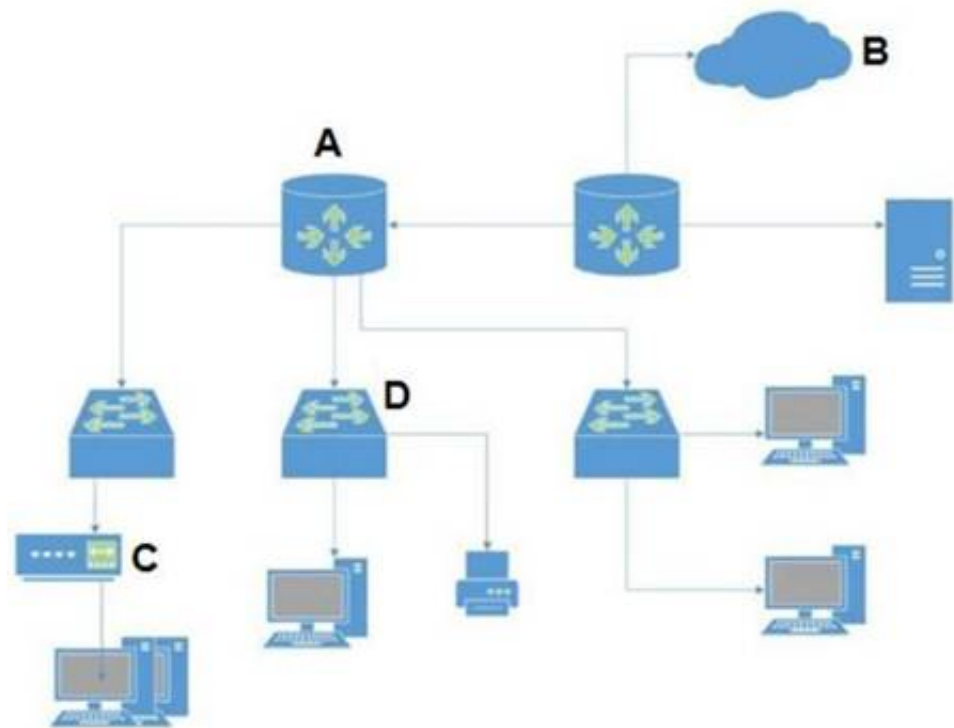
Answer: C

NEW QUESTION 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 47
In the attached network diagram, which device is the switch?

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

Answer: D

NEW QUESTION 51
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 55
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

NEW QUESTION 56
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

NEW QUESTION 59
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 62
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 66
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 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 69
......

Relate Links

100% Pass Your PCCET Exam with Exambible Prep Materials

https://www.exambible.com/PCCET-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/