Free Questions for PSE-Strata by vceexamstest

Shared by Guerra on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following statements is valid with regard to Domain Name System (DNS) sinkholing?

Options:

A- it requires the Vulnerability Protection profile to be enabled

B- DNS sinkholing signatures are packaged and delivered through Vulnerability Protection updates

C- infected hosts connecting to the Sinkhole Internet Protocol (IP) address can be identified in the traffic logs

D- It requires a Sinkhole license in order to activate

Answer:

C

Question 2

Question Type: MultipleChoice

What is the recommended way to ensure that firewalls have the most current set of signatures for up-to-date protection?

Options:

A- Run a Perl script to regularly check for updates and alert when one is released

B- Monitor update announcements and manually push updates to Crewall

C- Store updates on an intermediary server and point all the firewalls to it

D- Use dynamic updates with the most aggressive schedule required by business needs

Answer:

D

Question 3

Question Type: **MultipleChoice**

In Panorama, which three reports or logs will help identify the inclusion of a host source in a command-and-control (C2) incident? (Choose three.)

Options:

A- SaaS reports

B- data filtering logs

C- WildFire analysis reports

D- threat logs

E- botnet reports

Answer:

C, D, E

Question 4

Question Type: **MultipleChoice**

WildFire can discover zero-day malware in which three types of traffic? (Choose three)

Options:

A- SMTP

B- HTTPS

C- FTP

D- DNS

E- TFTP

Answer:

A, B, C

Question 5

Question Type: MultipleChoice

Which statement applies to Palo Alto Networks Single Pass Parallel Processing (SP3)?

Options:

A- It processes each feature in a separate single pass with additional performance impact for each enabled feature.

B- Its processing applies only to security features and does not include any networking features.

C- It processes all traffic in a single pass with no additional performance impact for each enabled feature.

D- It splits the traffic and processes all security features in a single pass and all network features in a separate pass

Answer:

C

Question 6

Question Type: **MultipleChoice**

When HTTP header logging is enabled on a URL Filtering profile, which attribute-value can be logged?

Options:

A- X-Forwarded-For

B- HTTP method

C- HTTP response status code

D- Content type

Answer:

A

Question 7

Question Type: MultipleChoice

Which proprietary technology solutions will allow a customer to identify and control traffic sources regardless of internet protocol (IP) address or network segment?

Options:

A- User ID and Device-ID

B- Source-D and Network.ID

C- Source ID and Device-ID

D- User-ID and Source-ID

Answer:

A

Question 8

Question Type: MultipleChoice

A customer is starting to understand their Zero Trust protect surface using the Palo Alto Networks Zero Trust reference architecture.

What are two steps in this process? (Choose two.)

Options:

A- Validate user identities through authentication

B- Gain visibility of and control over applications and functionality in the traffic flow using a port and protocol firewall

C- Categorize data and applications by levels of sensitivity

D- Prioritize securing the endpoints of privileged users because if non-privileged user endpoints are exploited, the impact will be minimal due to perimeter controls

Answer:

A, C

Question 9

Question Type: MultipleChoice

Which filtering criterion is used to determine users to be included as members of a dynamic user group (DUG)?

Options:

A- Security policy rule

B- Tag

C- Login ID

D- IP address

Answer:

B

Question 10

Question Type: MultipleChoice

A Fortune 500 customer has expressed interest in purchasing WildFire; however, they do not want to send discovered malware outside of their network.

Which version of WildFire will meet this customer's requirements?

Options:

A- WildFire Private Cloud

B- WildFire Government Cloud

C- WildFire Secure Cloud

D- WildFire Public Cloud

Answer:

A

Question 11

Question Type: **MultipleChoice**

WildFire machine learning (ML) for portable executable (PE) files is enabled in the antivirus profile and added to the appropriate firewall rules in the profile. In the Palo Alto Networks WildFire test av file, an attempt to download the test file is allowed through.

Which command returns a valid result to verify the ML is working from the command line.

Options:

A- show wfml cloud-status

B- show mlav cloud-status

C- show ml cloud-status

D- show av cloud-status

Answer:

B

Question 12

Question Type: MultipleChoice

A customer worried about unknown attacks is hesitant to enable SSL decryption due to privacy

and regulatory issues. How does the platform address the customer's concern?

Options:

A- It overcomes reservations about SSL decrypt by offloading to a higher-capacity firewall to help with the decrypt throughput

B- It shows how AutoFocus can provide visibility into targeted attacks at the industry sector

C- It allows a list of websites or URL categories to be defined for exclusion from decryption

D- It bypasses the need to decrypt SSL traffic by analyzing the file while still encrypted

Answer:

C