Free Questions for PSE-Platform by go4braindumps

Shared by Walls on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are two core values of the Palo Alto Network Security Platform? (Choose two)

Options:

A- Sale enablement of all applications

B- Deployment of multiple point-based solutions to provide full security coverage

C- Prevention of cyberattacks

D- Threat remediation

E- Defense against threats with static security solution

Answer:

B, C

Question 2

Question Type: MultipleChoice

A customer is targeted by a true zero-day, targeted attack. However, the customer is protected by the Palo Alto Networks security platform.

The attack leverages a previously unknown vulnerability in IE but utilizes existing hacking techniques on the endpoint. It is transported over standard HTTP traffic and conforms to the HTML standards. It then attempts to download from a website, compromised specifically for this attack, a custom piece of malware to run on the endpoints.

Which element of the platform will stop this attack?

Options:

A- App-ID

B- PAN-DB

C- Traps

D- WildFire

Answer:

D

Question 3

Question Type: **MultipleChoice**

Palo Alto Networks publishes updated Command and Control signatures.

How frequently should the related signatures schedule be set?

Options:

A- Once an hour

B- Once every minute

C- Once a week

D- Once a day

Answer:

D

Question 4

Question Type: **MultipleChoice**

How many recursion levels are supported for compressed files in PAN-OS 8.0?

Options:

A- 2

B- 5

C- 4

D- 3

Answer:

D

Question 5

Question Type: **MultipleChoice**

Which Palo Alto Networks security platform component should an administrator use to extend policies to remote users are not connecting to the internet from behind a firewall?

Options:

A- Threat Intelligence Cloud

B- Traps

C- GlobalProtect

D- Aperture

Answer:

C

Question 6

Question Type: **MultipleChoice**

Which four actions can be configured in an Anti-Spyware profile to address command-and-control traffic from compromised hosts? (Choose four.)

Options:

A- Allow

B- Drop

C- Quarantine

D- Redirect

E- Alert

F- Reset

Answer:

A, B, E, F

Explanation:

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/anti-spyware-profiles.html

Question 7

Question Type: **MultipleChoice**

A customer is seeing an increase in the number of malicious files coming in from undetectable sources in their network. These files include doc and .pdf file types. The customer believes that someone has clicked an email that might have contained a malicious file type. The customer already uses a firewall with User-ID enabled.

Which feature must also be enabled to prevent these attacks?

Options:

A- WildFire

B- App-ID

C- Custom App-ID rules

D- Content Filtering

Answer:

A

Question 8

Question Type: **MultipleChoice**

How does SSL Forward Proxy decryption work?

Options:

A- SSL Forward Proxy decryption policy decrypts and inspects SSL/TLS traffic from internal users to the web.

B- The SSL Forward Proxy Firewall creates a certificate intended for the client that is intercepted and altered by the firewall.

C- If the server's certificate is signed by a CA that the firewall does not trust, the firewall will use the certificate only on Forward Trust.

D- The firewall resides between the internal client and internal server to intercept traffic between the two.

Answer:

A

Question 9

Question Type: **MultipleChoice**

Which three network events are highlighted through correlation objects as a potential security risks? (Choose three.)

Options:

A- Identified vulnerability exploits

B- Suspicious traffic patterns

C- Known command-and-control activity

D- Launch of an identified malware executable file

E- Endpoints access files from a removable drive

Answer:

A, B, C

Question 10

Question Type: MultipleChoice

A customer is worried about unknown attacks, but due to privacy and regulatory issues, won't implement SSL decrypt.

How can the platform still address this customer's concern?

Options:

A- It pivots the conversation to Traps on the endpoint preventing unknown exploits and malware there instead.

B- It bypasses the need to decrypt SSL Traffic by analyzing the file while still encrypted.

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

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

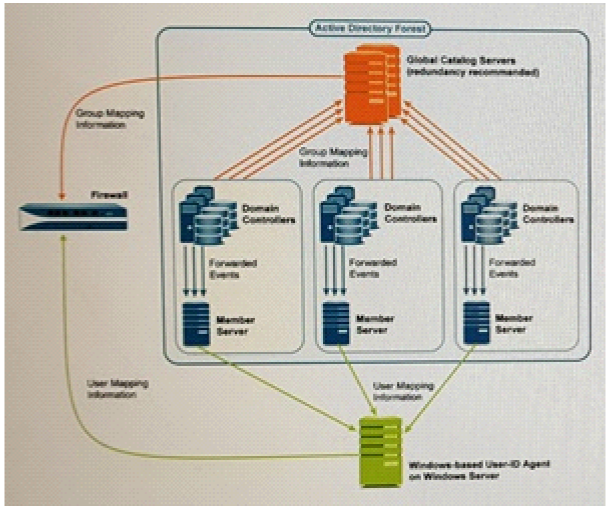
Answer:

A

Question 11

Question Type: **MultipleChoice**

Given the following network diagram, an administrator is considering the use of Windows Log Forwarding and Global Catalog servers for User-ID implementation. What are two potential bandwidth and processing bottlenecks to consider? (Choose two.)



Options:

A- Member Servers

B- Firewall

C- Domain Controllers

D- Windows Server

Answer:

A, C

Question 12

Question Type: **MultipleChoice**

The botnet report displays a confidence score of 1 to 5 indicating the likelihood of a botnet infection.

Which three sources are used by the firewall as the basis of this score? (Choose three.)

Options:

A- Bad Certificate Reports

B- Traffic Type

C- Botnet Reports

D- Number of Events

E- Executable Downloads

F- Threat Landscape

Answer:

B, D, E

Explanation:

https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/monitoring/generate-botnet-reports