PSE-PLATFORM Q&As

PSE-Platform Professional

Pass Palo Alto Networks PSE-PLATFORM Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/pse-platform.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Palo Alto Networks Official Exam Center

QUESTION 1

What are three sources of malware sample data for the Palo Alto Networks Threat Intelligence Cloud? (Choose three.)

A. Third-Party data feeds, like the partnership with ProofPoint and the Cyber Threat Alliance

B. Palo Alto Networks AutoFocus generated Correlation Objects

C. Palo Alto Networks Next Generation Firewalls deployed with Wildfire Analysis Security Profiles

D. WF-500 configured as private clouds for privacy concerns

E. Palo Alto Networks non-firewall products, like Traps and Aperture

Correct Answer: ABE

https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/autofocus

QUESTION 2

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

A. Store updates on an intermediary server and point all the firewalls to it

B. Monitor update announcements and manually push updates to firewalls

C. Utilize dynamic updates with an aggressive update schedule

D. Run a Perl script to regularly check for updates and alert when one in released

Correct Answer: B

QUESTION 3

An SE is preparing an SLR report for a school and wants to emphasize URL filtering capabilities because the school is concerned that its students are accessing inappropriate websites. The URL categories being chosen by default in the report are not highlighting these types of websites.

How should the SE show the customer the firewall can detect that these websites are being accessed?

A. Remove unwanted categories listed under "High Risk" and use relevant information

B. Create a footnote within the SLR generation tool

C. Edit the Key-Findings text to list the other types of categories that may be of interest

D. Produce the report and edit the PDF manually

Correct Answer: A

QUESTION 4

XYZ Corporation has a legacy environment with asymmetric routing. The customer understands that Palo Alto Networks firewalls can support asymmetric routing with redundancy.

Which two features must be enabled to meet the customer\\'s requirements? (Choose two.)

A. Virtual systems

B. HA active/active

C. Policy-based forwarding

D. HA active/passive

Correct Answer: BC

Explanation: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high- availability/routebased-redundancy

QUESTION 5

Which profile or policy should be applied to protect against port scans from the internet?

A. An App-ID security policy rule to block traffic sourcing from the untrust zone

B. Security profiles to security policy rules for traffic sourcing from the untrust zone

C. Interface management profile on the zone of the ingress interface

D. Zone protection profile on the zone of the ingress interface

Correct Answer: D

QUESTION 6

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

A. Allow

B. Drop

C. Quarantine

D. Redirect

E. Alert

F. Reset

Correct Answer: ABEF

Explanation: https://www.paloaltonetworks.com/documentation/71/pan-os/pan- os/policy/anti-spywareprofiles.html

QUESTION 7

What is a best practice when configuring a security policy to completely block a specific application?

A. One the Service/URL. Category tab, set the service to any

B. On the Actions tab, configure a file blocking security profile

C. On the Service/URL. Category tab, set the service to application-default

D. On the Service/URL. Category tab, manually specify a port/service

Correct Answer: A

QUESTION 8

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.)

A. Bad Certificate Reports

B. Traffic Type

C. Botnet Reports

D. Number of Events

E. Executable Downloads

F. Threat Landscape

Correct Answer: BDE

Explanation: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/monitoring/generatebotnet- reports

QUESTION 9

How do Highly Suspicious artifacts in-AutoFocus help identify when an unknown, potential zero-day, targeted attack occur to allow one to adjust the security posture?

A. Highly Suspicious artifacts are associated with High-Risk payloads that are inflicting massive amounts of damage to end customers.

B. All High Risk artifacts are automatically classified as Highly Suspicious.

C. Highly Suspicious artifacts are High Risk artifacts that have been seen in very few samples.

D. Highly Suspicious artifacts have been seen infecting a broad, significant range of companies.

Correct Answer: C

QUESTION 10

DNS sinkholing helps identify infected hosts on the protected network using DNS traffic in situations where the firewall cannot see the infected client\\'s DNS query (that is, the firewall cannot see the originator of DNS query)

Which of the following Statements is true?

A. DNS Sinkholing requires the Vulnerability Protection Profile be enabled.

B. Sinkholing malware DNS queries solves this visibilty problem by forging responses to the client host queries directed at fake domains created in a controlled "Fake Internet" called Zanadu which designed for testing and honeypots.

C. Infected hosts can then be easily identified in the traffic logs because any host that attempts to connect the sinkhole IP address are most likely infected with malware.

D. DNS Sinkholing requires a license SinkHole license in order to activate.

Correct Answer: C