PSE-STRATA$^{Q\&As}$

Palo Alto Networks System Engineer Professional-Strata

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

QUESTION 1

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

A. User ID and Device-ID

B. Source-D and Network.ID

C. Source ID and Device-ID

D. User-ID and Source-ID

Correct Answer: A

QUESTION 2

An endpoint, inside an organization, is infected with known malware that attempts to make a command-and-control connection to a C2 server via the destination IP address

Which mechanism prevents this connection from succeeding?

A. DNS Sinkholing

B. DNS Proxy

C. Anti-Spyware Signatures

D. Wildfire Analysis

Correct Answer: A

QUESTION 3

An administrator wants to justify the expense of a second Panorama appliance for HA of the management layer.

The customer already has multiple M-100s set up as a log collector group. What are two valid reasons for deploying Panorama in High Availability? (Choose two.)

A. Control of post rules

B. Control local firewall rules

C. Ensure management continuity

D. Improve log collection redundancy

Correct Answer: CD

QUESTION 4

Which built-in feature of PAN-OS allows the NGFW administrator to create a policy that provides autoremediation for anomalous user behavior and malicious activity while maintaining user visibility?

A. Dynamic user groups (DUGS)

B. tagging groups

C. remote device User-ID groups

D. dynamic address groups (DAGs)

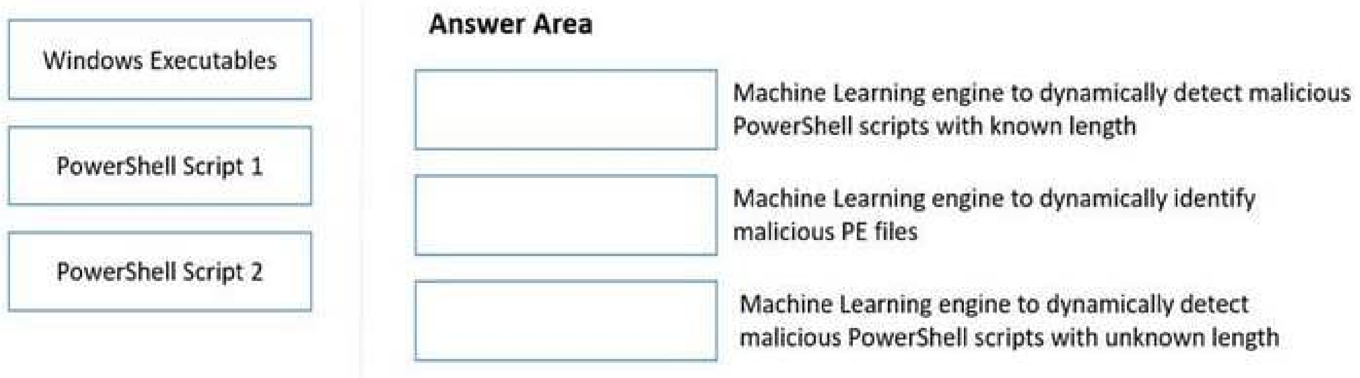
Correct Answer: A

QUESTION 5

DRAG DROP

Match the WildFire Inline Machine Learning Model to the correct description for that model.

Select and Place:



Windows Executables

PowerShell Script 1

PowerShell Script 2

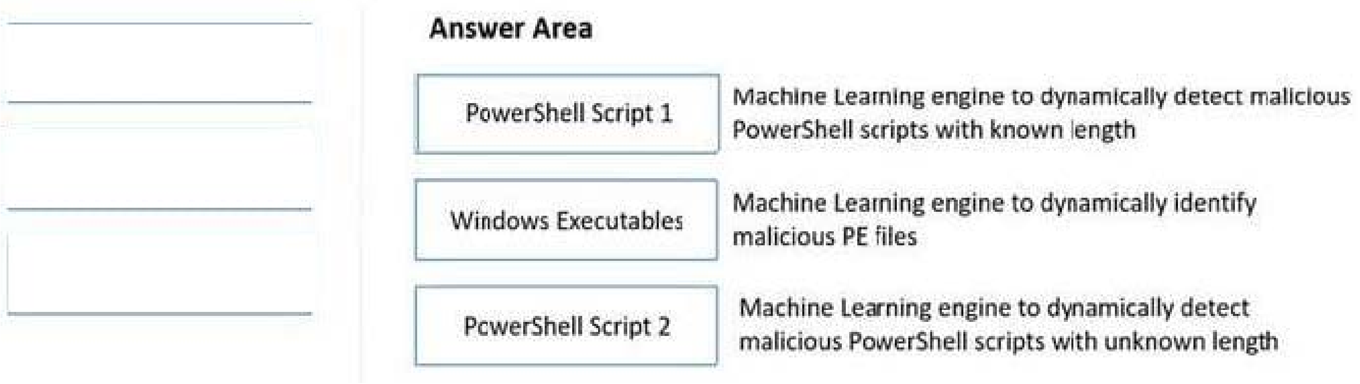
Answer Area

Machine Learning engine to dynamically detect malicious PowerShell scripts with known length

Machine Learning engine to dynamically identify malicious PE files

Machine Learning engine to dynamically detect malicious PowerShell scripts with unknown length

Correct Answer:



Answer Area

PowerShell Script 1	Machine Learning engine to dynamically detect malicious PowerShell scripts with known length
Windows Executables	Machine Learning engine to dynamically identify malicious PE files
PcwerShell Script 2	Machine Learning engine to dynamically detect malicious PowerShell scripts with unknown length

QUESTION 6

What are two presales selling advantages of using Expedition? (Choose two.)

A. map migration gaps to professional services statement of Works (SOWs)

B. streamline and migrate to Layer7 policies using Policy Optimizer

C. reduce effort to implement policies based on App-ID and User-ID

D. easy migration process to move to Palo Alto Networks NGFWs

Correct Answer: AD

QUESTION 7

When having a customer pre-sales call, which aspects of the NGFW should be covered?

A. The NGFW simplifies your operations through analytics and automation while giving you consistent protection through exceptional visibility and control across the data center, perimeter, branch, mobile and cloud networks

B. The Palo Alto Networks-developed URL filtering database, PAN-DB provides high-performance local caching for maximum inline performance on URL lookups, and offers coverage against malicious URLs and IP addresses. As WildFire identifies unknown malware, zero-day exploits, and advanced persistent threats (APTs), the PAN-DB database is updated with information on malicious URLs so that you can block malware downloads and disable Command and Control (C2) communications to protect your network from cyberthreats. URL categories that identify confirmed malicious content --malware, phishing, and C2 are updated every five minutes --to ensure that you can manage access to these sites within minutes of categorization

C. The NGFW creates tunnels that allow users/systems to connect securely over a public network, as if they were connecting over a local area network (LAN). To set up a VPN tunnel you need a pair of devices that can authenticate each other and encrypt the flow of information between them The devices can be a pair of Palo Alto Networks firewalls, or a Palo Alto Networks firewall along with a VPN-capable device from another vendor

D. Palo Alto Networks URL Filtering allows you to monitor and control the sites users can access, to prevent phishing attacks by controlling the sites to which users can submit valid corporate credentials, and to enforce safe search for search engines like Google and Bing

Correct Answer: D

Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/url-filtering

QUESTION 8

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

A. Identified vulnerability exploits

B. Launch of an identified malware executable file

C. Endpoints access files from a removable drive

D. Suspicious host behavior

Correct Answer: AD

QUESTION 9

As you prepare to scan your Amazon S3 account, what enables Prisma service permission to access Amazon S3?

A. access key ID

B. secret access key

C. administrative Password

D. AWS account ID

Correct Answer: A

https://docs.paloaltonetworks.com/prisma/prisma-saas/prisma-saas-admin/secure-cloud-apps/add-cloud-apps-to-prisma-saas/begin-scanning-an-amazon-s3-app.html

QUESTION 10

A packet that is already associated with a current session arrives at the firewall.

What is the flow of the packet after the firewall determines that it is matched with an existing session?

A. it is sent through the fast path because session establishment is not required. If subject to content inspection, it will pass through a single stream-based content inspection engine before egress.

B. It is sent through the slow path for further inspection. If subject to content inspection, it will pass through a single stream-based content inspection engines before egress

C. It is sent through the fast path because session establishment is not required. If subject to content inspection, it will pass through multiple content inspection engines before egress

D. It is sent through the slow path for further inspection. If subject to content inspection, it will pass through multiple content inspection engines before egress

Correct Answer: A

QUESTION 11

Which three signature-based Threat Prevention features of the firewall are informed by intelligence from the Threat Intelligence Cloud? (Choose three.)

A. Vulnerability protection

B. Anti-Spyware

C. Anti-Virus

D. Botnet detection

E. App-ID protection

Correct Answer: ABE

QUESTION 12

A customer has business-critical applications that rely on the general web-browsing application. Which security profile can help prevent drive-by-downloads while still allowing web-browsing traffic?

A. File Blocking Profile

B. DoS Protection Profile

C. URL Filtering Profile

D. Vulnerability Protection Profile

Correct Answer: A

Reference: https://www.google.com/url?sa=tandrct=jandq=andesrc=sandsource=webandcd=andved=2ahUKEwjaw53CvdHyAhUPy4UKHXT5D-MQFnoECAMQAQandurl=https%3A%2F%2Fknowledgebase.paloaltonetworks.com%2Fservlet%2FfileField%3FentityId%3Dka10g000000U0roAAC%26field%3DAttachment_1__Body__sandusg=AOvVaw3DCBM7-FwWInkWYANLrzUt (32)

QUESTION 13

Which two features are key in preventing unknown targeted attacks? (Choose two)

A. nighty botnet report

B. App-ID with the Zero Trust model

C. WildFire Cloud threat analysis

D. Single Pass Parallel Processing (SP3)

Correct Answer: BC

QUESTION 14

Which two products can send logs to the Cortex Data Lake? (Choose two.)

A. AutoFocus

B. PA-3260 firewall

C. Prisma Access

D. Prisma Public Cloud

Correct Answer: BC

https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-cortex-data-lake/forward-logs-to-cortex-data-lake

QUESTION 15

Which Palo Alto Networks security component should an administrator use to and NGFW policies to remote users?

A. Prisma SaaS API

B. Threat intelligence Cloud

C. GlobalProtect

D. Cortex XDR

Correct Answer: C