VCEplus VCEUp

Palo Alto Networks.Premium.PSE-Strata.30q - DEMO

Number: PSE-Strata
Passing Score: 800
Time Limit: 120 min

Exam Code: PSE-Strata
Exam Name: Palo Alto Networks System Engineer - Strata
Website: https://VCEup.com/
Team-Support: https://VCEplus.io/

CEplus
VCEUp

Exam A

QUESTION 1
What are three sources of malware sample data for the Threat Intelligence Cloud? (Choose three)

A. Next-generation firewalls deployed with WildFire Analysis Security Profiles
B. WF-500 configured as private clouds for privacy concerns
C. Correlation Objects generated by AutoFocus
D. Third-party data feeds such as partnership with ProofPomt and the Cyber Threat Alliance
E. Palo Alto Networks non-firewall products such as Traps and Prisma SaaS

Correct Answer: CDE
Section: (none)
Explanation

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

QUESTION 2
What are two core values of the Palo Alto Network Security Operating Platform? (Choose two.}

A. prevention of cyber attacks
B. safe enablement of all applications
C. threat remediation
D. defense against threats with static security solution

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
What are two advantages of the DNS Sinkholing feature? (Choose two.)

A. It forges DNS replies to known malicious domains.
B. It monitors DNS requests passively for malware domains.
C. It can be deployed independently of an Anti-Spyware Profile.
D. It can work upstream from the internal DNS server.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/threat-prevention/dnssinkholing

QUESTION 4
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

www.VCEplus.io

CEplus
VCEUp

Section: (none)
Explanation

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

QUESTION 5
Which two components must be configured within User-ID on a new firewall that has been implemented? (Choose two.)

A. User Mapping
B. Proxy Authentication
C. Group Mapping
D. 802.1X Authentication

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/enable-user-id

QUESTION 6
Which four steps of the cyberattack lifecycle does the Palo Alto Networks Security Operating Platform prevent? (Choose four.)

A. breach the perimeter
B. weaponize vulnerabilities
C. lateral movement
D. exfiltrate data
E. recon the target
F. deliver the malware

www.VCEplus.io

Correct Answer: ACDF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
Which three settings must be configured to enable Credential Phishing Prevention? (Choose three.)

A. define an SSL decryption rulebase
B. enable User-ID
C. validate credential submission detection
D. enable App-ID
E. define URL Filtering Profile

Correct Answer: BCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/preventcredential-phishing.html

QUESTION 8
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. Create a footnote within the SLR generation tool
B. Edit the Key-Findings text to list the other types of categories that may be of interest
C. Remove unwanted categories listed under 'High Risk' and use relevant information
D. Produce the report and edit the PDF manually

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
Which three methods used to map users to IP addresses are supported in Palo Alto Networks firewalls? (Choose three.)

A. eDirectory monitoring
B. Client Probing
C. SNMP server
D. TACACS
E. Active Directory monitoring
F. Lotus Domino
G. RADIUS

Correct Answer: BDG
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/user-idconcepts/user-mapping

QUESTION 10
When the Cortex Data Lake is sized for Traps Management Service, which two factors should be considered? (Choose two.)

A. retention requirements
B. Traps agent forensic data
C. the number of Traps agents
D. agent size and OS

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
What are two benefits of using Panorama for a customer who is deploying virtual firewalls to secure data center traffic? (Choose two.)

A. It can provide the Automated Correlation Engine functionality, which the virtual firewalls do not support.
B. It can monitor the virtual firewalls' physical hosts and Vmotion them as necessary
C. It can automatically create address groups for use with KVM.
D. It can bootstrap the virtual firewalls for dynamic deployment scenarios.

Correct Answer: AD
Section: (none)

www.VCEplus.io

CEplus
VCEUp

Explanation

Explanation/Reference:
Explanation:

QUESTION 12
Which two tabs in Panorama can be used to identify templates to define a common base configuration? (Choose two.)

A. Network Tab
B. Policies Tab
C. Device Tab
D. Objects Tab

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/panorama-webinterface/panorama-templates/template-stacks

QUESTION 13
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
How frequently do WildFire signatures move into the antivirus database?

A. every 24 hours
B. every 12 hours
C. once a week
D. every 1 hour

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfireconcepts/wildfire-signatures

QUESTION 15
What are two presales selling advantages of using Expedition? (Choose two.)

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

www.VCEplus.io

CEplus
VCEUp

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
Which two features are found in a Palo Alto Networks NGFW but are absent in a legacy firewall product? (Choose two.)

A. Traffic is separated by zones
B. Policy match is based on application
C. Identification of application is possible on any port
D. Traffic control is based on IP port, and protocol

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
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

www.VCEplus.io

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
Which CLI allows you to view the names of SD-WAN policy rules that send traffic to the specified virtual SD-WAN interface, along with the performance metrics?

A.
```
>show sdwan rule interface <sdwan.x>
```

B.
```
>show sdwan connection all | <sdwan-interface>
```

C.
```
>show sdwan path-monitor stats vif <sdwan.x>
```

D.
```
=>show sdwan session distribution policy-name <sdwan-policy-name>
```

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/troubleshooting/use-cli-commands-for-sd-wan-tasks.html

QUESTION 19

CEplus
VCEUp

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
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 20
Which three categories are identified as best practices in the Best Practice Assessment tool? (Choose three.)

A. use of decryption policies
B. measure the adoption of URL filters. App-ID. User-ID
C. use of device management access and settings
D. expose the visibility and presence of command-and-control sessions
E. identify sanctioned and unsanctioned SaaS applications

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

www.VCEplus.io

QUESTION 21
In which two cases should the Hardware offering of Panorama be chosen over the Virtual Offering?
(Choose two.)

A. Dedicated Logger Mode is required
B. Logs per second exceed 10,000
C. Appliance needs to be moved into data center
D. Device count is under 100

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
How do you configure the rate of file submissions to WildFire in the NGFW?

A. based on the purchased license uploaded
B. QoS tagging
C. maximum number of files per minute
D. maximum number of files per day

Correct Answer: C
Section: (none)
Explanation

CEplus
VCEUp

Explanation/Reference:
Explanation:
https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/submit-files-for-wildfire-analysis/firewall-file-forwarding-capacity-by-model

QUESTION 23
Palo Alto Networks publishes updated Command-and-Control signatures. How frequently should the related signatures schedule be set?

A. Once a day
B. Once a week
C. Once every minute
D. Once an hour

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
Which are the three mandatory components needed to run Cortex XDR? (Choose three.)

A. Panorama
B. NGFW with PANOS 8 0.5 or later
C. Cortex Data Lake
D. Traps
E. Pathfinder
F. Directory Syn Service

www.VCEplus.io

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/cortex-xdr-prevent-overview/cortex-xdr-prevent-architecture

QUESTION 25
Which selection must be configured on PAN-OS External Dynamic Lists to support MineMeld indicators?

A. Prototype
B. Inputs
C. Class
D. Feed Base URL

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://live.paloaltonetworks.com/t5/minemeld-articles/connecting-pan-os-to-minemeld-using-external-dynamic-lists/ta-p/190414

QUESTION 26
Which two new file types are supported on the WF-500 in PAN-OS 9? (Choose two)

A. ELF
B. 7-Zip
C. Zip

CEplus
VCEUp

D. RAR

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:
Explanation:
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-file-type-support

QUESTION 27
A customer is concerned about zero-day targeted attacks against its intellectual property.
Which solution informs a customer whether an attack is specifically targeted at them?

A. Traps TMS
B. AutoFocus
C. Panorama Correlation Report
D. Firewall Botnet Report

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Prisma SaaS provides which two SaaS threat prevention capabilities? (Choose two)

A. shellcode protection
B. file quarantine
C. SaaS AppID signatures
D. WildFire analysis
E. remote procedural call (RPC) interrogation

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
A client chooses to not block uncategorized websites.
Which two additions should be made to help provide some protection? (Choose two.)

A. A URL filtering profile with the action set to continue for unknown URL categories to security policy rules that allow web access
B. A data filtering profile with a custom data pattern to security policy rules that deny uncategorized websites
C. A file blocking profile attached to security policy rules that allow uncategorized websites to help reduce the risk of drive by downloads
D. A security policy rule using only known URL categories with the action set to allow

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30

www.VCEplus.io

CEplus
VCEUp

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 uses a firewall with User-ID enabled
Which feature must also be enabled to prevent these attacks?

A. Content Filtering
B. WildFire
C. Custom App-ID rules
D. App-ID

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

www.VCEplus.io