Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

NEW QUESTION 1
What method does the Traps agent use to identify malware during a scheduled scan?

A. Heuristic analysis
B. Local analysis
C. Signature comparison
D. WildFire hash comparison and dynamic analysis

Answer: D

NEW QUESTION 2
What is the result of creating an exception from an exploit security event?

A. White lists the process from Wild Fire analysis
B. exempts the user from generating events for 24 hours
C. exempts administrators from generating alerts for 24 hours
D. disables the triggered EPM for the host and process involve

Answer: D

NEW QUESTION 3
Which CLI query would bring back Notable Events from Splunk?
A)

```
!splunk-search query="`notable` | head 3"
```

B)

```
!splunk-search query="'notable' | head 3"
```

C)

```
!splunk-search query="*"
```

D)

```
!splunk-search query="* | head 3"
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

NEW QUESTION 4
Which option describes a Load-Balancing Engine Group?

A. A group of engines that use an algorithm to efficiently share the workload for integrations
B. A group of engines that ensure High Availability of Demisto backend databases.
C. A group of engines that use an algorithm to efficiently share the workload for automation scripts
D. A group of D2 agents that share processing power across multiple endpoints

Answer: C

NEW QUESTION 5
The certificate used for decryption was installed as a trusted toot CA certificate to ensure communication between the Cortex XDR Agent and Cortex XDR Management Console. What action needs to be taken if the administrator determines the Cortex XDR Agents are not communicating with the Cortex XDR Management Console?

A. add paloaltonetworks.com to the SSL Decryption Exclusion list
B. enable SSL decryption
C. disable SSL decryption
D. reinstall the root CA certificate

Answer: D

NEW QUESTION 6
What is the difference between an exception and an exclusion?

A. An exception is based on rules and exclusions are on alerts
B. An exclusion is based on rules and exceptions are based on alerts.
C. An exception does not exist

D. An exclusion does not exist

Answer: A

NEW QUESTION 7
What are two manual actions allowed on War Room entries? (Choose two.)

A. Mark as artifact
B. Mark as scheduled entry
C. Mark as note
D. Mark as evidence

Answer: CD

NEW QUESTION 8
In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three)

A. alert root cause
B. hostname
C. domain/workgroup membership
D. OS
E. presence of Flash executable

Answer: BCD

NEW QUESTION 9
Rearrange the steps into the correct order for modifying an incident layout.

Unordered Options

- Edit the layout
- Select the Edit Layout option
- Navigate to Settings > Advanced > Incident Types
- Select the incident type you want to customize the layout view for
- Navigate to Settings > Layout Builder

Ordered Options

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

| Navigate to Settings > Advanced > Incident Types |
| Select the incident type you want to customize the layout view for |
| Edit the layout |
| Select the Edit Layout option |
| Navigate to Settings > Layout Builder |

NEW QUESTION 10
The certificate used for decryption was installed as a trusted root CA certificate to ensure communication between the Cortex XDR Agent and Cortex XDR Management Console What action needs to be taken if the administrator determines the Cortex XDR Agents are not communicating with the Cortex XDR Management Console?

A. add paloaltonetworks com to the SSL Decryption Exclusion list
B. enable SSL decryption
C. disable SSL decryption
D. reinstall the root CA certificate

Answer: D

NEW QUESTION 10
In Cortex XDR Prevent, which three matching criteria can be used to dynamically group endpoints? (Choose three.)

A. Domain/workgroup membership
B. quarantine status
C. hostname
D. OS
E. attack threat intelligence tag

Answer: BCD

NEW QUESTION 13
An EDR project was initiated by a CISO. Which resource will likely have the most heavy influence on the project?

A. desktop engineer
B. SOC manager
C. SOC analyst IT
D. operations manager

Answer: B

NEW QUESTION 16
How many use cases should a POC success criteria document include?

A. only 1
B. 3 or more
C. no more than 5
D. no more than 2

Answer: A

NEW QUESTION 20
In the DBotScore context field, which context key would differentiate between multiple entries for the same indicator in a multi-TIP environment?

A. Vendor
B. Type
C. Using
D. Brand

Answer: A

NEW QUESTION 21
Which two types of IOCs are available for creation in Cortex XDR? (Choose two.)

A. IP
B. endpoint hostname
C. domain
D. registry entry

Answer: AC

NEW QUESTION 23
An Administrator is alerted to a Suspicious Process Creation security event from multiple users.
The users believe that these events are false positives Which two steps should the administrator take to confirm the false positives and create an exception? (Choose two)

A. With the Malware Security profile, disable the "Prevent Malicious Child Process Execution" module
B. Within the Malware Security profile add the specific parent process, child process, and command line argument to the child process whitelist
C. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments
D. Contact support and ask for a security exception.

Answer: BC

NEW QUESTION 25
Which three Demisto incident type features can be customized under Settings > Advanced > Incident Types? (Choose three.)

A. Define whether a playbook runs automatically when an incident type is encountered
B. Set reminders for an incident SLA
C. Add new fields to an incident type
D. Define the way that incidents of a specific type are displayed in the system
E. Drop new incidents of the same type that contain similar information

Answer: ABD

NEW QUESTION 29
How can you view all the relevant incidents for an indicator?

A. Linked Incidents column in Indicator Screen
B. Linked Indicators column in Incident Screen
C. Related Indicators column in Incident Screen
D. Related Incidents column in Indicator Screen

Answer: D

NEW QUESTION 32
Which deployment type supports installation of an engine on Windows, Mac OS. and Linux?

A. RPM
B. SH
C. DEB
D. ZIP

Answer: D

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/engines/install-deploy-and-confi

NEW QUESTION 37
Which two filter operators are available in Cortex XDR? (Choose two.)

A. not Contains
B. !*
C. =>
D. < >

Answer: AB

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/get-started-with-cortex-xdr-pro/use-c

NEW QUESTION 39
Which Cortex XDR Agent capability prevents loading malicious files from USB-connected removable equipment?

A. Agent Configuration
B. Device Control
C. Device Customization
D. Agent Management

Answer: B

Explanation:
https://live.paloaltonetworks.com/t5/blogs/cortex-xdr-features-introduced-in-december-2019/ba-p/302231

NEW QUESTION 41
The images show two versions of the same automation script and the results they produce when executed in Demisto. What are two possible causes of the exception thrown in the second Image? (Choose two.)
SUCCESS

A. The modified scnpt was run in the wrong Docker image
B. The modified script required a different parameter to run successfully.
C. The dictionary was defined incorrectly in the second script.
D. The modified script attempted to access a dictionary key that did not exist in the dictionary named "data"

Answer: A

NEW QUESTION 44
"Bob" is a Demisto user. Which command is used to add 'Bob" to an investigation from the War Room CLI?

A. #Bob
B. /invite Bob
C. @Bob
D. !invite Bob

Answer: C

NEW QUESTION 46
An antivirus refresh project was initiated by the IT operations executive. Who is the best source for discussion about the project's operational considerations'?

A. endpoint manager
B. SOC manager
C. SOC analyst
D. desktop engineer

Answer: C

NEW QUESTION 51
Which Cortex XDR capability extends investigations to an endpoint?

A. Log Stitching
B. Causality Chain
C. Sensors
D. Live Terminal

Answer: A

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/cortex-xdr-overview/cortex-xdr-conc

NEW QUESTION 56
Cortex XDR can schedule recurring scans of endpoints for malware. Identify two methods for initiating an on-demand malware scan (Choose two)

A. Response > Action Center
B. the local console
C. Telnet
D. Endpoint > Endpoint Management

Answer: AD

NEW QUESTION 61
An administrator of a Cortex XDR protected production environment would like to test its ability to protect users from a known flash player exploit.
What is the safest way to do it?

A. The administrator should attach a copy of the weapomzed flash file to an email, send the email to a selected group of employees, and monitor the Events tab on the Cortex XDR console
B. The administrator should use the Cortex XDR tray icon to confirm his corporate laptop is fully protected then open the weaponized flash file on his machine, and monitor the Events tab on the Cortex XDR console.
C. The administrator should create a non-production Cortex XDR test environment that accurately represents the production environment, introduce the weaponized flash file, and monitor the Events tab on the Cortex XDR console.
D. The administrator should place a copy of the weaponized flash file on several USB drives, scatter them around the office and monitor the Events tab on the Cortex XDR console

Answer: C

NEW QUESTION 64
What is the retention requirement for Cortex Data Lake sizing?

A. number of endpoints
B. number of VM-Series NGFW
C. number of days
D. logs per second

Answer: C

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-corte

NEW QUESTION 65
A customer wants to modify the retention periods of their Threat logs in Cortex Data Lake. Where would the user configure the ratio of storage for each log type?

A. Within the TMS, create an agent settings profile and modify the Disk Quota value
B. It is not possible to configure Cortex Data Lake quota for specific log types.
C. Go to the Cortex Data Lake App in Cloud Services, then choose Configuration and modify the Threat Quota
D. Write a GPO for each endpoint agent to check in less often

Answer: C

NEW QUESTION 67
Which step is required to prepare the VDI Golden Image?

A. Review any PE files that WildFire determined to be malicious
B. Ensure the latest content updates are installed
C. Run the VDI conversion tool
D. Set the memory dumps to manual setting

Answer: A

NEW QUESTION 71
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PSE-Cortex Practice Exam Features:

* PSE-Cortex Questions and Answers Updated Frequently

* PSE-Cortex Practice Questions Verified by Expert Senior Certified Staff

* PSE-Cortex Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PSE-Cortex Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The PSE-Cortex Practice Test Here