

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

<https://www.2passeasy.com/dumps/PSE-Cortex/>



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

A prospect has agreed to do a 30-day POC and asked to integrate with a product that Demisto currently does not have an integration with. How should you respond?

- A. Extend the POC window to allow the solution architects to build it
- B. Tell them we can build it with Professional Services.
- C. Tell them custom integrations are not created as part of the POC
- D. Agree to build the integration as part of the POC

Answer: C

NEW QUESTION 3

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 4

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 5

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 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

Which task allows the playbook to follow different paths based on specific conditions?

- A. Conditional
- B. Automation
- C. Manual
- D. Parallel

Answer: A

NEW QUESTION 8

If a customer activates a TMS tenant and has not purchased a Cortex Data Lake instance. Palo Alto Networks will provide the customer with a free instance. What size is this free Cortex Data Lake instance?

- A. 1 TB
- B. 10 GB
- C. 100 GB
- D. 10 TB

Answer: C

NEW QUESTION 9

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 10

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 10

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 15

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 20

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 25

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 28

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 30

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 34

When a Demisto Engine is part of a Load-Balancing group it?

- A. Must be in a Load-Balancing group with at least another 3 members
- B. It must have port 443 open to allow the Demisto Server to establish a connection
- C. Can be used separately as an engine, only if connected to the Demisto Server directly
- D. Cannot be used separately and does not appear in the in the engines drop-down menu when configuring an integration instance

Answer: D

NEW QUESTION 37

An adversary is attempting to communicate with malware running on your network for the purpose of controlling malware activities or for ex filtrating data from your network. Which Cortex XDR Analytics alert is this activity most likely to trigger'?

- A. Uncommon Local Scheduled Task Creation
- B. Malware
- C. New Administrative Behavior
- D. DNS Tunneling

Answer: B

NEW QUESTION 42

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 environmen
- C. Document indicators of compromise and compare to Traps protection capabilities
- D. Run a known 2015 flash exploit on a Windows XP SP3 V
- 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 47

Given the integration configuration and error in the screenshot what is the cause of the problem?

- A. incorrect instance name
- B. incorrect Username and Password
- C. incorrect appliance port
- D. incorrect server URL

Answer: B

NEW QUESTION 50

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 53

Which process in the causality chain does the Cortex XDR agent identify as triggering an event sequence?

- A. the relevant shell
- B. The causality group owner
- C. the adversary's remote process
- D. the chain's alert initiator

Answer: B

NEW QUESTION 54

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 59

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

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 63

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 67

"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 68

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 70

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 74

If you have a playbook task that errors out. where could you see the output of the task?

- A. /var/log/messages
- B. War Room of the incident
- C. Demisto Audit log
- D. Playbook Editor

Answer: B

NEW QUESTION 76

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PSE-Cortex Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PSE-Cortex Product From:

<https://www.2passeasy.com/dumps/PSE-Cortex/>

Money Back Guarantee

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