# Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

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

**NEW QUESTION 1**
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 2**
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 3**
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 4**
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 5**
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 6**
Given the exception thrown in the accompanying image by the Demisto REST API integration, which action would most likely solve the problem?

Which two playbook functionalities allow looping through a group of tasks during playbook execution? (Choose two.)

A. Generic Polling Automation Playbook
B. Playbook Tasks
C. Sub-Play books
D. Playbook Functions

**Answer:** AC

**NEW QUESTION 7**
How do sub-playbooks affect the Incident Context Data?

A. When set to private, task outputs do not automatically get written to the root context
B. When set to private, task outputs automatically get written to the root context
C. When set to global, allows parallel task execution.
D. When set to global, sub-playbook tasks do not have access to the root context

**Answer:** A

**NEW QUESTION 8**
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 9**
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 10**
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 10**
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 11**
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;

What is the remaining configuration?
A)

B)

C)

D)

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

**Answer:** D

**NEW QUESTION 13**
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 17**
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 22**
Which two items are stitched to the Cortex XDR causality chain'' (Choose two)

A. firewall alert
B. SIEM alert
C. full URL
D. registry set value

**Answer:** AC

**NEW QUESTION 25**
When integrating with Splunk, what will allow you to push alerts into Cortex XSOAR via the REST API?

A. splunk-get-alerts integration command
B. Cortex XSOAR TA App for Splunk
C. SplunkSearch automation
D. SplunkGO integration

**Answer:** B

**NEW QUESTION 26**
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 27**
.....

# 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