



Free Questions for PSE-Cortex by dumpshq

Shared by Mcgee on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

- 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

Question 2

Question Type: MultipleChoice

What is the retention requirement for Cortex Data Lake sizing?

Options:

- 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-cortex-data-lake/set-log-storage-quota>

Question 3

Question Type: MultipleChoice

What is the result of creating an exception from an exploit security event?

Options:

- 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

Question 4

Question Type: MultipleChoice

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

Show Library

UnhandledExceptionExampleScript

```
1 data = {  
2   'a': 1,  
3   'b': 2  
4 }  
5  
6 demisto.log(data['b'])
```

Script



admin

January 13, 2020 10:40 AM

!UnhandledExceptionExampleScript

Command



DBot

January 13, 2020 10:40 AM

Command: !UnhandledExceptionExampleScript (Scripts)

2



Result



DBot

January 13, 2020 10:43 AM

Scripts returned an error

Command: !UnhandledExceptionExampleScript   

Reason

Error from Scripts is : Script failed to run:

Error: {Traceback (most recent call last):

```
File "<string>", line 6, in <module>
```

```
KeyError: 'c'
```

```
] (2604) (2603)
```

Result



Options:

- A- The modified script 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

Question 5

Question Type: MultipleChoice

Which two types of IOCs are available for creation in Cortex XDR? (Choose two.)

Options:

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

Answer:

A, C

Question 6

Question Type: MultipleChoice

In the DBotScore context field, which context key would differentiate between multiple entries for the same indicator in a multi-TIP environment?

Options:

- A- Vendor
- B- Type

C- Using

D- Brand

Answer:

A

Question 7

Question Type: MultipleChoice

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?

Options:

A- The administrator should attach a copy of the weaponized 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

Question 8

Question Type: MultipleChoice

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?

Options:

- A- 1 TB
- B- 10 GB
- C- 100 GB
- D- 10 TB

Answer:

C

Question 9

Question Type: MultipleChoice

What is the difference between an exception and an exclusion?

Options:

- 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

Question 10

Question Type: MultipleChoice

Given the integration configuration and error in the screenshot what is the cause of the problem?

RSA NetWitness Packets and ...



Name *

RSA NetWitness Packets and Logs_instance_2

Server URL (e.g. http(s)://192.168.0.1) *

http://

Appliance Port - Logs(50102) / Packets(50104) /
Concentrator (50105) / Broker (50103) *

50102

Username *

admin

Password *

.....

Validate server certificate

Use system proxy settings

Expiration time

Do not use by default

Use single engine: No engine ▾

Use Load-Balancing Group ?

Options:

A- incorrect instance name

B- incorrect Username and Password

C- incorrect appliance port

D- incorrect server URL

Answer:

B

Question 11

Question Type: MultipleChoice

If you have a playbook task that errors out. where could you see the output of the task?

Options:

- A- /var/log/messages
- B- War Room of the incident
- C- Demisto Audit log
- D- Playbook Editor

Answer:

B

Question 12

Question Type: MultipleChoice

What method does the Traps agent use to identify malware during a scheduled scan?

Options:

- A- Heuristic analysis
- B- Local analysis
- C- Signature comparison

D- WildFire hash comparison and dynamic analysis

Answer:

D

To Get Premium Files for PSE-Cortex Visit

<https://www.p2pexams.com/products/pse-cortex>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/pse-cortex>

