PSE-Cortex Dumps

Palo Alto Networks System Engineer - Cortex Professional

https://www.certleader.com/PSE-Cortex-dumps.html

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
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 3
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 4
The certificate used for decryption was installed as a trusted toot 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
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 6
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 7
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?
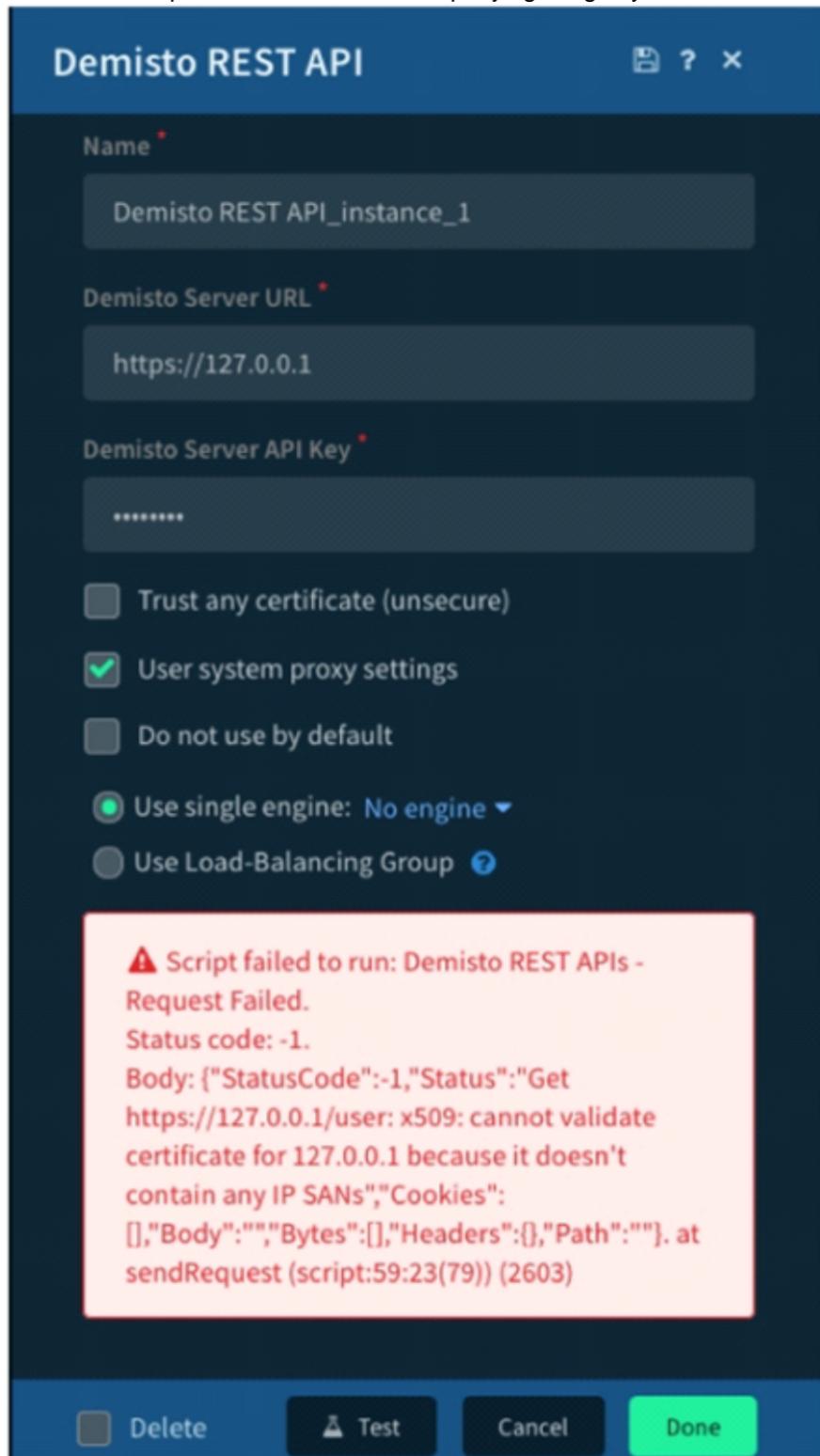
A. add paloaltonetworks com to the SSL Decryption Exclusion list
B. enable SSL decryption

C. disable SSL decryption
D. reinstall the root CA certificate

Answer: D

NEW QUESTION 8
Given the exception thrown in the accompanying image by the Demisto REST API integration, which action would most likely solve the problem?

Which two playbook functionalities allow looping through a group of tasks during playbook execution? (Choose two.)

A. Generic Polling Automation Playbook
B. Playbook Tasks
C. Sub-Play books
D. Playbook Functions

Answer: AC

NEW QUESTION 9
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 10
How many use cases should a POC success criteria document include?

A. only 1
B. 3 or more

C. no more than 5
D. no more than 2

Answer: A

NEW QUESTION 10
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 11
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 13
How does an "inline" auto-extract task affect playbook execution?

A. Doesn't wait until the indicators are enriched and continues executing the next step
B. Doesn't wait until the indicators are enriched but populate context data before executing the next
C. ste
D. Wait until the indicators are enriched but doesn't populate context data before executing the next step.
E. Wait until the indicators are enriched and populate context data before executing the next step.

Answer: D

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 20
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 22
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 27

Which two formats are supported by Whitelist? (Choose two)

A. Regex
B. STIX
C. CSV
D. CIDR

Answer: AD

NEW QUESTION 29
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 30
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 32
During the TMS instance activation, a tenant (Customer) provides the following information for the fields in the Activation - Step 2 of 2 window.

Field	Value
Company Name	XNet Education Systems
Instance Name	xnet50
Subdomain	xnet
Region	EU

During the service instance provisioning which three DNS host names are created? (Choose three.)

A. cc-xnet50.traps.paloaltonetworks.com
B. hc-xnet50.traps.paloaltonetworks.com
C. cc-xnet.traps.paloaltonetworks.com
D. cc.xnet50traps.paloaltonetworks.com
E. xnettraps.paloaltonetworks.com
F. ch-xnet.traps.paloaltonetworks.com

Answer: ACF

NEW QUESTION 36
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 37
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,                          Script
3        'b': 2
4 }
5
6   demisto.log(data['b'])
```

admin
January 13, 2020 10:40 AM   **Command**

!UnhandledExceptionExampleScript

DBot
January 13, 2020 10:40 AM   **Result**

Command: *!UnhandledExceptionExampleScript* (Scripts)
        2

⚠ DBot
January 13, 2020 10:43 AM   **Result**

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)

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 40
"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 42
Which Cortex XDR capability extends investigations to an endpoint?

A. Log Stitching
B. Causality Chain
C. Sensors
D. Live Terminal

Answer: A

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

NEW QUESTION 44
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 45
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 48
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 51
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 54
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your PSE-Cortex Exam with Our Prep Materials Via below:

https://www.certleader.com/PSE-Cortex-dumps.html