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 four types of Traps logs are stored within Cortex Data Lake?

A. Threat, Config, System, Data
B. Threat, Config, System, Analytic
C. Threat, Monito
D. System, Analytic
E. Threat, Config, Authentication, Analytic

Answer: B

NEW QUESTION 3
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 4
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 5
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 6
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

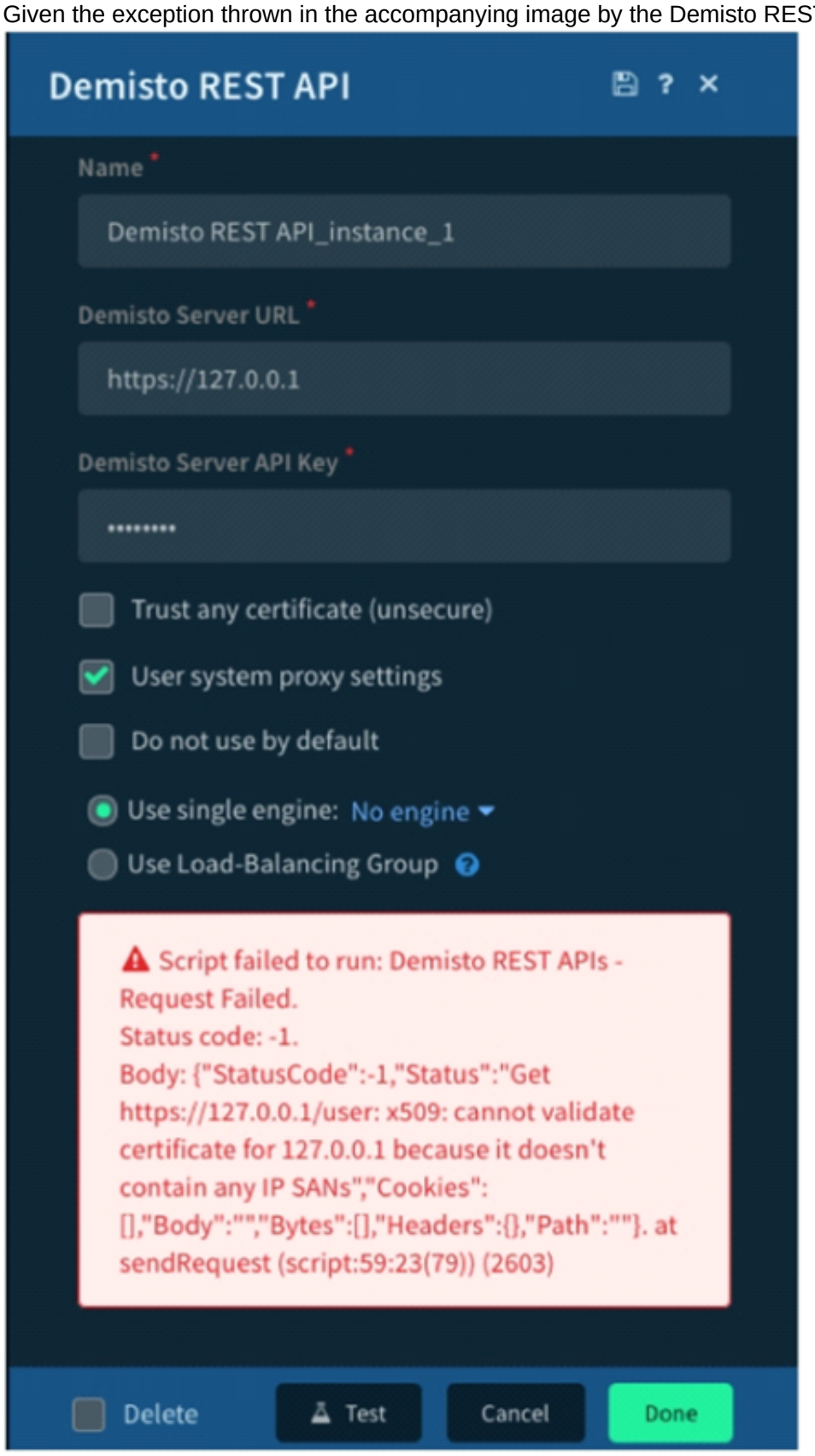
Answer: C

NEW QUESTION 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
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
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 10
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 15
Which deployment type supports installation of an engine on Windows, Mac OS. and Linux?

A. RPM
B. SH
C. DEB
D. ZIP

Answer: D

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar/6-0/cortex-xsoar-admin/engines/install-deploy-and-confi

NEW QUESTION 17
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 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 27
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 31
A General Purpose Dynamic Section can be added to which two layouts for incident types? (Choose two)

A. "Close" Incident Form
B. Incident Summary
C. Incident Quick View
D. "New"/Edit" Incident Form

Answer: BC

NEW QUESTION 32
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

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 two items are stitched to the Cortex XDR causality chain" (Choose two)

A. firewall alert
B. SIEM alert
C. full URL
D. registry set value

Answer: AC

NEW QUESTION 43
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 48

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 49
.....

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