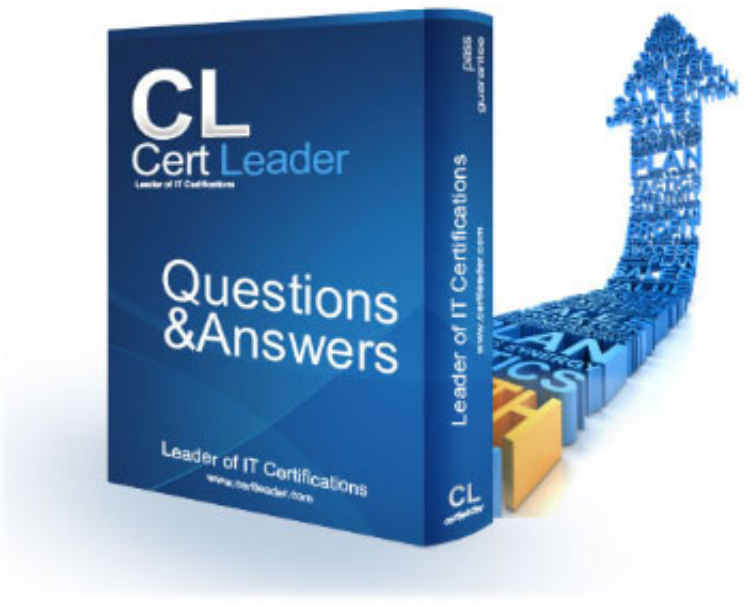
PSE-Cortex Dumps

Palo Alto Networks System Engineer - Cortex Professional

https://www.certleader.com/PSE-Cortex-dumps.html



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
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 5
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 6
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 7
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 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
Rearrange the steps into the correct order for modifying an incident layout.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10
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 12
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 17
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 21
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 22
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 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 26
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 28
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 30
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 35
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 36
Which two log types should be configured for firewall forwarding to the Cortex Data Lake for use by Cortex XDR? (Choose two)

A. Security Event
B. HIP
C. Correlation
D. Analytics

Answer: AB

NEW QUESTION 40
An administrator of a Cortex XDR protected production environment would like to test its ability to protect users from a known flash player exploit.
What is the safest way to do it?

A. The administrator should attach a copy of the weapomzed flash file to an email, send the email to a selected group of employees, and monitor the Events tab on the Cortex XDR console
B. The administrator should use the Cortex XDR tray icon to confirm his corporate laptop is fully protected then open the weaponized flash file on his machine, and monitor the Events tab on the Cortex XDR console.
C. The administrator should create a non-production Cortex XDR test environment that accurately represents the production environment, introduce the weaponized flash file, and monitor the Events tab on the Cortex XDR console.
D. The administrator should place a copy of the weaponized flash file on several USB drives, scatter them around the office and monitor the Events tab on the Cortex XDR console

Answer: C

NEW QUESTION 45
What is the retention requirement for Cortex Data Lake sizing?

A. number of endpoints
B. number of VM-Series NGFW
C. number of days
D. logs per second

Answer: C

Explanation:
https://docs.paloaltonetworks.com/cortex/cortex-data-lake/cortex-data-lake-getting-started/get-started-with-corte

NEW QUESTION 49
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 53
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
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 62
.....

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