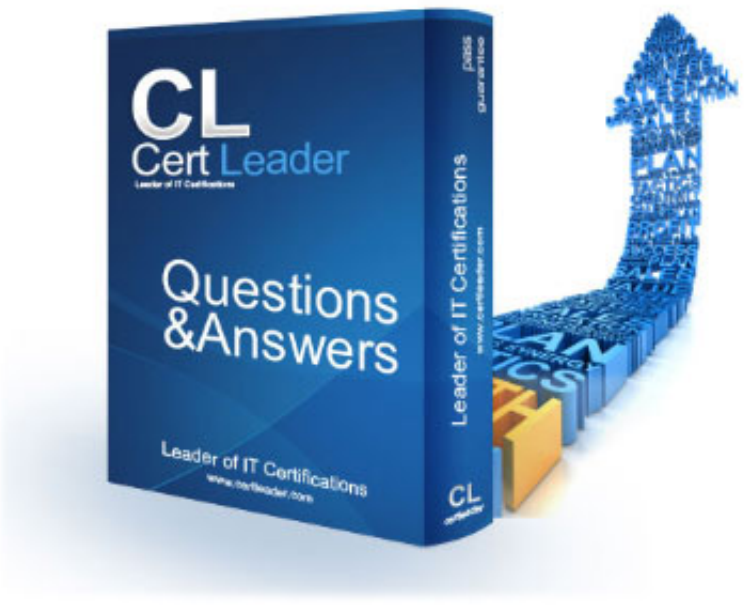
PSE-Cortex Dumps

Palo Alto Networks System Engineer - Cortex Professional

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



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
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
Which option describes a Load-Balancing Engine Group?

A. A group of engines that use an algorithm to efficiently share the workload for integrations
B. A group of engines that ensure High Availability of Demisto backend databases.
C. A group of engines that use an algorithm to efficiently share the workload for automation scripts
D. A group of D2 agents that share processing power across multiple endpoints

Answer: C

NEW QUESTION 4
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 5
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 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
What are two manual actions allowed on War Room entries? (Choose two.)

A. Mark as artifact
B. Mark as scheduled entry
C. Mark as note
D. Mark as evidence

Answer: CD

NEW QUESTION 8
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 9
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 10
How many use cases should a POC success criteria document include?

A. only 1
B. 3 or more
C. no more than 5
D. no more than 2

Answer: A

NEW QUESTION 10
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 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 15
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 20
How can you view all the relevant incidents for an indicator?

A. Linked Incidents column in Indicator Screen
B. Linked Indicators column in Incident Screen
C. Related Indicators column in Incident Screen
D. Related Incidents column in Indicator Screen

Answer: D

NEW QUESTION 22
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 23
An adversary is attempting to communicate with malware running on your network for the purpose of controlling malware activities or for ex filtrating data from your network. Which Cortex XDR Analytics alert is this activity most likely to trigger'?

A. Uncommon Local Scheduled Task Creation
B. Malware
C. New Administrative Behavior
D. DNS Tunneling

Answer: B

NEW QUESTION 27
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 31
Which two formats are supported by Whitelist? (Choose two)

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

Answer: AD

NEW QUESTION 34
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 38
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 40
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 43
The images show two versions of the same automation script and the results they produce when executed in Demisto. What are two possible causes of the exception thrown in the second Image? (Choose two.)
SUCCESS

A. The modified scnpt was run in the wrong Docker image
B. The modified script required a different parameter to run successfully.
C. The dictionary was defined incorrectly in the second script.
D. The modified script attempted to access a dictionary key that did not exist in the dictionary named "data”

Answer: A

NEW QUESTION 47
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 49
Which Cortex XDR capability extends investigations to an endpoint?

A. Log Stitching
B. Causality Chain
C. Sensors
D. Live Terminal

Answer: A

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

NEW QUESTION 51
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 56
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 57
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 59
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 60
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 65
.....

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