PaloAltoNetworks.PCDRA.v2023-11-07.q21

Exam Code:	PCDRA
Exam Name:	Palo Alto Networks Certified Detection and Remediation Analyst
Certification Provider:	Palo Alto Networks
Free Question Number:	21
Version:	v2023-11-07
# of views:	648
# of Questions views:	210
https://www.freeqas.com/qa/Palo-Alto-Networks/PCDRA/PaloAltoNetworks.PCDRA.v2023-11-07.q21.html	

NEW QUESTION: 1
What is the purpose of targeting software vendors in a supply-chain attack?
A. to access source code.
B. to take advantage of a trusted software delivery method.
C. to steal users' login credentials.
D. to report Zero-day vulnerabilities.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 2
With a Cortex XDR Prevent license, which objects are considered to be sensors?
A. Syslog servers
B. Palo Alto Networks Next-Generation Firewalls
C. Cortex XDR agents
D. Third-Party security devices
Answer: (SHOW ANSWER)

NEW QUESTION: 3
In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the singer?
A. In the Restrictions Profile, add the file name and path to the Executable Files allow list.
B. Add the signer to the allow list under the action center page.
C. Add the signer to the allow list in the malware profile.
D. Create a new rule exception and use the singer as the characteristic.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
Which of the following is NOT a precanned script provided by Palo Alto Networks?
A. list_directories
B. process_kill_name
C. quarantine_file
D. delete_file
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?
A. Log Stitching Engine
B. Causality Analysis Engine
C. Causality Chain Engine
D. Sensor Engine
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Which type of BIOC rule is currently available in Cortex XDR?
A. Network
B. Discovery
C. Dropper
D. Threat Actor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 7
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)
A. Automatically close the connections involved in malicious traffic.
B. Automatically kill the processes involved in malicious activity.
C. Automatically terminate the threads involved in malicious activity.
D. Automatically block the IP addresses involved in malicious traffic.
Answer: A,D (LEAVE A REPLY)
Reference:
%20threat%20protection%2C%20the,appear%20legitimate%20if%20inspected%20individually

NEW QUESTION: 8
Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

A. Hash Verdict Determination
B. Behavioral Threat Protection
C. Restriction Policy
D. Child Process Protection
Answer: B (LEAVE A REPLY)
Cortex XDR agent offers a complete prevention stack with cutting-edge protection for exploits, malware, ransomware, and fileless attacks. It includes the broadest set of exploit protection modules available to block the exploits that lead to malware infections. Every file is examined by an adaptiveAI-driven local analysis engine that's always learning to counter new attack techniques. A BehavioralThreat Protection engine examines the behavior of multiple, related processes to uncover attacks as they occur. Integration with the Palo Alto Networks WildFire® malware prevention service boosts security accuracy and coverage.

NEW QUESTION: 9
Phishing belongs which of the following MITRE ATT&CK tactics?
A. Persistence, Command and Control
B. Reconnaissance, Initial Access
C. Initial Access, Persistence
D. Reconnaissance, Persistence
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?
A. create an exception to prevent future false positives
B. mark the incident as Resolved - False Positive
C. create a BIOC rule excluding this behavior
D. mark the incident as Unresolved
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
Which module provides the best visibility to view vulnerabilities?
A. Live Terminal module
B. Forensics module
C. Host Insights module
D. Device Control Violations module
Answer: C (LEAVE A REPLY)

NEW QUESTION: 12
Which of the following policy exceptions applies to the following description?

'An exception allowing specific PHP files'
A. Support exception
B. Local file threat examination exception
C. Process exception
D. Behavioral threat protection rule exception
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
Which statement regarding scripts in Cortex XDR is true?
A. The level of risk is assigned to the script upon import.
B. Any version of Python script can be run.
C. Any script can be imported including Visual Basic (VB) scripts.
D. The script is run on the machine uploading the script to ensure that it is operational.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?
A. Agent Installer and Content Caching
B. Syslog Collector
C. CSV Collector
D. Agent Proxy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
When is the wss (WebSocket Secure) protocol used?
A. when the Cortex XDR agent establishes a bidirectional communication channel
B. when the Cortex XDR agent uploads alert data
C. when the Cortex XDR agent downloads new security content
D. when the Cortex XDR agent connects to WildFire to upload files for analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 16
As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?
A. Enable DLL Protection on all servers but there might be some false positives.
B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
C. Create IOCs of the malicious files you have found to prevent their execution.

D. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.
Answer: (SHOW ANSWER)

NEW QUESTION: 17
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?
A. WebSocket
B. UDP and a random port
C. TCP, over port 80
D. NetBIOS over TCP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Which Type of IOC can you define in Cortex XDR?
A. full path
B. App-ID
C. destination port
D. e-mail address
Answer: A (LEAVE A REPLY)

NEW QUESTION: 19
After scan, how does file quarantine function work on an endpoint?
A. Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.
B. Quarantine takes ownership of the files and folders and prevents execution through access control.
C. Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.
D. Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 20
In incident-related widgets, how would you filter the display to only show incidents that were "starred"?
A. Create a custom XQL widget
B. This is not currently supported
C. Create a custom report and filter on starred incidents
D. Click the star in the widget
Answer: D (LEAVE A REPLY)
Reference:
%20you%20clear%20the%20star

NEW QUESTION: 21
What is by far the most common tactic used by ransomware to shut down a victim's operation?
A. restricting access to administrative accounts to the victim
B. encrypting certain files to prevent access by the victim
C. preventing the victim from being able to access APIs to cripple infrastructure
D. denying traffic out of the victims network until payment is received
Answer: B (LEAVE A REPLY)