Palo Alto Networks

PCDRA Exam

Palo Alto Networks Certified Detection and Remediation Analyst

Questions & Answers

(Demo Version - Limited Content)

Thank you for Downloading PCDRA exam PDF Demo

Get Full File:

https://dumpstoday.com/pcdra-dumps/

QUESTION 1

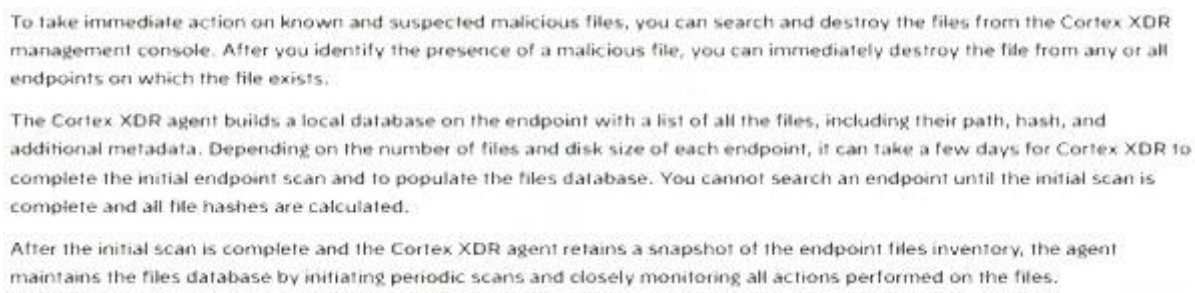
When using the “File Search and Destroy” feature, which of the following search hash type is supported?

A. SHA256 hash of the file
B. AES256 hash of the file
C. MD5 hash of the file
D. SHA1 hash of the file

Correct Answer: A

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-pro-admin/investigation-andresponse/response-actions/search-file-and-destroy.html



To take immediate action on known and suspected malicious files, you can search and destroy the files from the Cortex XDR management console. After you identify the presence of a malicious file, you can immediately destroy the file from any or all endpoints on which the file exists.

The Cortex XDR agent builds a local database on the endpoint with a list of all the files, including their path, hash, and additional metadata. Depending on the number of files and disk size of each endpoint, it can take a few days for Cortex XDR to complete the initial endpoint scan and to populate the files database. You cannot search an endpoint until the initial scan is complete and all file hashes are calculated.

After the initial scan is complete and the Cortex XDR agent retains a snapshot of the endpoint files inventory, the agent maintains the files database by initiating periodic scans and closely monitoring all actions performed on the files.

QUESTION 2

What is the function of WildFire for Cortex XDR?

A. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.
B. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.
C. WildFire accepts and analyses a sample to provide a verdict
D. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Correct Answer: C

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/investigation-andresponse/investigate-files/review-wildfire-analysis-details.html

For each file, Cortex XDR receives a file verdict and the WildFire Analysis Report. This report contains the detailed sample information and behavior analysis in different sandbox environments, leading to the WildFire verdict. You can use the report to assess whether the file poses a real threat on an endpoint. The details in the WildFire analysis report for each event vary depending on the file type and the behavior of the file.

QUESTION 3

What kind of the threat typically encrypts user files?

A. ransomware
B. SQL injection attacks
C. Zero-day exploits
D. supply-chain attacks

Correct Answer: A

Explanation/Reference:

Reference: https://www.proofpoint.com/us/threat-reference/ransomware#:~:text=Ransomware is a type of,ransom fee to the attacker

Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever or the ransom increases.

Ransomware attacks are all too common these days. Major companies in North America and Europe alike have fallen victim to it. Cybercriminals will attack any consumer or any business and victims come from all industries.

Several government agencies, including the FBI, advise against paying the ransom to keep from encouraging the ransomware cycle, as does the No More Ransom Project. Furthermore, half of the victims who pay the ransom are likely to suffer from repeat ransomware attacks, especially if it is not cleaned from the system.

QUESTION 4

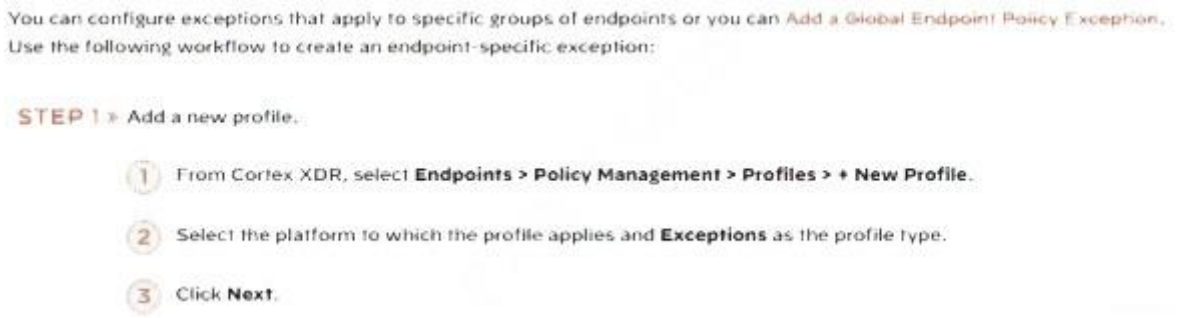
Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

A. Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list
B. From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.
C. Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.
D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.

Correct Answer: B

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/ exceptions-security-profiles/add-exceptions-profile.html


You can configure exceptions that apply to specific groups of endpoints or you can Add a Global Endpoint Policy Exception.
Use the following workflow to create an endpoint-specific exception:

STEP 1 » Add a new profile.

1. From Cortex XDR, select **Endpoints > Policy Management > Profiles > + New Profile**.
2. Select the platform to which the profile applies and **Exceptions** as the profile type.
3. Click **Next**.

QUESTION 5

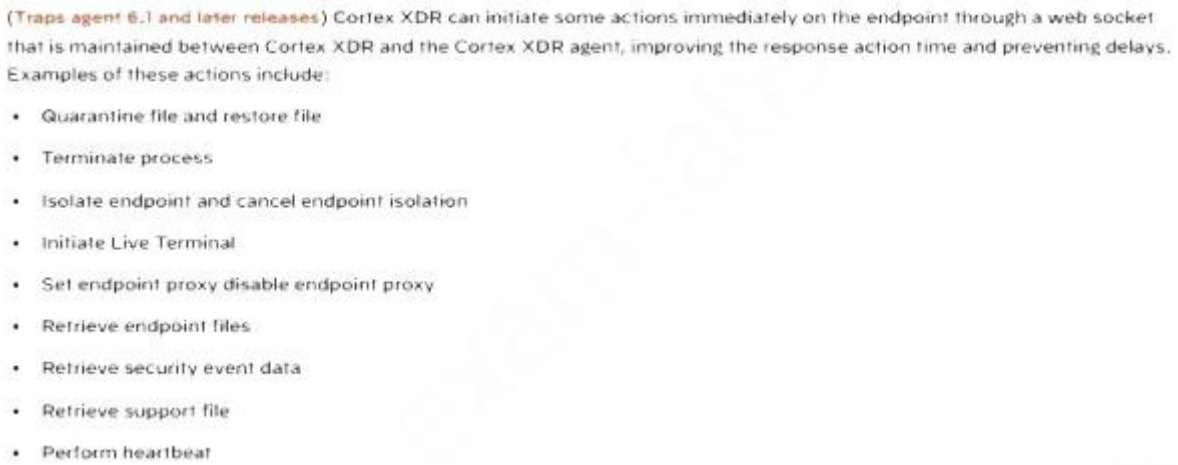
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

A. NetBIOS over TCP
B. WebSocket
C. UDP and a random port
D. TCP, over port 80

Correct Answer: B

Explanation/Reference:

Reference: https://docs.paloaltonetworks.com/cortex/cortex-xdr/cortex-xdr-prevent-admin/endpoint-security/ communication-between-cortex-xdr-and-agents.html


(Traps agent 6.1 and later releases) Cortex XDR can initiate some actions immediately on the endpoint through a web socket that is maintained between Cortex XDR and the Cortex XDR agent, improving the response action time and preventing delays. Examples of these actions include:

- Quarantine file and restore file
- Terminate process
- Isolate endpoint and cancel endpoint isolation
- Initiate Live Terminal
- Set endpoint proxy disable endpoint proxy
- Retrieve endpoint files
- Retrieve security event data
- Retrieve support file
- Perform heartbeat

Thank You for trying PCDRA PDF Demo

https://dumpstoday.com/pcdra-dumps/

Start Your PCDRA Preparation

[Limited Time Offer] Use Coupon "SAVE20" for extra 20% discount the purchase of PDF file. Test your PCDRA preparation with actual exam questions