



Palo Alto Networks XDR-Analyst Practice Questions

Shared by Wolfe on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

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?

Options:

- A- Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- B- Enable DLL Protection on all servers but there might be some false positives.
- 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:

A

Explanation:

To ensure that the same protection is extended to all your servers, you need to create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can use various operators, functions, and variables to define the criteria and the actions for the rules. By creating BTP rules that match the behaviors of the supply chain attack, you can prevent the attack from compromising your servers¹².

Let's briefly discuss the other options to provide a comprehensive explanation:

B . Enable DLL Protection on all servers but there might be some false positives: This is not the correct answer. Enabling DLL Protection on all servers will not ensure that the same protection is extended to all your servers. DLL Protection is a feature of Cortex XDR that allows you to block the execution of unsigned or untrusted DLL files on your endpoints. DLL Protection can help to prevent some types of attacks that use malicious DLL files, but it may not be effective against the supply chain attack that used a Trojanized DLL file that was digitally signed by a trusted vendor. DLL Protection may also cause some false positives, as it may block some legitimate DLL files that are unsigned or untrusted³.

C . Create IOCs of the malicious files you have found to prevent their execution: This is not the correct answer. Creating IOCs of the malicious files you have found will not ensure that the same protection is extended to all your servers. IOCs are indicators of compromise that you can

create to detect and respond to known threats on your endpoints, such as file hashes, registry keys, IP addresses, domain names, or full paths. IOCs can help to identify and block the malicious files that you have already discovered, but they may not be effective against the supply chain attack that used different variants of the malicious files with different hashes or names. IOCs may also become outdated, as the attackers may change or update their files to evade detection⁴.

D . Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading: This is not the correct answer. Enabling BTP with cytool will not ensure that the same protection is extended to all your servers. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can help to prevent the attack from spreading, but they need to be created and configured in the Cortex XDR app, not with cytool. Cytool is a command-line tool that allows you to perform various operations on the Cortex XDR agent, such as installing, uninstalling, upgrading, or troubleshooting. Cytool does not have an option to enable or configure BTP rules.

In conclusion, to ensure that the same protection is extended to all your servers, you need to create BTP rules to recognize and prevent the activity. By using BTP rules, you can create custom and flexible prevention rules that match the behaviors of the supply chain attack.

Behavioral Threat Protection

Create a BTP Rule

DLL Protection

Create an IOC Rule

[Cytool]

Question 2

Question Type: MultipleChoice

To stop a network-based attack, any interference with a portion of the attack pattern is enough to prevent it from succeeding. Which statement is correct regarding the Cortex XDR Analytics module?

Options:

- A- It does not interfere with any portion of the pattern on the endpoint.
- B- It interferes with the pattern as soon as it is observed by the firewall.
- C- It does not need to interfere with the any portion of the pattern to prevent the attack.
- D- It interferes with the pattern as soon as it is observed on the endpoint.

Answer:

D

Explanation:

The correct statement regarding the Cortex XDR Analytics module is D, it interferes with the pattern as soon as it is observed on the endpoint. The Cortex XDR Analytics module is a feature of Cortex XDR that uses machine learning and behavioral analytics to detect and prevent network-based attacks on endpoints. The Cortex XDR Analytics module analyzes the network traffic and activity on the endpoint, and compares it with the attack patterns defined by Palo Alto Networks threat research team. The Cortex XDR Analytics module interferes with the attack pattern as soon as it is observed on the endpoint, by blocking the malicious network connection, process, or file. This way, the Cortex XDR Analytics module can stop the attack before it causes any damage or compromise.

The other statements are incorrect for the following reasons:

A is incorrect because the Cortex XDR Analytics module does interfere with the attack pattern on the endpoint, by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on the firewall or any other network device to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.

B is incorrect because the Cortex XDR Analytics module does not interfere with the attack pattern as soon as it is observed by the firewall. The Cortex XDR Analytics module does not depend on the firewall or any other network device to detect or prevent the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the analysis and interference. The firewall may not be able to observe or block the attack pattern if it is encrypted, obfuscated, or bypassed by the attacker.

C is incorrect because the Cortex XDR Analytics module does need to interfere with the attack pattern to prevent the attack. The Cortex XDR Analytics module does not only detect the attack pattern, but also prevents it from succeeding by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on any other response mechanism or human intervention to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.

Cortex XDR Analytics Module

Cortex XDR Analytics Module Detection and Prevention

Question 3

Question Type: MultipleChoice

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

Options:

- A- Assign incidents to an analyst in bulk.
- B- Change the status of multiple incidents.
- C- Investigate several Incidents at once.
- D- Delete the selected Incidents.

Answer:

A, B

Explanation:

When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, right-click on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents¹²

Assign Incidents to an Analyst in Bulk

Change the Status of Multiple Incidents

Question 4

Question Type: MultipleChoice

How does Cortex XDR agent for Windows prevent ransomware attacks from compromising the file system?

Options:

- A- by encrypting the disk first.
- B- by utilizing decoy Files.
- C- by retrieving the encryption key.
- D- by patching vulnerable applications.

Answer:

B

Explanation:

Cortex XDR agent for Windows prevents ransomware attacks from compromising the file system by utilizing decoy files. Decoy files are randomly generated files that are placed in strategic locations on the endpoint, such as the user's desktop, documents, and pictures folders. These files are designed to look like valuable data that ransomware would target for encryption. When Cortex XDR agent detects that a process is attempting to access or modify a decoy file, it immediately blocks the process and alerts the administrator. This way, Cortex XDR agent can stop ransomware attacks before they can cause any damage to the real files on the endpoint. Reference:

Anti-Ransomware Protection

PCDRA Study Guide

Question 5

Question Type: MultipleChoice

Which profiles can the user use to configure malware protection in the Cortex XDR console?

Options:

- A- Malware Protection profile
- B- Malware profile
- C- Malware Detection profile
- D- Anti-Malware profile

Answer:

A

Explanation:

The user can use the Malware Protection profile to configure malware protection in the Cortex XDR console. The Malware Protection profile defines the actions that Cortex XDR takes when it detects malware on your endpoints. You can configure different actions for different types of malware, such as ransomware, password theft, or child process. You can also configure the scan frequency and scope for periodic malware scans. The Malware Protection profile is part of the Endpoint Security policy that you assign to your endpoints. Reference:

Malware Protection Profile

Endpoint Security Policy



Question 6

Question Type: MultipleChoice

What types of actions you can execute with live terminal session?

Options:

- A- Manage Network configurations, Quarantine Files, Run PowerShell scripts
- B- Manage Processes, Manage Files, Run Operating System Commands, Run Ruby Commands and Scripts
- C- Apply patches, Reboot System, send notification for end user, Run Python Commands and Scripts
- D- Manage Processes, Manage Files, Run Operating System Commands, Run Python Commands and Scripts



Answer:

D

Explanation:

Live terminal session is a feature of Cortex XDR that allows you to remotely access and control endpoints from the Cortex XDR console. With live terminal session, you can execute various actions on the endpoints, such as:

Manage Processes: You can view, start, or kill processes on the endpoint, and monitor their CPU and memory usage.

Manage Files: You can view, create, delete, or move files and folders on the endpoint, and upload or download files to or from the endpoint.

Run Operating System Commands: You can run commands on the endpoint using the native command-line interface of the operating system, such as cmd.exe for Windows, bash for Linux, or zsh for macOS.

Run Python Commands and Scripts: You can run Python commands and scripts on the endpoint using the Python interpreter embedded in the Cortex XDR agent. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint.

Initiate a Live Terminal Session

Manage Processes

Manage Files

Run Operating System Commands

Run Python Commands and Scripts



Question 7

Question Type: MultipleChoice

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

Options:

- A- Remediation Automation
- B- Machine Remediation
- C- Automatic Remediation
- D- Remediation Suggestions



Answer:

D

Explanation:

When investigating security events, the feature in Cortex XDR that is useful for reverting the changes on the endpoint is Remediation Suggestions. Remediation Suggestions are a feature of

Cortex XDR that provide you with recommended actions to undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR. Reference:

Remediation Suggestions

Apply Remediation Suggestions

Question 8

Question Type: MultipleChoice

Which of the following represents the correct relation of alerts to incidents?

Options:

- A- Only alerts with the same host are grouped together into one Incident in a given time frame.
- B- Alerts that occur within a three-hour time frame are grouped together into one Incident.
- C- Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
- D- Every alert creates a new Incident.

Answer:

C

Explanation:

The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts, such as the alert source, type, and time period, to determine if they belong to the same causality chain. By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details¹.

Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a

malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack.

Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack.

Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes.

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9

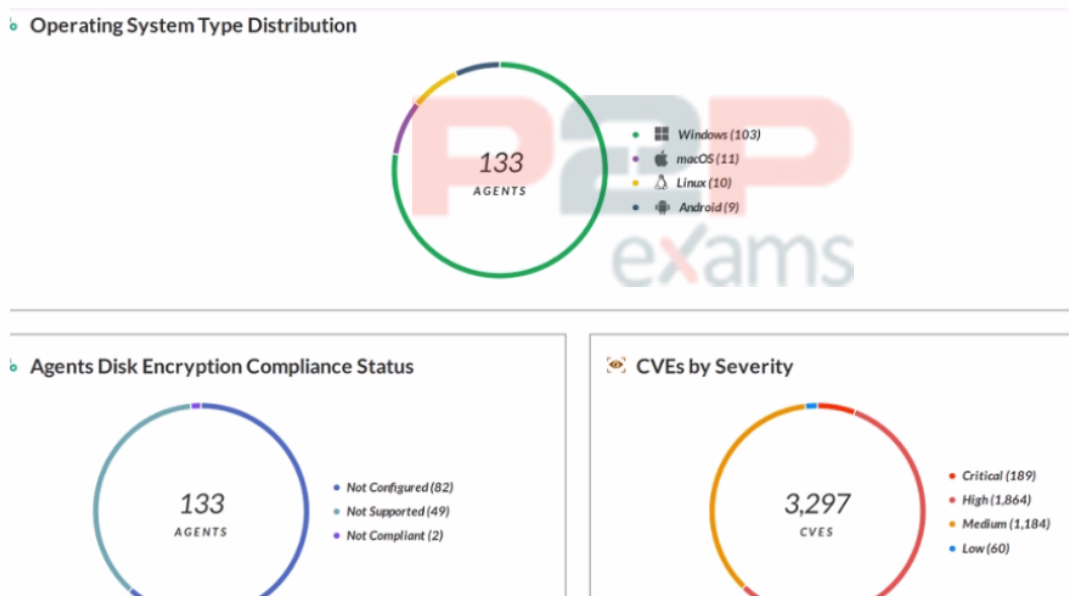
Palo Alto Networks Cortex XDR Documentation, Incident Management Overview²

Cortex XDR: Stop Breaches with AI-Powered Cybersecurity¹

Question 9

Question Type: MultipleChoice

Which statement is correct based on the report output below?



Options:

- A- Host Inventory Data Collection is enabled.
- B- 3,297 total incidents have been detected.
- C- Forensic inventory data collection is enabled.
- D- 133 agents have full disk encryption.

Answer:

C

Explanation:

The report output shows the number of endpoints that have forensic inventory data collection enabled, which is a feature of Cortex XDR that allows the collection of detailed information about the endpoint's hardware, software, and network configuration. This feature helps analysts to investigate and respond to incidents more effectively by providing a comprehensive view of the endpoint's state and activity. Forensic inventory data collection can be enabled or disabled per policy in Cortex XDR. Reference:

Forensic Inventory Data Collection

Cortex XDR 3: Getting Started with Endpoint Protection

Question 10

Question Type: MultipleChoice

What is the outcome of creating and implementing an alert exclusion?

Options:

- A- The Cortex XDR agent will allow the process that was blocked to run on the endpoint.
- B- The Cortex XDR console will hide those alerts.
- C- The Cortex XDR agent will not create an alert for this event in the future.
- D- The Cortex XDR console will delete those alerts and block ingestion of them in the future.

Answer:

B

Explanation:

The outcome of creating and implementing an alert exclusion is that the Cortex XDR console will hide those alerts that match the exclusion criteria. An alert exclusion is a policy that allows you to filter out alerts that are not relevant, false positives, or low priority, and focus on the alerts that require your attention. When you create an alert exclusion, you can specify the criteria that define which alerts you want to exclude, such as alert name, severity, source, or endpoint. After you create an alert exclusion, Cortex XDR will hide any future alerts that match the criteria, and exclude them from incidents and search query results. However, the alert exclusion does not affect the behavior of the Cortex XDR agent or the security policy on the endpoint. The Cortex XDR agent will still create an alert for the event and apply the appropriate action, such as blocking or quarantining, according to the security policy. The alert exclusion only affects the visibility of the alert on the Cortex XDR console, not the actual protection of the endpoint. Therefore, the correct answer is B, the Cortex XDR console will hide those alerts¹²

Alert Exclusions

Create an Alert Exclusion Policy

To Get Premium Files for XDR-Analyst Visit

<https://www.p2pexams.com/products/xdr-analyst>

For More Free Questions Visit

<https://www.p2pexams.com/palo-alto-networks/pdf/xdr-analyst>

20%
DISCOUNT

P2P
exams