Free Questions for PCDRA by vceexamstest

Shared by Mendoza on 09-08-2024

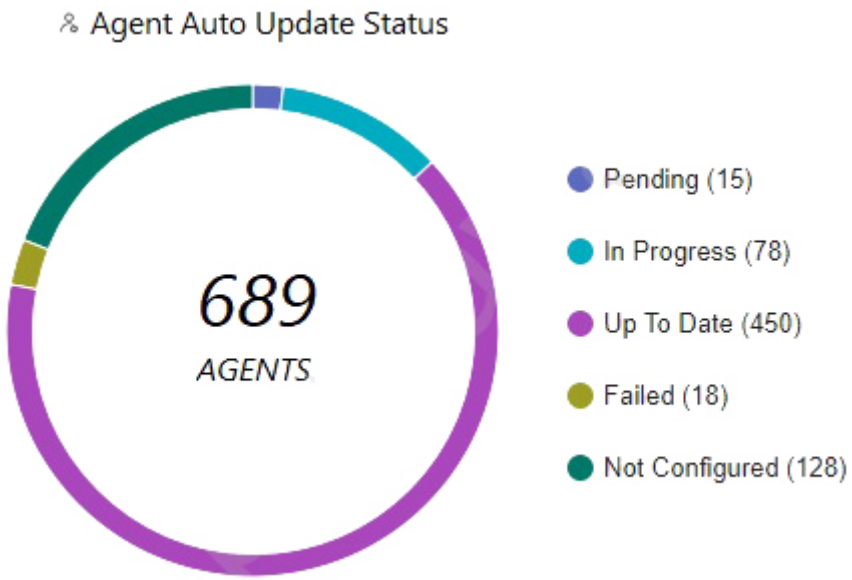
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which statement is true based on the following Agent Auto Upgrade widget?



Options:

A- There are a total of 689 Up To Date agents.

B- Agent Auto Upgrade was enabled but not on all endpoints.

C- Agent Auto Upgrade has not been enabled.

D- There are more agents in Pending status than In Progress status.

Answer:

B

Explanation:

The Agent Auto Upgrade widget shows the status of the agent auto upgrade feature on the endpoints. The widget displays the number of agents that are up to date, in progress, pending, failed, and not configured. In this case, the widget shows that there are 450 agents that are up to date, 78 in progress, 15 pending, 18 failed, and 128 not configured. This means that the agent auto upgrade feature was enabled but not on all endpoints.Reference:

Cortex XDR Agent Auto Upgrade

PCDRA Study Guide

Question 2

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 3

Question Type: **MultipleChoice**

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?

Options:

A- In the Restrictions Profile, add the file name and path to the Executable Files allow list.

B- Create a new rule exception and use the singer as the characteristic.

C- Add the signer to the allow list in the malware profile.

D- Add the signer to the allow list under the action center page.

Answer:

C

Explanation:

To prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. A malware profile is a profile that defines the settings and actions for malware prevention and detection on the endpoints. A malware profile allows you to specify a list of files, folders, or signers that you want to exclude from malware scanning and blocking.By adding the signer to the allow list in the malware profile, you can prevent the Cortex XDR Agent from blocking any file that is signed by that signer1.

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

A) In the Restrictions Profile, add the file name and path to the Executable Files allow list: This is not the correct answer. Adding the file name and path to the Executable Files allow list in the Restrictions Profile will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A Restrictions Profile is a profile that defines the settings and actions for restricting the execution of files or processes on the endpoints. A Restrictions Profile allows you to specify a list of executable files that you want to allow or block based on the file name and path.However, this method does not take into account the digital signer of the file, and it may not be effective

if the file name or path changes2.

B) Create a new rule exception and use the signer as the characteristic: This is not the correct answer. Creating a new rule exception and using the signer as the characteristic will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A rule exception is an exception that you can create to modify the behavior of a specific prevention rule or BIOC rule. A rule exception allows you to specify the characteristics and the actions that you want to apply to the exception, such as file hash, process name, IP address, or domain name.However, this method does not support using the signer as a characteristic, and it may not be applicable to all prevention rules or BIOC rules3.

D) Add the signer to the allow list under the action center page: This is not the correct answer. Adding the signer to the allow list under the action center page will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. The action center page is a page that allows you to create and manage actions that you can perform on your endpoints, such as isolating, scanning, collecting files, or executing scripts.The action center page does not have an option to add a signer to the allow list, and it is not related to the malware prevention or detection functionality4.

In conclusion, to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the allow list in the malware profile. By using this method, you can exclude the files that are signed by the trusted signer from the malware scanning and blocking.

Add a New Malware Security Profile

Add a New Restrictions Security Profile

Create a Rule Exception

Action Center

Question 4

Question Type: MultipleChoice

Which type of BIOC rule is currently available in Cortex XDR?

Options:

A- Threat Actor

B- Discovery

C- Network

D- Dropper

Answer:

B

Explanation:

The type of BIOC rule that is currently available in Cortex XDR is Discovery. A Discovery BIOC rule is a rule that detects suspicious or malicious behavior on endpoints based on the Cortex XDR data. A Discovery BIOC rule can use various event types, such as file,

injection, load image, network, process, registry, or user, to define the criteria for the rule. A Discovery BIOC rule can also use operators, functions, and variables to create complex logic and conditions for the rule.A Discovery BIOC rule can generate alerts when the rule is triggered, and these alerts can be grouped into incidents for further investigation and response12.

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

A) Threat Actor: This is not the correct answer. Threat Actor is not a type of BIOC rule that is currently available in Cortex XDR. Threat Actor is a term that refers to an individual or a group that is responsible for a cyberattack or a threat campaign.Cortex XDR does not support creating BIOC rules based on threat actors, but it can provide threat intelligence and context from various sources, such as Unit 42, AutoFocus, or Cortex XSOAR3.

C) Network: This is not the correct answer. Network is not a type of BIOC rule that is currently available in Cortex XDR. Network is an event type that can be used in a Discovery BIOC rule to define the criteria based on network attributes, such as source IP, destination IP, source port, destination port, protocol, or domain.Network is not a standalone type of BIOC rule, but a part of the Discovery BIOC rule2.

D) Dropper: This is not the correct answer. Dropper is not a type of BIOC rule that is currently available in Cortex XDR. Dropper is a term that refers to a type of malware that is designed to download and install other malicious files or programs on a compromised system.Cortex XDR does not support creating BIOC rules based on droppers, but it can detect and prevent droppers using various methods, such as behavioral threat protection, exploit prevention, or WildFire analysis4.

In conclusion, the type of BIOC rule that is currently available in Cortex XDR is Discovery. By using Discovery BIOC rules, you can create custom detection rules that match your specific use cases and scenarios.

Create a BIOC Rule

BIOC Rule Event Types

Threat Intelligence and Context

Malware Prevention

Question 5

Question Type: **MultipleChoice**

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?

Options:

A- Sensor Engine

B- Causality Analysis Engine

C- Log Stitching Engine

D- Causality Chain Engine

Answer:

B

Explanation:

The engine that determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident is the Causality Analysis Engine. The Causality Analysis Engine is one of the core components of Cortex XDR that performs advanced analytics on the data collected from various sources, such as endpoints, networks, and clouds. The Causality Analysis Engine uses machine learning and behavioral analysis to identify the root cause, the attack chain, and the impact of each alert. It also groups related alerts into incidents based on the temporal and logical relationships among the alerts.The Causality Analysis Engine helps to reduce the noise and complexity of alerts and incidents, and provides a clear and concise view of the attack story12.

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

A) Sensor Engine: This is not the correct answer. The Sensor Engine is not responsible for determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident. The Sensor Engine is the component that runs on the Cortex XDR agents installed on the endpoints. The Sensor Engine collects and analyzes endpoint data, such as processes, files, registry keys, network connections, and user activities.The Sensor Engine also enforces the endpoint security policies and performs prevention and response actions3.

C) Log Stitching Engine: This is not the correct answer. The Log Stitching Engine is not responsible for determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident. The Log Stitching Engine is the component that runs on the Cortex Data Lake, which is the cloud-based data storage and processing platform for Cortex XDR. The Log Stitching Engine normalizes and stitches together the data from different sources, such as firewalls, proxies, endpoints, and clouds.The Log Stitching Engine enables Cortex XDR to correlate and analyze data from multiple sources and provide a unified view of the network activity and

threat landscape4.

D) Causality Chain Engine: This is not the correct answer. Causality Chain Engine is not a valid name for any of the Cortex XDR engines. There is no such engine in Cortex XDR that performs the function of determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident.

In conclusion, the Causality Analysis Engine is the engine that determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident. By using the Causality Analysis Engine, Cortex XDR can provide a comprehensive and accurate detection and response capability for security analysts.

Cortex XDR Pro Admin Guide: Causality Analysis Engine

Cortex XDR Pro Admin Guide: View Incident Details

Cortex XDR Pro Admin Guide: Sensor Engine

Cortex XDR Pro Admin Guide: Log Stitching Engine

Question 6

Question Type: **MultipleChoice**

What does the following output tell us?

Top Hosts (Top 10 | Last 30 days)

HOST NAME	INCIDENTS BREAKDOWN	
shpapy_win10	**6**	[• 5 • 1]
win7mickey	**5**	[• 5]
desktop-vjb9012	**5**	[• 4 • 1]
cpsp-enzo	**4**	[• 3 • 1]
win10lab-thomas	**3**	[• 3]
pure_windows_10	**3**	[• 3]
lab1-8-cpsp	**3**	[• 3]
guru-pf	**3**	[• 3]
roneytestwindow	**3**	[• 3]
erikj-cpsp	**3**	[• 3]

Options:

A- There is one low severity incident.

B- Host shpapy_win10 had the most vulnerabilities.

C- There is one informational severity alert.

D- This is an actual output of the Top 10 hosts with the most malware.

Answer:

D

Explanation:

The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more .

Use the ACC to Analyze Network Activity

Top 10 Hosts with the Most Malware