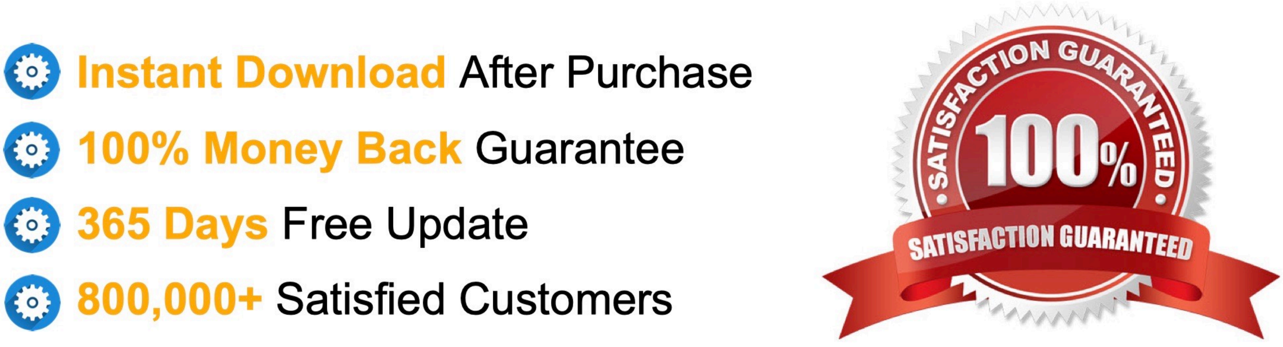
Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

What is an example of an attack vector for ransomware?

A. Performing DNS queries for suspicious domains

B. Performing SSL Decryption on an endpoint

C. Phishing emails containing malicious attachments

D. A URL filtering feature enabled on a firewall

Correct Answer: C

Explanation: An example of an attack vector for ransomware is phishing emails containing malicious attachments. Phishing is a technique that involves sending fraudulent emails that appear to come from alegitimate source, such as a bank, a company, or a government agency. The emails typically contain a malicious attachment, such as a PDF document, a ZIP archive, or a Microsoft Office document, that contains ransomware or a ransomware downloader. When the recipient opens or downloads the attachment, the ransomware is executed and encrypts the files or data on the victim\\'s system. The attacker then demands a ransom for the decryption key, usually in cryptocurrency. Phishing emails are one of the most common and effective ways of delivering ransomware, as they can bypass security measures such as firewalls, antivirus software, or URL filtering. Phishing emails can also exploit the human factor, as they can trick the recipient into opening the attachment by using social engineering techniques, such as impersonating a trusted sender, creating a sense of urgency, or appealing to curiosity or greed. Phishing emails can also target specific individuals or organizations, such as executives, employees, or customers, in a technique called spear phishing, which increases the chances of success. According to various sources, phishing emails are the main vector of ransomware attacks, accounting for more than 90% of all ransomware infections12. Some of the most notorious ransomware campaigns, such as CryptoLocker, Locky, and WannaCry, have used phishing emails as their primary delivery method3 . Therefore, it is essential to educate users on how to recognize and avoid phishing emails, as well as to implement security solutions that can detect and block malicious attachments. References: Top 7 Ransomware Attack Vectors and How to Avoid Becoming a Victim - Bitsight What Is the Main Vector of Ransomware Attacks? A Definitive Guide CryptoLocker Ransomware Information Guide and FAQ [Locky Ransomware Information, Help Guide, and FAQ] [WannaCry ransomware attack]

QUESTION 2

When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

A. The agent technical support file.

B. The prevention archive from the alert.

C. The distribution id of the agent.

D. A list of all the current exceptions applied to the agent.

E. The unique agent id.

Correct Answer: AB

Explanation: When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are: The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself. The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself. The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example: The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder. A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent\\'s security policies. The exceptions can help TAC understand the agent\\'s configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file. The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file. References: Generate and Download the Agent Technical Support File Generate and Download the Prevention Archive Cortex XDR Agent Administrator Guide: Agent Distribution ID Cortex XDR Agent Administrator Guide: Exception Security Profiles [Cortex XDR Agent Administrator Guide: Unique Agent ID]

QUESTION 3

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

A. Malware Protection profile

B. Malware profile

C. Malware Detection profile

D. Anti-Malware profile

Correct 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. References: Malware Protection Profile Endpoint Security Policy

QUESTION 4

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

A. Only alerts with the same host are grouped together into one Incident in a given time frame.

B. Alerts that occur within athree-hourtime 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.

Correct 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. References: 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 5

What is by far the most common tactic used by ransomware to shut down a victim\\'s operation?

A. preventing the victim from being able to access APIs to cripple infrastructure

B. denying traffic out of the victims network until payment is received

C. restricting access to administrative accounts to the victim

D. encrypting certain files to prevent access by the victim

Correct Answer: D

Explanation: Ransomware is a type of malicious software, or malware, that encrypts certain files or data on the victim\\'s system or network and prevents them from accessing their data until they pay a ransom. This is by far the most common tactic used by ransomware to shut down a victim\\'s operation, as it can cause costly disruptions, data loss, and reputational damage. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again. Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack1234 References: What is Ransomware? | How to Protect Against Ransomware in 2023 Ransomware - Wikipedia What is ransomware? | Ransomware meaning | Cloudflare [What Is Ransomware? | Ransomware.org] [Ransomware -- FBI]