Free Questions for PCDRA by actualtestdumps

Shared by Washington on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

How can you pivot within a row to Causality view and Timeline views for further investigate?

Options:

A- Using the Open Card Only

B- Using the Open Card and Open Timeline actions respectively

C- You can't pivot within a row to Causality view and Timeline views

D- Using Open Timeline Actions Only

Answer:

B

Explanation:

To pivot within a row to Causality view and Timeline views for further investigation, you can use the Open Card and Open Timeline actions respectively. The Open Card action will open a new tab with the Causality view of the selected row, showing the causal chain of events that led to the alert. The Open Timeline action will open a new tab with the Timeline view of the selected row, showing the chronological sequence of events that occurred on the affected endpoint. These actions allow you to drill down into the details of each alert and understand the root cause and impact of the incident.Reference:

Cortex XDR User Guide, Chapter 9: Investigate Alerts, Section: Pivot to Causality View and Timeline View

PCDRA Study Guide, Section 3: Investigate and Respond to Alerts, Objective 3.1: Investigate alerts using the Causality view and Timeline view

Question 2

Question Type: MultipleChoice

What is the Wildfire analysis file size limit for Windows PE files?

Options:

A- No Limit

B- 500MB

C- 100MB

D- 1GB

Answer:

C

Explanation:

The Wildfire analysis file size limit for Windows PE files is 100MB. Windows PE files are executable files that run on the Windows operating system, such as .exe, .dll, .sys, or .scr files. Wildfire is a cloud-based service that analyzes files and URLs for malicious behavior and generates signatures and protections for them. Wildfire can analyze various file types, such as PE, APK, PDF, MS Office, and others, but each file type has a different file size limit. The file size limit determines the maximum size of the file that can be uploaded or forwarded to Wildfire for analysis. If the file size exceeds the limit, Wildfire will not analyze the file and will return an error message.

According to the Wildfire documentation1, the file size limit for Windows PE files is 100MB. This means that any PE file that is larger than 100MB will not be analyzed by Wildfire. However, the firewall can still apply other security features, such as antivirus, anti-spyware, vulnerability protection, and file blocking, to the PE file based on the security policy settings.The firewall can also perform local analysis on the PE file using the Cortex XDR agent, which uses machine learning models to assess the file and assign it a verdict2.

WildFire File Size Limits: This document provides the file size limits for different file types that can be analyzed by Wildfire.

Local Analysis: This document explains how the Cortex XDR agent performs local analysis on files that cannot be sent to Wildfire for analysis.

Question 3

Question Type: **MultipleChoice**

What is an example of an attack vector for ransomware?

Options:

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

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 a legitimate 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.Reference:

Top 7 Ransomware Attack Vectors & 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 4

Question Type: MultipleChoice

Which of the following paths will successfully activate Remediation Suggestions?

Options:

A- Incident View > Actions > Remediation Suggestions

B- Causality View > Actions > Remediation Suggestions

C- Alerts Table > Right-click on a process node > Remediation Suggestions

D- Alerts Table > Right-click on an alert > Remediation Suggestions

Answer:

B

Explanation:

Remediation Suggestions is a feature of Cortex XDR that provides you with recommended actions to remediate the root cause and impact of an incident. Remediation Suggestions are based on the analysis of the causality chain, the behavior of the malicious files or processes, and the best practices for incident response. Remediation Suggestions can help you to quickly and effectively contain and resolve an incident, as well as prevent future recurrence.

To activate Remediation Suggestions, you need to follow these steps:

In the Cortex XDR management console, go toIncidentsand select an incident that you want to remediate.

ClickCausality Viewto see the graphical representation of the causality chain of the incident.

ClickActionsand selectRemediation Suggestions. This will open a new window that shows the suggested actions for each node in the causality chain.

Review the suggested actions and select the ones that you want to apply. You can also edit or delete the suggested actions, or add your own custom actions.

ClickApplyto execute the selected actions on the affected endpoints. You can also schedule the actions to run at a later time or date.

Remediate Changes from Malicious Activity: This document explains how to use Remediation Suggestions to remediate the root cause and impact of an incident.

Causality View: This document describes how to use Causality View to investigate the causality chain of an incident.

Question 5

Question Type: **MultipleChoice**

The Cortex XDR console has triggered an incident, blocking a vitally important piece of software in your organization that is known to be benign. Which of the following options would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization?

Options:

A- Create an individual alert exclusion.

B- Create a global inclusion.

C- Create an endpoint-specific exception.

D- Create a global exception.

Answer:

D

Explanation:

A global exception is a rule that allows you to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR. A global exception applies to all endpoints in your organization that are protected by Cortex XDR. Creating a global exception for a vitally important piece of software that is known to be benign would prevent Cortex XDR from blocking this software in the future, for all endpoints in your organization.

To create a global exception, you need to follow these steps:

In the Cortex XDR management console, go toPolicy Management > Exceptionsand clickAdd Exception.

Select theGlobal Exceptionoption and clickNext.

Enter a name and description for the exception and clickNext.

Select the type of exception you want to create, such as file, process, or behavior, and clickNext.

Specify the criteria for the exception, such as file name, hash, path, process name, command line, or behavior name, and clickNext.

Review the summary of the exception and clickFinish.

Create Global Exceptions: This document explains how to create global exceptions to exclude specific files, processes, or behaviors from being blocked or detected by Cortex XDR.

Exceptions Overview: This document provides an overview of exceptions and how they can be used to fine-tune the Cortex XDR security policy.

Question 6

Question Type: **MultipleChoice**

Which minimum Cortex XDR agent version is required for Kubernetes Cluster?

Options:

A- Cortex XDR 6.1

B- Cortex XDR 7.4

C- Cortex XDR 7.5

D- Cortex XDR 5.0

Answer:

C

Explanation:

The minimum Cortex XDR agent version required for Kubernetes Cluster is Cortex XDR 7.5. This version introduces the Cortex XDR agent for Kubernetes hosts, which provides protection and visibility for Linux hosts that run on Kubernetes clusters. The Cortex XDR agent for Kubernetes hosts supports the following features:

Anti-malware protection

Behavioral threat protection

Exploit protection

File integrity monitoring

Network security

Audit and remediation

Live terminal

To install the Cortex XDR agent for Kubernetes hosts, you need to deploy the Cortex XDR agent as a DaemonSet on your Kubernetes cluster. You also need to configure the agent settings profile and the agent installer in the Cortex XDR management console.Reference:

Cortex XDR Agent Release Notes: This document provides the release notes for Cortex XDR agent versions, including the new features, enhancements, and resolved issues.

Install the Cortex XDR Agent for Kubernetes Hosts: This document explains how to install and configure the Cortex XDR agent for Kubernetes hosts using the Cortex XDR management console and the Kubernetes command-line tool.

Question 7

Question Type: **MultipleChoice**

Why would one threaten to encrypt a hypervisor or, potentially, a multiple number of virtual machines running on a server?

Options:

A- To extort a payment from a victim or potentially embarrass the owners.

B- To gain notoriety and potentially a consulting position.

C- To better understand the underlying virtual infrastructure.

D- To potentially perform a Distributed Denial of Attack.

Answer:

A

Explanation:

Encrypting a hypervisor or a multiple number of virtual machines running on a server is a form of ransomware attack, which is a type of cyberattack that involves locking or encrypting the victim's data or system and demanding a ransom for its release. The attacker may threaten to encrypt the hypervisor or the virtual machines to extort a payment from the victim or potentially embarrass the owners by exposing their sensitive or confidential information. Encrypting a hypervisor or a multiple number of virtual machines can have a severe impact on the victim's business operations, as it can affect the availability, integrity, and confidentiality of their data and applications. The attacker may also use the encryption as a leverage to negotiate a higher ransom or to coerce the victim into complying with their demands.Reference:

Encrypt an Existing Virtual Machine or Virtual Disk: This document explains how to encrypt an existing virtual machine or virtual disk using the vSphere Client.

How to Encrypt an Existing or New Virtual Machine: This article provides a guide on how to encrypt an existing or new virtual machine using AOMEI Backupper.

Ransomware: This document provides an overview of ransomware, its types, impacts, and prevention methods.

Question 8

Question Type: MultipleChoice

Which Exploit Protection Module (EPM) can be used to prevent attacks based on OS function?

Options:

A- UASLR

B- JIT Mitigation

C- Memory Limit Heap Spray Check

D- DLL Security

Answer:

B

Explanation:

JIT Mitigation is an Exploit Protection Module (EPM) that can be used to prevent attacks based on OS function. JIT Mitigation protects against exploits that use the Just-In-Time (JIT) compiler of the OS to execute malicious code. JIT Mitigation monitors the memory pages that are allocated by the JIT compiler and blocks any attempts to execute code from those pages. This prevents attackers from using the JIT compiler as a way to bypass other security mechanisms such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR).Reference:

Palo Alto Networks. (2023). PCDRA Study Guide. PDF file. Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf

Palo Alto Networks. (2021). Exploit Protection Modules. Web page. Retrieved from https://docs.paloaltonetworks.com/traps/6-0/traps-endpoint-security-manager-admin/traps-endpoint-security-policies/exploit-protection-modules.html

Question 9

Question Type: MultipleChoice

What is the maximum number of agents one Broker VM local agent applet can support?

Options:

A- 5,000

B- 10,000

C- 15,000

D- 20,000

Answer:

B

Explanation:

The Broker VM is a virtual machine that you can deploy in your network to provide various services and functionalities to the Cortex XDR agents. One of the services that the Broker VM offers is the Local Agent Settings applet, which allows you to configure the agent proxy, agent installer, and content caching settings for the agents. The Local Agent Settings applet can support a maximum number of10,000 agentsper Broker VM. If you have more than 10,000 agents in your network, you need to deploy additional Broker VMs and distribute the load among them.Reference:

Broker VM Overview: This document provides an overview of the Broker VM and its features, requirements, and deployment options.

Configure the Broker VM: This document explains how to install, set up, and configure the Broker VM in an ESXi environment.

Manage Broker VM from the Cortex XDR Management Console: This document describes how to activate and manage the Broker VM applets from the Cortex XDR management console.

Question 10

Question Type: **MultipleChoice**

Which of the following represents a common sequence of cyber-attack tactics?

Options:

A- Actions on the objective Reconnaissance Weaponization & Delivery Exploitation Installation Command & Control

B- Installation >> Reconnaissance Weaponization & Delivery Exploitation Command & Control Actions on the objective

C- Reconnaissance Weaponization & Delivery Exploitation Installation Command & Control Actions on the objective

D- Reconnaissance >> Installation Weaponization & Delivery Exploitation Command & Control Actions on the objective

Answer:

C

Explanation:

A common sequence of cyber-attack tactics is based on the Cyber Kill Chain model, which describes the stages of a cyber intrusion from the perspective of the attacker. The Cyber Kill Chain model consists of seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. These phases are briefly explained below:

Reconnaissance: The attacker gathers information about the target, such as its network, systems, vulnerabilities, employees, and business operations. The attacker may use various methods, such as scanning, phishing, or searching open sources, to collect data that can help them plan the attack.

Weaponization: The attacker creates or obtains a malicious payload, such as malware, exploit, or script, that can be used to compromise the target. The attacker may also embed the payload into a delivery mechanism, such as an email attachment, a web link, or a removable media.

Delivery: The attacker sends or delivers the weaponized payload to the target, either directly or indirectly. The attacker may use various channels, such as email, web, or physical access, to reach the target's network or system.

Exploitation: The attacker exploits a vulnerability or weakness in the target's network or system to execute the payload. The vulnerability may be technical, such as a software flaw, or human, such as a social engineering trick.

Installation: The attacker installs or drops additional malware or tools on the target's network or system to establish a foothold and maintain persistence. The attacker may use various techniques, such as registry modification, file manipulation, or process injection, to hide their presence and evade detection.

Command and Control: The attacker establishes a communication channel between the compromised target and a remote server or controller. The attacker may use various protocols, such as HTTP, DNS, or IRC, to send commands and receive data from the target.

Actions on the objective: The attacker performs the final actions that achieve their goal, such as stealing data, destroying files, encrypting systems, or disrupting services. The attacker may also try to move laterally within the target's network or system to access more resources or data.

Cyber Kill Chain: This document explains the Cyber Kill Chain model and how it can be used to analyze and respond to cyberattacks.

Cyber Attack Tactics: This document provides an overview of some common cyber attack tactics and examples of how they are used by threat actors.

Question 11

Question Type: MultipleChoice

Can you disable the ability to use the Live Terminal feature in Cortex XDR?

Options:

A- Yes, via the Cortex XDR console or with an installation switch.

B- No, a separate installer package without Live Terminal is required.

C- No, it is a required feature of the agent.

D- Yes, via Agent Settings Profile.

Answer:

D

Explanation:

The Live Terminal feature in Cortex XDR allows you to initiate a remote connection to an endpoint and perform various actions such as running commands, uploading and downloading files, and terminating processes. You can disable the ability to use the Live Terminal feature in Cortex XDR by configuring the Agent Settings Profile. The Agent Settings Profile defines the behavior and functionality of the Cortex XDR agent on the endpoint. You can create different profiles for different groups of endpoints and assign them accordingly. To disable the Live Terminal feature, you need to uncheck theEnable Live Terminaloption in the Agent Settings Profile and save the changes. This will prevent the Cortex XDR agent from accepting any Live Terminal requests from the Cortex XDR management console.Reference:

Live Terminal: This document explains how to use the Live Terminal feature to investigate and respond to security events on Windows endpoints.

Agent Settings Profile: This document describes how to create and manage Agent Settings Profiles to define the behavior and functionality of the Cortex XDR agent on the endpoint.