

PaloAltoNetworks.XDR-Analyst.v2026-03-30.q39

Exam Code:	XDR-Analyst
Exam Name:	Palo Alto Networks XDR Analyst
Certification Provider:	Palo Alto Networks
Free Question Number:	39
Version:	v2026-03-30
# of views:	140
# of Questions views:	390
https://www.freepdf dumps.com/PaloAltoNetworks.XDR-Analyst.v2026-03-30.q39.html	

NEW QUESTION: 1

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

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

Answer: D ([LEAVE A REPLY](#))

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

NEW QUESTION: 2

Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

- A. in the macOS Malware Protection Profile to indicate allowed signers
- B. in the Linux Malware Protection Profile to indicate allowed Java libraries
- C. SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles
- D. in the Windows Malware Protection Profile to indicate allowed executables

Answer: D ([LEAVE A REPLY](#))

Cortex XDR Malware Protection Profiles allow you to configure the malware prevention settings for Windows, Linux, and macOS endpoints. You can use SHA256 hash values in the Windows Malware Protection Profile to indicate allowed executables that you want to exclude from malware scanning. This can help you reduce false positives and improve performance by skipping the scanning of known benign files. You can add up to 1000 SHA256 hash values per profile. You cannot use SHA256 hash values in the Linux or macOS Malware Protection Profiles, but you can use other criteria such as file path, file name, or signer to exclude files from scanning. Reference: Malware Protection Profiles
Configure a Windows Malware Protection Profile
PCDRA Study Guide

NEW QUESTION: 3

What is the action taken out by Managed Threat Hunting team for Zero Day Exploits?

- A. MTH researches for threats in the tenant and generates a report with the findings.
- B. MTH researches for threats in the logs and reports to engineering.
- C. MTH runs queries and investigative actions and no further action is taken.
- D. MTH pushes content updates to prevent against the zero-day exploits.

Answer: A ([LEAVE A REPLY](#))

The Managed Threat Hunting (MTH) team is a group of security experts who proactively hunt for threats in the Cortex XDR tenant and generate a report with the findings. The MTH team uses advanced queries and investigative actions to identify and analyze potential threats, such as zero-day exploits, that may have bypassed the prevention and detection capabilities of Cortex XDR. The MTH team also provides recommendations and best practices to help customers remediate the threats and improve their security posture. Reference:
Managed Threat Hunting Service
Managed Threat Hunting Report

NEW QUESTION: 4

Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

- A. Search & destroy
- B. Isolation
- C. Quarantine
- D. Flag for removal

Answer: C ([LEAVE A REPLY](#))

The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a

hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console. Reference:

Quarantine Files

Manage Quarantined Files

NEW QUESTION: 5

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

Answer: ([SHOW ANSWER](#))

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]

NEW QUESTION: 6

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

- A. No Limit
- B. 500MB
- C. 100MB
- D. 1GB

Answer: ([SHOW ANSWER](#))

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.

Reference:

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.

NEW QUESTION: 7

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

- A. Threat Actor
- B. Discovery
- C. Network
- D. Dropper

Answer: B ([LEAVE A REPLY](#))

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.

Reference:

Create a BIOC Rule

BIOC Rule Event Types

Threat Intelligence and Context

Malware Prevention

NEW QUESTION: 8

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

A. UASLR

B. JIT Mitigation

C. Memory Limit Heap Spray Check

D. DLL Security

Answer: B ([LEAVE A REPLY](#))

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>

NEW QUESTION: 9

Which of the following policy exceptions applies to the following description?

'An exception allowing specific PHP files'

- A. Support exception
- B. Local file threat examination exception
- C. Behavioral threat protection rule exception
- D. Process exception

Answer: B ([LEAVE A REPLY](#))

The policy exception that applies to the following description is B, local file threat examination exception. A local file threat examination exception is an exception that allows you to exclude specific files or folders from being scanned by the Cortex XDR agent for malware or threats. You can use this exception to prevent false positives, performance issues, or compatibility problems with legitimate files or applications. You can define the local file threat examination exception by file name, file path, file hash, or digital signer. For example, you can create a local file threat examination exception for specific PHP files by entering their file names or paths in the exception configuration. Reference:

Local File Threat Examination Exceptions

Create a Local File Threat Examination Exception

NEW QUESTION: 10

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

- 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: ([SHOW ANSWER](#)**)**

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 Reference:

Alert Exclusions

Create an Alert Exclusion Policy

NEW QUESTION: 11

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

- 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 ([LEAVE A REPLY](#))

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.

Reference:

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.

NEW QUESTION: 12

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically close the connections involved in malicious traffic.
- B. Automatically kill the processes involved in malicious activity.
- C. Automatically terminate the threads involved in malicious activity.
- D. Automatically block the IP addresses involved in malicious traffic.

Answer: B,D (LEAVE A REPLY)

The "Respond to Malicious Causality Chains" feature in a Cortex XDR Windows Malware profile allows the agent to take automatic actions against network connections and processes that are involved in malicious activity on the endpoint. The feature has two modes: Block IP Address and Kill Process¹.

The two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile are:

Automatically kill the processes involved in malicious activity. This can help to stop the malware from spreading or doing any further damage.

Automatically block the IP addresses involved in malicious traffic. This can help to prevent the malware from communicating with its command and control server or other malicious hosts.

The other two options, automatically close the connections involved in malicious traffic and automatically terminate the threads involved in malicious activity, are not specific to "Respond to Malicious Causality Chains". They are general security measures that the agent can perform regardless of the feature.

Reference:

Cortex XDR Agent Security Profiles

Cortex XDR Agent 7.5 Release Notes

PCDRA: What are purposes of "Respond to Malicious Causality Chains" in ...

NEW QUESTION: 13

Which two types of exception profiles you can create in Cortex XDR? (Choose two.)

- A. exception profiles that apply to specific endpoints
- B. agent exception profiles that apply to specific endpoints
- C. global exception profiles that apply to all endpoints

D. role-based profiles that apply to specific endpoints

Answer: B,C ([LEAVE A REPLY](#))

Cortex XDR allows you to create two types of exception profiles: agent exception profiles and global exception profiles. Agent exception profiles apply to specific endpoints that are assigned to the profile. Global exception profiles apply to all endpoints in your network. You can use exception profiles to configure different types of exceptions, such as process exceptions, support exceptions, behavioral threat protection rule exceptions, local analysis rules exceptions, advanced analysis exceptions, or digital signer exceptions. Exception profiles help you fine-tune the security policies for your endpoints and reduce false positives. Reference:

Exception Security Profiles

Create an Agent Exception Profile

Create a Global Exception Profile

NEW QUESTION: 14

Which search methods is supported by File Search and Destroy?

A. File Seek and Destroy

B. File Search and Destroy

C. File Seek and Repair

D. File Search and Repair

Answer: B ([LEAVE A REPLY](#))

File Search and Destroy is a feature of Cortex XDR that allows you to search for and remove malicious files from endpoints. You can use this feature to find files by their hash, full path, or partial path using regex parameters. You can then select the files from the search results and destroy them by hash or by path. When you destroy a file by hash, all the file instances on the endpoint are removed. File Search and Destroy is useful for quickly responding to threats and preventing further damage. Reference:

Search and Destroy Malicious Files

Cortex XDR Pro Administrator Guide

NEW QUESTION: 15

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

A. Cortex XDR 6.1

B. Cortex XDR 7.4

C. Cortex XDR 7.5

D. Cortex XDR 5.0

Answer: C ([LEAVE A REPLY](#))

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.

NEW QUESTION: 16

Network attacks follow predictable patterns. If you interfere with any portion of this pattern, the attack will be neutralized. Which of the following statements is correct?

- A. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.
- B. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.
- C. Cortex XDR Analytics does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.
- D. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

Answer: ([SHOW ANSWER](#))

Cortex XDR Analytics is a cloud-based service that uses machine learning and artificial intelligence to detect and prevent network attacks. Cortex XDR Analytics can interfere with the attack pattern as soon as it is observed on the endpoint by applying protection policies that block malicious processes, files, or network connections. This way, Cortex XDR Analytics can stop the attack before it causes any damage or compromises the system. Reference:

[Cortex XDR Analytics Overview]

[Cortex XDR Analytics Protection Policies]

Valid XDR-Analyst Dumps shared by Actual4test.com for Helping Passing XDR-Analyst Exam! Actual4test.com now offer the **newest XDR-Analyst exam dumps**, the Actual4test.com XDR-Analyst exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com XDR-Analyst dumps with Test Engine here:

NEW QUESTION: 17

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

- 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 (LEAVE A REPLY)

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 the Enable Live Terminal option 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.

NEW QUESTION: 18

What is the purpose of the Unit 42 team?

- A. Unit 42 is responsible for automation and orchestration of products
- B. Unit 42 is responsible for the configuration optimization of the Cortex XDR server
- C. Unit 42 is responsible for threat research, malware analysis and threat hunting
- D. Unit 42 is responsible for the rapid deployment of Cortex XDR agents

Answer: C (LEAVE A REPLY)

Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities¹².

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

A . Unit 42 is not responsible for automation and orchestration of products. Automation and orchestration are capabilities that are provided by Palo Alto Networks products such as Cortex XSOAR, which is a security orchestration, automation and response platform that helps security teams automate tasks, coordinate actions and manage incidents³.

B . Unit 42 is not responsible for the configuration optimization of the Cortex XDR server. The Cortex XDR server is the cloud-based platform that provides detection and response capabilities across network, endpoint and cloud data sources. The configuration optimization of the Cortex XDR server is the responsibility of the Cortex XDR administrators, who can use the Cortex XDR app to manage the settings and policies of the Cortex XDR server⁴.

C . Unit 42 is not responsible for the rapid deployment of Cortex XDR agents. The Cortex XDR agents are the software components that are installed on endpoints to provide protection and visibility. The rapid deployment of Cortex XDR agents is the responsibility of the Cortex XDR administrators, who can use various methods such as group policy objects, scripts, or third-party tools to deploy the Cortex XDR agents to multiple endpoints⁵.

In conclusion, Unit 42 is the threat intelligence and response team of Palo Alto Networks that is responsible for threat research, malware analysis and threat hunting. By leveraging the expertise and insights of Unit 42, organizations can enhance their security posture and protect against the latest cyberthreats.

Reference:

About Unit 42: Our Mission and Team

Unit 42: Threat Intelligence & Response

Cortex XSOAR

Cortex XDR Pro Admin Guide: Manage Cortex XDR Settings and Policies

Cortex XDR Pro Admin Guide: Deploy Cortex XDR Agents

NEW QUESTION: 19

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?

- A. Create an individual alert exclusion.
- B. Create a global inclusion.
- C. Create an endpoint-specific exception.
- D. Create a global exception.

Answer: D ([LEAVE A REPLY](#))

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 to Policy Management > Exceptions and click Add Exception.

Select the Global Exception option and click Next.

Enter a name and description for the exception and click Next.

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

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

Review the summary of the exception and click Finish.

Reference:

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.

NEW QUESTION: 20

A Linux endpoint with a Cortex XDR Pro per Endpoint license and Enhanced Endpoint Data enabled has reported malicious activity, resulting in the creation of a file that you wish to delete. Which action could you take to delete the file?

- A. Manually remediate the problem on the endpoint in question.
- B. Open X2go from the Cortex XDR console and delete the file via X2go.
- C. Initiate Remediate Suggestions to automatically delete the file.
- D. Open an NFS connection from the Cortex XDR console and delete the file.

Answer: ([SHOW ANSWER](#))

The best action to delete the file on the Linux endpoint is to initiate Remediation Suggestions from the Cortex XDR console. 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.

The other options are incorrect for the following reasons:

A is incorrect because manually remediating the problem on the endpoint is not a convenient or efficient way to delete the file. Manually remediating the problem would require you to access the endpoint directly, log in as root, locate the file, and delete it. This would also require you to have the necessary permissions and credentials to access the endpoint, and to know the exact path and name of the file. Manually remediating the problem would also not provide you with any audit trail or confirmation of the deletion.

B is incorrect because opening X2go from the Cortex XDR console is not a supported or secure way to delete the file. X2go is a third-party remote desktop software that allows you to access Linux endpoints from a graphical user interface. However, X2go is not integrated with Cortex XDR, and using it would require you to install and configure it on both the Cortex XDR console and the endpoint. Using X2go would also expose the endpoint to potential network attacks or unauthorized access, and would not provide you with any audit trail or confirmation of the deletion.

D is incorrect because opening an NFS connection from the Cortex XDR console is not a feasible or reliable way to delete the file. NFS is a network file system protocol that allows you to access

files on remote servers as if they were local. However, NFS is not integrated with Cortex XDR, and using it would require you to set up and maintain an NFS server and client on both the Cortex XDR console and the endpoint. Using NFS would also depend on the network availability and performance, and would not provide you with any audit trail or confirmation of the deletion.

Reference:

Remediation Suggestions

Apply Remediation Suggestions

NEW QUESTION: 21

What motivation do ransomware attackers have for returning access to systems once their victims have paid?

- A. There is organized crime governance among attackers that requires the return of access to remain in good standing.
- B. Nation-states enforce the return of system access through the use of laws and regulation.
- C. Failure to restore access to systems undermines the scheme because others will not believe their valuables would be returned.
- D. The ransomware attackers hope to trace the financial trail back and steal more from traditional banking institutions. -

Answer: C ([LEAVE A REPLY](#))

Ransomware attackers have a motivation to return access to systems once their victims have paid because they want to maintain their reputation and credibility. If they fail to restore access to systems, they risk losing the trust of future victims who may not believe that paying the ransom will result in getting their data back. This would reduce the effectiveness and profitability of their scheme. Therefore, ransomware attackers have an incentive to honor their promises and decrypt the data after receiving the ransom. Reference:

What is the motivation behind ransomware? | Foresite

As Ransomware Attackers' Motives Change, So Should Your Defense - Forbes

NEW QUESTION: 22

When creating a custom XQL query in a dashboard, how would a user save that XQL query to the Widget Library?

- A. Click the three dots on the widget and then choose "Save" and this will link the query to the Widget Library.
- B. This isn't supported, you have to exit the dashboard and go into the Widget Library first to create it.
- C. Click on "Save to Action Center" in the dashboard and you will be prompted to give the query a name and description.
- D. Click on "Save to Widget Library" in the dashboard and you will be prompted to give the query a name and description.

Answer: ([SHOW ANSWER](#))

To save a custom XQL query to the Widget Library, you need to click on "Save to Widget Library" in the dashboard and you will be prompted to give the query a name and description. This will allow you to reuse the query in other dashboards or reports. You cannot save a query to the Widget Library by clicking the three dots on the widget, as this will only give you options to edit, delete, or clone the widget. You also cannot save a query to the Action Center, as this is a different feature that allows you to create alerts or remediation actions based on the query results. You do not have to exit the dashboard and go into the Widget Library first to create a query, as you can do it directly from the dashboard. Reference:

Cortex XDR Pro Admin Guide: Save a Custom Query to the Widget Library

Cortex XDR Pro Admin Guide: Create a Dashboard

NEW QUESTION: 23

Which statement regarding scripts in Cortex XDR is true?

- A. Any version of Python script can be run.
- B. The level of risk is assigned to the script upon import.
- C. Any script can be imported including Visual Basic (VB) scripts.
- D. The script is run on the machine uploading the script to ensure that it is operational.

Answer: (SHOW ANSWER)

The correct answer is B, the level of risk is assigned to the script upon import. When you import a script to the Agent Script Library in Cortex XDR, you need to specify the level of risk associated with the script. The level of risk determines the permissions and restrictions for running the script on endpoints. The levels of risk are:

Low: The script can be run on any endpoint without requiring approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.

Medium: The script can be run on any endpoint, but requires approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.

High: The script can only be run on isolated endpoints, and requires approval from the Cortex XDR administrator. The script cannot be used in remediation suggestions or automation actions.

The other options are incorrect for the following reasons:

A is incorrect because not any version of Python script can be run in Cortex XDR. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. For example, the scripts must not exceed 64 KB in size, must not use external libraries or modules, and must not contain malicious or harmful code.

C is incorrect because not any script can be imported to Cortex XDR, including Visual Basic (VB) scripts. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. VB scripts are not supported by Cortex XDR, and will not run on the endpoints.

D is incorrect because the script is not run on the machine uploading the script to ensure that it is operational. The script is only validated for syntax errors and size limitations when it is imported to the Agent Script Library. The script is not executed or tested on the machine uploading the script, and the script may still fail or cause errors when it is run on the endpoints.

Reference:

Agent Script Library

Import a Script

Run Scripts on an Endpoint

NEW QUESTION: 24

In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

- A. Agent Proxy
- B. Agent Installer and Content Caching
- C. Syslog Collector
- D. CSV Collector

Answer: B (LEAVE A REPLY)

The Agent Installer and Content Caching applet of the Broker VM is used to download and cache the Cortex XDR agent installation packages and content updates from Palo Alto Networks servers. This applet also acts as a proxy server for the Cortex XDR agents to communicate with the Cortex Data Lake and the Cortex XDR management console. To ensure secure communication between the Broker VM and the Cortex XDR agents, you are required to install a strong cipher SHA256-based SSL certificate on the Broker VM. The SSL certificate must have a common name or subject alternative name that matches the Broker VM FQDN or IP address. The SSL certificate must also be trusted by the Cortex XDR agents, either by using a certificate signed by a public CA or by manually installing the certificate on the endpoints. Reference:

Agent Installer and Content Caching

Install an SSL Certificate on the Broker VM

NEW QUESTION: 25

Which statement is correct based on the report output below?

Operating System Type Distribution



Agents Disk Encryption Compliance Status



CVEs by Severity



- 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 ([LEAVE A REPLY](#))

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

NEW QUESTION: 26

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

Answer: (SHOW ANSWER)

Live Terminal uses the WebSocket protocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic. Reference:

Initiate a Live Terminal Session

WebSocket

NEW QUESTION: 27

You can star security events in which two ways? (Choose two.)

- A. Create an alert-starring configuration.
- B. Create an Incident-starring configuration.
- C. Manually star an alert.
- D. Manually star an Incident.

Answer: C,D ([LEAVE A REPLY](#))

You can star security events in Cortex XDR in two ways: manually star an alert or an incident, or create an alert-starring or incident-starring configuration. Starring security events helps you

prioritize and track the events that are most important to you. You can also filter and sort the events by their star status in the Cortex XDR console.

To manually star an alert or an incident, you can use the star icon in the Alerts table or the Incidents table. You can also star an alert from the Causality View or the Query Center Results table. You can star an incident from the Incident View or the Query Center Results table. You can also unstar an event by clicking the star icon again.

To create an alert-starring or incident-starring configuration, you can use the Alert Starring Configuration or the Incident Starring Configuration pages in the Cortex XDR console. You can define the criteria for starring alerts or incidents based on their severity, category, source, or other attributes. You can also enable or disable the configurations as needed.

Reference:

Star Security Events

Create an Alert Starring Configuration

Create an Incident Starring Configuration

NEW QUESTION: 28

Which built-in dashboard would be the best option for an executive, if they were looking for the Mean Time to Resolution (MTTR) metric?

- A. Security Manager Dashboard
- B. Data Ingestion Dashboard
- C. Security Admin Dashboard
- D. Incident Management Dashboard

Answer: ([SHOW ANSWER](#))

The Incident Management Dashboard provides a high-level overview of the incident response process, including the Mean Time to Resolution (MTTR) metric. This metric measures the average time it takes to resolve an incident from the moment it is created to the moment it is closed. The dashboard also shows the number of incidents by status, severity, and assigned analyst, as well as the top alerts by category, source, and destination. The Incident Management Dashboard is designed for executives and managers who want to monitor the performance and efficiency of their security teams. Reference: [PCDRA Study Guide], page 18.

NEW QUESTION: 29

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?

- 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 ([LEAVE A REPLY](#))

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.

Reference:

Behavioral Threat Protection

Create a BTP Rule

DLL Protection

Create an IOC Rule
[Cytool]

NEW QUESTION: 30

When is the wss (WebSocket Secure) protocol used?

- A. when the Cortex XDR agent downloads new security content
- B. when the Cortex XDR agent uploads alert data
- C. when the Cortex XDR agent connects to WildFire to upload files for analysis
- D. when the Cortex XDR agent establishes a bidirectional communication channel

Answer: D ([LEAVE A REPLY](#))

The WSS (WebSocket Secure) protocol is an extension of the WebSocket protocol that provides a secure communication channel over the internet. It is used to establish a persistent, full-duplex communication channel between a client (in this case, the Cortex XDR agent) and a server (such as the Cortex XDR management console or other components). The Cortex XDR agent uses the WSS protocol to establish a secure and real-time bidirectional communication channel with the Cortex XDR management console or other components in the Palo Alto Networks security ecosystem. This communication channel allows the agent to send data, such as security events, alerts, and other relevant information, to the management console, and receive commands, policy updates, and responses in return. By using the WSS protocol, the Cortex XDR agent can maintain a persistent connection with the management console, which enables timely communication of security-related information and allows for efficient incident response and remediation actions. It's important to note that the other options mentioned in the question also involve communication between the Cortex XDR agent and various components, but they do not specifically mention the use of the WSS protocol. For example:

- A . The Cortex XDR agent downloading new security content typically utilizes protocols like HTTP or HTTPS.
- B . When the Cortex XDR agent uploads alert data, it may use protocols like HTTP or HTTPS to transmit the data securely.
- C . When the Cortex XDR agent connects to WildFire to upload files for analysis, it typically uses protocols like HTTP or HTTPS. Therefore, the correct answer is D, when the Cortex XDR agent establishes a bidirectional communication channel. Reference:

Device communication protocols - AWS IoT Core

WebSocket - Wikipedia

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) - Palo Alto Networks
[What are WebSockets? | Web Security Academy]

[Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification exam practice question and answer (Q&A) dump with detail explanation and reference available free, helpful to pass the Palo Alto Networks Certified Detection and Remediation Analyst PCDRA exam and earn Palo Alto Networks Certified Detection and Remediation Analyst PCDRA certification.]

NEW QUESTION: 31

Where would you view the WildFire report in an incident?

- A. next to relevant Key Artifacts in the incidents details page
- B. under Response --> Action Center
- C. under the gear icon --> Agent Audit Logs
- D. on the HUB page at apps.paloaltonetworks.com

Answer: A ([LEAVE A REPLY](#))

To view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. A key artifact is a piece of evidence that is associated with an alert or an incident, such as a file hash, a registry key, an IP address, a domain name, or a full path. If a key artifact is related to a WildFire analysis, you will see a WildFire icon next to it, indicating that there is a WildFire report available for that artifact. You can click on the WildFire icon to view the report, which will show you the detailed information about the artifact, such as the verdict, the behavior, the severity, the signatures, and the screenshots¹².

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

B . under Response --> Action Center: This is not the correct answer. The Action Center is a feature 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 does not show you the WildFire reports for the incidents, but it can help you to remediate the incidents by applying the appropriate actions³.

C . under the gear icon --> Agent Audit Logs: This is not the correct answer. The Agent Audit Logs are logs that show you the activities and events that occurred on the Cortex XDR agents, such as installation, upgrade, connection, policy update, or prevention. The Agent Audit Logs do not show you the WildFire reports for the incidents, but they can help you to troubleshoot the agent issues or verify the agent status⁴.

D . on the HUB page at apps.paloaltonetworks.com: This is not the correct answer. The HUB page is a web portal that allows you to access and manage your Palo Alto Networks applications, such as Cortex XDR, Cortex XSOAR, Prisma Cloud, or AutoFocus. The HUB page does not show you the WildFire reports for the incidents, but it can help you to navigate to the different applications or view the notifications and alerts⁵.

In conclusion, to view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. By viewing the WildFire report, you can gain more insights and context about the incident and the artifact.

Reference:

View Incident Details

View WildFire Reports

Action Center

Agent Audit Logs

HUB

Valid XDR-Analyst Dumps shared by Actual4test.com for Helping Passing XDR-Analyst Exam! Actual4test.com now offer the **newest XDR-Analyst exam dumps**, the Actual4test.com XDR-Analyst exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com XDR-Analyst dumps with Test Engine here:

https://www.actual4test.com/XDR-Analyst_examcollection.html (93 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

What is the standard installation disk space recommended to install a Broker VM?

- A.** 1GB disk space
- B.** 2GB disk space
- C.** 512GB disk space
- D.** 256GB disk space

Answer: D ([LEAVE A REPLY](#))

The Broker VM for Cortex XDR is a virtual machine that serves as the central communication hub for all Cortex XDR agents deployed in your organization. It enables agents to communicate with the Cortex XDR cloud service and allows you to manage and monitor the agents' activities from a centralized location. The system requirements for the Broker VM are as follows:

CPU: 4 cores

RAM: 8 GB

Disk space: 256 GB

Network: Internet access and connectivity to all Cortex XDR agents

The disk space requirement is based on the number of agents and the frequency of content updates. The Broker VM stores the content updates locally and distributes them to the agents.

The disk space also depends on the retention period of the content updates, which can be configured in the Broker VM settings. The default retention period is 30 days.

Reference:

Broker VM for Cortex XDR

PCDRA Study Guide

NEW QUESTION: 33

Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

- A.** a hierarchical database that stores settings for the operating system and for applications
- B.** a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"
- C.** a central system, available via the internet, for registering officially licensed versions of software to prove ownership
- D.** a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system

Answer: A ([LEAVE A REPLY](#))

The Windows Registry is a hierarchical database that stores settings for the operating system and for applications that run on Windows. The registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. The registry is organized into five main sections, called hives, each of which contains keys, subkeys, and values. The Cortex XDR agent uses the registry to store its configuration, status, and logs, as well as to monitor and control the endpoint's security features. The Cortex XDR agent also allows you to run scripts that can read, write, or delete registry keys and values on the endpoint. Reference:

Windows Registry - Wikipedia

Registry Operations

NEW QUESTION: 34

A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

- A. It is true positive.
- B. It is false positive.
- C. It is a false negative.
- D. It is true negative.

Answer: B ([LEAVE A REPLY](#))

A false positive is a situation where a file or activity is incorrectly identified as malicious by a security tool, when in fact it is benign or harmless. A false positive can cause unnecessary alerts, disruptions, or remediation actions, and reduce the confidence and efficiency of the security system. In this question, a file is identified as malware by the Local Analysis module, whereas WildFire verdict is Benign, assuming WildFire is accurate. This means that the Local Analysis module has made a mistake and flagged a legitimate file as malicious, while WildFire has correctly determined that the file is safe. Therefore, this is an example of a false positive. The Local Analysis module is a feature of the Cortex XDR agent that uses a static set of pattern-matching rules and a statistical model to determine if an unknown file is likely to be malware. The Local Analysis module can provide a fast and offline verdict for files that are not yet analyzed by WildFire, but it is not as accurate or comprehensive as WildFire, which uses dynamic analysis and machine learning to examine the behavior and characteristics of files in a sandbox environment. WildFire verdicts are considered more reliable and authoritative than Local Analysis verdicts, and can override them in case of a discrepancy. Therefore, if a file is identified as malware by the Local Analysis module, but as Benign by WildFire, the WildFire verdict should be trusted and the Local Analysis verdict should be disregarded.¹²³ Reference:

False positive (security) - Wikipedia

Local Analysis

WildFire Overview

NEW QUESTION: 35

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?

- A. Sensor Engine
- B. Causality Analysis Engine
- C. Log Stitching Engine
- D. Causality Chain Engine

Answer: ([SHOW ANSWER](#))

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.

Reference:

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

NEW QUESTION: 36

Which license is required when deploying Cortex XDR agent on Kubernetes Clusters as a DaemonSet?

- A. Cortex XDR Pro per TB
- B. Host Insights
- C. Cortex XDR Pro per Endpoint
- D. Cortex XDR Cloud per Host

Answer: D ([LEAVE A REPLY](#))

When deploying Cortex XDR agent on Kubernetes clusters as a DaemonSet, the license required is Cortex XDR Cloud per Host. This license allows you to protect and monitor your cloud workloads, such as Kubernetes clusters, containers, and serverless functions, using Cortex XDR. With Cortex XDR Cloud per Host license, you can deploy Cortex XDR agents as DaemonSets on your Kubernetes clusters, which ensures that every node in the cluster runs a copy of the agent. The Cortex XDR agent collects and sends data from the Kubernetes cluster, such as pod events, container logs, and network traffic, to the Cortex Data Lake for analysis and correlation. Cortex XDR can then detect and respond to threats across your cloud environment, and provide visibility and context into your cloud workloads. The Cortex XDR Cloud per Host license is based on the number of hosts that run the Cortex XDR agent, regardless of the number of containers or functions on each host. A host is defined as a virtual machine, a physical server, or a Kubernetes node that runs the Cortex XDR agent. You can read more about the Cortex XDR Cloud per Host license and how to deploy Cortex XDR agent on Kubernetes clusters [here1](#) and [here2](#).

Reference:

Cortex XDR Cloud per Host License

Deploy Cortex XDR Agent on Kubernetes Clusters as a DaemonSet

NEW QUESTION: 37

What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

- A. Automatically block the IP addresses involved in malicious traffic.
- B. Automatically kill the processes involved in malicious activity.
- C. Automatically terminate the threads involved in malicious activity.
- D. Automatically close the connections involved in malicious traffic.

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 38

What is the difference between presets and datasets in XQL?

- A. A dataset is a Cortex data lake data source only; presets are built-in data source.

- B. A dataset is a built-in or third-party source; presets group XDR data fields.
- C. A dataset is a database; presets is a field.
- D. A dataset is a third-party data source; presets are built-in data source.

Answer: ([SHOW ANSWER](#))

The difference between presets and datasets in XQL is that a dataset is a built-in or third-party data source, while a preset is a group of XDR data fields. A dataset is a collection of data that you can query and analyze using XQL. A dataset can be a Cortex data lake data source, such as endpoints, alerts, incidents, or network flows, or a third-party data source, such as AWS CloudTrail, Azure Activity Logs, or Google Cloud Audit Logs. A preset is a predefined set of XDR data fields that are relevant for a specific use case, such as process execution, file operations, or network activity. A preset can help you simplify and standardize your XQL queries by selecting the most important fields for your analysis. You can use presets with any Cortex data lake data source, but not with third-party data sources. Reference:

Datasets and Presets

XQL Language Reference

NEW QUESTION: 39

Phishing belongs to which of the following MITRE ATT&CK tactics?

- A. Initial Access, Persistence
- B. Persistence, Command and Control
- C. Reconnaissance, Persistence
- D. Reconnaissance, Initial Access

Answer: D ([LEAVE A REPLY](#))

Phishing is a technique that belongs to two MITRE ATT&CK tactics: Reconnaissance and Initial Access. Reconnaissance is the process of gathering information about a target before launching an attack. Phishing for information is a sub-technique of Reconnaissance that involves sending phishing messages to elicit sensitive information that can be used during targeting. Initial Access is the process of gaining a foothold in a network or system. Phishing is a sub-technique of Initial Access that involves sending phishing messages to execute malicious code on victim systems. Phishing can be used for both Reconnaissance and Initial Access depending on the objective and content of the phishing message. Reference:

Phishing, Technique T1566 - Enterprise | MITRE ATT&CK 1

Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK 2 Phishing for

information, Part 2: Tactics and techniques 3 PHISHING AND THE MITRE ATT&CK

FRAMEWORK - EnterpriseTalk 4 Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK 5

Valid XDR-Analyst Dumps shared by Actual4test.com for Helping Passing XDR-Analyst Exam! Actual4test.com now offer the **newest XDR-Analyst exam dumps**, the Actual4test.com XDR-Analyst exam **questions have been updated** and **answers have been corrected** get

the **newest** Actual4test.com XDR-Analyst dumps with Test Engine here:

https://www.actual4test.com/XDR-Analyst_examcollection.html (**93** Q&As Dumps, **30%OFF**

Special Discount: **Freepdfdumps**)