

PaloAltoNetworks.XDR-Analyst.v2026-06-24.q32

Exam Code:	XDR-Analyst
Exam Name:	Palo Alto Networks XDR Analyst
Certification Provider:	Palo Alto Networks
Free Question Number:	32
Version:	v2026-06-24
# of views:	113
# of Questions views:	320
https://www.exam-tests.com/XDR-Analyst-exam/PaloAltoNetworks.XDR-Analyst.v2026-06-24.q32.html	

NEW QUESTION: 1

What should you do to automatically convert leads into alerts after investigating a lead?

- A. Lead threats can't be prevented in the future because they already exist in the environment.
- B. Create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.
- C. Create BIOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.
- D. Build a search query using Query Builder or XQL using a list of IOCs.

Answer: (SHOW ANSWER)

To automatically convert leads into alerts after investigating a lead, you should create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting. IOC rules are used to detect known threats based on indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, etc. By creating IOC rules from the leads, you can prevent future occurrences of the same threats and generate alerts for them. Reference:

PCDRA Study Guide, page 25

Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2

Cortex XDR Documentation, section "Create IOC Rules"

NEW QUESTION: 2

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

Answer: D (LEAVE A REPLY)

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 Reference:

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]

NEW QUESTION: 3

Cortex XDR is deployed in the enterprise and you notice a cobalt strike attack via an ongoing supply chain compromise was prevented on 1 server. What steps can you take to ensure the same protection is extended to all your servers?

- A. Conduct a thorough Endpoint Malware scan.
- B. Enable DLL Protection on all servers but there might be some false positives.
- C. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.
- D. Create IOCs of the malicious files you have found to prevent their execution.

Answer: ([SHOW ANSWER](#))

The best step to ensure the same protection is extended to all your servers is to create indicators of compromise (IOCs) of the malicious files you have found to prevent their execution. IOCs are pieces of information that indicate a potential threat or compromise on an endpoint, such as file hashes, IP addresses, domain names, or registry keys. You can create IOCs in Cortex XDR to block or alert on any file or network activity that matches the IOCs. By creating IOCs of the malicious files involved in the cobalt strike attack, you can prevent them from running or spreading on any of your servers.

The other options are not the best steps for the following reasons:

A is not the best step because conducting a thorough Endpoint Malware scan may not detect or prevent the cobalt strike attack if the malicious files are obfuscated, encrypted, or hidden. Endpoint Malware scan is a feature of Cortex XDR that allows you to scan endpoints for known malware and quarantine any malicious files found. However, Endpoint Malware scan may not be effective against unknown or advanced threats that use evasion techniques to avoid detection.

B is not the best step because enabling DLL Protection on all servers may cause some false positives and disrupt legitimate applications. DLL Protection is a feature of Cortex XDR that allows you to block or alert on any DLL loading activity that matches certain criteria, such as unsigned DLLs, DLLs loaded from network locations, or DLLs loaded by specific processes. However, DLL Protection may also block or alert on benign DLL loading activity that is part of normal system or application operations, resulting in false positives and performance issues.

C is not the best step because enabling Behavioral Threat Protection (BTP) with cytool may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection. Behavioral Threat Protection is a feature of Cortex XDR that allows you to block or alert on any endpoint behavior that matches certain patterns, such as ransomware, credential theft, or lateral movement. Cytool is a command-line tool that allows you to configure and manage the Cortex XDR agent on the endpoint. However, Behavioral Threat Protection may not prevent the attack from spreading if the

malicious files are already on the endpoints or if the attack uses other methods to evade detection, such as encryption, obfuscation, or proxy servers.

Reference:

Create IOCs

Scan an Endpoint for Malware

DLL Protection

Behavioral Threat Protection

Cytool for Windows

NEW QUESTION: 4

What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

A. Netflow Collector

B. Syslog Collector

C. DB Collector

D. Pathfinder

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

The Broker VM is a virtual machine that acts as a data broker between third-party data sources and the Cortex Data Lake. It can ingest different types of data, such as syslog, netflow, database, and pathfinder. The Syslog Collector functionality of the Broker VM allows it to receive syslog messages from third-party devices, such as firewalls, routers, switches, and servers, and forward them to the Cortex Data Lake. The Syslog Collector can be configured to filter, parse, and enrich the syslog messages before sending them to the Cortex Data Lake. The Syslog Collector can also be used to ingest logs from third-party firewall vendors, such as Cisco, Fortinet, and Check Point, to the Cortex Data Lake. This enables Cortex XDR to analyze the firewall logs and provide visibility and threat detection across the network perimeter. Reference:

Cortex XDR Data Broker VM

Syslog Collector

Supported Third-Party Firewall Vendors

NEW QUESTION: 5

An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

A. DDL Security

B. Hot Patch Protection

C. Kernel Integrity Monitor (KIM)

D. Dylib Hijacking

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

The correct answer is D. Dylib Hijacking. Dylib Hijacking, also known as Dynamic Library Hijacking, is a technique used by attackers to load malicious dynamic libraries on macOS from an unsecure location. This technique takes advantage of the way macOS searches for dynamic libraries to load when an application is executed. To prevent such attacks, Palo Alto Networks offers the Dylib Hijacking prevention capability as part of their Cortex XDR platform. This capability is designed to detect and block attempts to load dynamic libraries from unauthorized or unsecure locations¹.

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

A . DDL Security: This is not the correct answer. DDL Security is not specifically designed to prevent dynamic library loading attacks on macOS. DDL Security is focused on protecting against DLL (Dynamic Link Library) hijacking on Windows systems².
B . Hot Patch Protection: Hot Patch Protection is not directly related to preventing dynamic library loading attacks. It is a security feature that protects against runtime patching or modification of code in memory, often used by advanced attackers to bypass security measures³. While Hot Patch Protection is a valuable security feature, it is not directly relevant to the scenario described.
C . Kernel Integrity Monitor (KIM): Kernel Integrity Monitor is also not the correct answer. KIM is a module in Cortex XDR that focuses on monitoring and protecting the integrity of the macOS kernel. It detects and prevents unauthorized modifications to critical kernel components⁴. While KIM plays an essential role in overall macOS security, it does not specifically address the prevention of dynamic library loading attacks.

In conclusion, Dylib Hijacking is the Cortex XDR module that specifically addresses the prevention of attackers loading dynamic libraries from unsecure locations on macOS. By leveraging this module, organizations can enhance their security posture and protect against this specific attack vector.

Reference:

Endpoint Protection Modules

DDL Security

Hot Patch Protection

Kernel Integrity Monitor

NEW QUESTION: 6

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: 7

When creating a BIOC rule, which XQL query can be used?

A. dataset = xdr_data
| filter event_sub_type = PROCESS_START and
action_process_image_name =~ ".*?\.(?:pdf|docx)\.exe"

B. dataset = xdr_data
| filter event_type = PROCESS and
event_sub_type = PROCESS_START and
action_process_image_name =~ ".*?\.(?:pdf|docx)\.exe"

C. dataset = xdr_data
| filter action_process_image_name =~ ".*?\.(?:pdf|docx)\.exe"
| fields action_process_image

D. dataset = xdr_data
| filter event_behavior = true
event_sub_type = PROCESS_START and
action_process_image_name =~ ".*?\.(?:pdf|docx)\.exe"

Answer: B (LEAVE A REPLY)

A BIOC rule is a custom detection rule that uses the Cortex Query Language (XQL) to define the behavior or actions that indicate a potential threat. A BIOC rule can use the xdr_data and cloud_audit_log datasets and presets for these datasets. A BIOC rule can also use the filter stage, alter stage, and functions without any aggregations in the XQL query. The query must return a single field named action_process_image, which is the process image name of the suspicious process. The query must also include the event_type and event_sub_type fields in the filter stage to specify the type and sub-type of the event that triggers the rule.

Option B is the correct answer because it meets all the requirements for a valid BIOC rule query. It uses the xdr_data dataset, the filter stage, the event_type and event_sub_type fields, and the action_process_image_name field with a regular expression to match any process image name that ends with .pdf.exe or .docx.exe, which are common indicators of malicious files.

Option A is incorrect because it does not include the event_type field in the filter stage, which is mandatory for a BIOC rule query.

Option C is incorrect because it does not include the event_type and event_sub_type fields in the filter stage, and it uses the fields stage, which is not supported for a BIOC rule query. It also returns the action_process_image field instead of the action_process_image_name field, which is the expected output for a BIOC rule query.

Option D is incorrect because it uses the event_behavior field, which is not supported for a BIOC rule query. It also does not include the event_type field in the filter stage, and it uses the event_sub_type field incorrectly. The event_sub_type field should be equal to PROCESS_START, not true.

Reference:

Working with BIOCs

Cortex Query Language (XQL) Reference

NEW QUESTION: 8

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

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: 9

What is the purpose of targeting software vendors in a supply-chain attack?

- A. to take advantage of a trusted software delivery method.
- B. to steal users' login credentials.
- C. to access source code.
- D. to report Zero-day vulnerabilities.

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

A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Software supply chain attacks inject malicious code into an application in order to infect all users of an app. The

purpose of targeting software vendors in a supply-chain attack is to take advantage of a trusted software delivery method, such as an update or a download, that can reach a large number of potential victims. By compromising a software vendor, an attacker can bypass the security measures of the downstream organizations and gain access to their systems, data, or networks. Reference: What Is a Supply Chain Attack? - Definition, Examples & More | Proofpoint US What Is a Supply Chain Attack? - CrowdStrike What Is a Supply Chain Attack? | Zscaler What Is a Supply Chain Attack? Definition, Examples & Prevention

NEW QUESTION: 10

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: B (LEAVE A REPLY)

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: 11

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: 12

What is the purpose of the Cortex Data Lake?

A. a local storage facility where your logs and alert data can be aggregated

B. a cloud-based storage facility where your firewall logs are stored

C. the interface between firewalls and the Cortex XDR agents

D. the workspace for your Cortex XDR agents to detonate potential malware files

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

The purpose of the Cortex Data Lake is to provide a cloud-based storage facility where your firewall logs are stored. Cortex Data Lake is a service that collects, transforms, and integrates your enterprise's security data to enable Palo Alto Networks solutions. It powers AI and machine learning, detection accuracy, and app and service innovation. Cortex Data Lake automatically collects, integrates, and normalizes data across your security infrastructure, including your next-generation firewalls, Prisma Access, and Cortex XDR. With unified data, you can run advanced AI and machine learning to radically simplify security operations with apps built on Cortex. Cortex Data Lake is available in multiple regions and supports data residency and privacy requirements.

Reference:

Cortex Data Lake - Palo Alto Networks

Cortex Data Lake - Palo Alto Networks

Cortex Data Lake, the technology behind Cortex XDR - Palo Alto Networks
CORTEX DATA LAKE - Palo Alto Networks
Sizing for Cortex Data Lake Storage - Palo Alto Networks

NEW QUESTION: 13

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

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: 14

Which module provides the best visibility to view vulnerabilities?

- A.** Live Terminal module
- B.** Device Control Violations module
- C.** Host Insights module
- D.** Forensics module

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

The Host Insights module provides the best visibility to view vulnerabilities on your endpoints. The Host Insights module is an add-on feature for Cortex XDR that combines vulnerability management, application and system visibility, and a Search and Destroy feature to help you identify and contain threats. The vulnerability management feature allows you to scan your Windows endpoints for known vulnerabilities and missing patches, and view the results in the Cortex XDR console. You can also filter and sort the vulnerabilities by severity, CVSS score, CVE ID, or patch availability. The Host Insights module helps you reduce your exposure to threats and improve your security posture. Reference:

Host Insights

Vulnerability Management

NEW QUESTION: 15

Which of the following paths will successfully activate Remediation Suggestions?

- 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: ([SHOW ANSWER](#))

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 to Incidents and select an incident that you want to remediate.

Click Causality View to see the graphical representation of the causality chain of the incident.

Click Actions and select Remediation 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.

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

Reference:

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.

NEW QUESTION: 16

Under which conditions is Local Analysis evoked to evaluate a file before the file is allowed to run?

- A. The endpoint is disconnected or the verdict from WildFire is of a type benign.
- B. The endpoint is disconnected or the verdict from WildFire is of a type unknown.
- C. The endpoint is disconnected or the verdict from WildFire is of a type malware.
- D. The endpoint is disconnected or the verdict from WildFire is of a type grayware.

Answer: B (LEAVE A REPLY)

Local Analysis is a feature of Cortex XDR that allows the agent to evaluate files locally on the endpoint, without sending them to WildFire for analysis. Local Analysis is evoked when the following conditions are met:

The endpoint is disconnected from the internet or the Cortex XDR management console, and therefore cannot communicate with WildFire.

The verdict from WildFire is of a type unknown, meaning that WildFire has not yet analyzed the file or has not reached a conclusive verdict.

Local Analysis uses machine learning models to assess the behavior and characteristics of the file and assign it a verdict of either benign, malware, or grayware. If the verdict is malware or grayware, the agent will block the file from running and report it to the Cortex XDR management console. If the verdict is benign, the agent will allow the file to run and report it to the Cortex XDR management console. Reference:

Local Analysis

WildFire File Verdicts

Valid XDR-Analyst Dumps shared by BraindumpsPass.com for Helping Passing XDR-Analyst Exam! BraindumpsPass.com now offer the **newest XDR-Analyst exam dumps**, the BraindumpsPass.com XDR-Analyst exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com XDR-Analyst dumps with Test Engine here: <https://www.braindumpspass.com/Palo-Alto-Networks/XDR-Analyst-practice-exam-dumps.html> (93 Q&As Dumps, **40%OFF**

Special Discount: Exam-Tests)

NEW QUESTION: 17

Which version of python is used in live terminal?

- A. Python 2 and 3 with standard Python libraries
- B. Python 2 and 3 with specific XDR Python libraries developed by Palo Alto Networks
- C. Python 3 with specific XDR Python libraries developed by Palo Alto Networks
- D. Python 3 with standard Python libraries

Answer: D (LEAVE A REPLY)

Live terminal uses Python 3 with standard Python libraries to run Python commands and scripts on the endpoint. Live terminal does not support Python 2 or any custom or external Python libraries. Live terminal uses the Python interpreter embedded in the Cortex XDR agent, which is based on Python 3.7.4. The standard Python libraries are the modules that are included with the Python installation and provide a wide range of functionalities, such as operating system interfaces, network programming, data processing, and more. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint, such as querying system information, modifying files or registry keys, or running other applications. Reference:

Run Python Commands and Scripts

Python Standard Library

NEW QUESTION: 18

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: 19

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

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

Answer: ([SHOW ANSWER](#))

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

Anti-Ransomware Protection
PCDRA Study Guide

NEW QUESTION: 20

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

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

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

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

The other statements are incorrect for the following reasons:

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

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

C is incorrect because the Cortex XDR Analytics module does need to interfere with the attack pattern to prevent the attack. The Cortex XDR Analytics module does not only detect the attack pattern, but also prevents it from succeeding by blocking the

malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on any other response mechanism or human intervention to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.

Reference:

Cortex XDR Analytics Module

Cortex XDR Analytics Module Detection and Prevention

NEW QUESTION: 21

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: ([SHOW ANSWER](#))

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: 22

Which of the following Live Terminal options are available for Android systems?

- A. Live Terminal is not supported.
- B. Stop an app.
- C. Run APK scripts.
- D. Run Android commands.

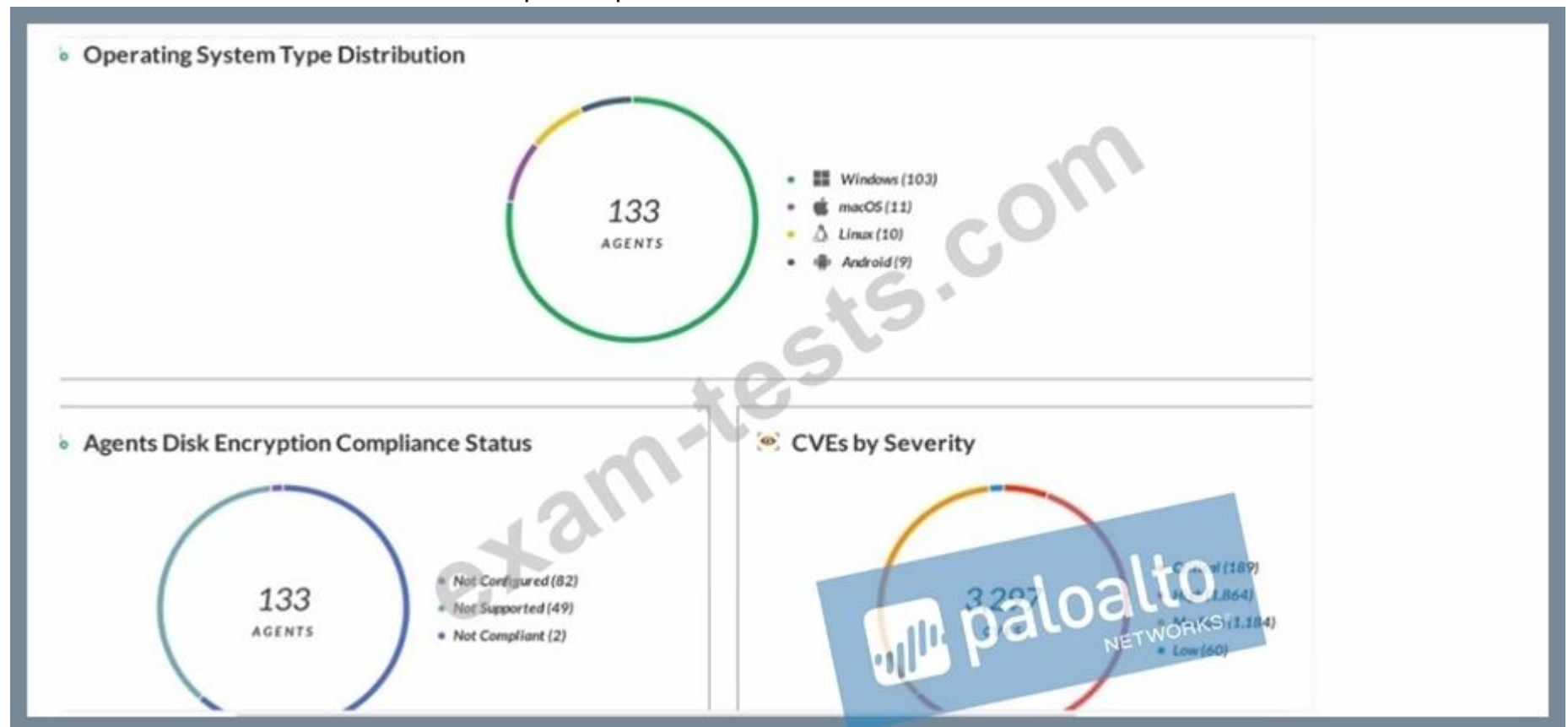
Answer: ([SHOW ANSWER](#))

Cortex XDR supports Live Terminal for Android systems, which allows you to remotely access and manage Android endpoints using a command-line interface. You can use Live Terminal to run Android commands, such as adb shell, adb logcat, adb install,

and adb uninstall. You can also use Live Terminal to view and modify files, directories, and permissions on the Android endpoints. Live Terminal for Android systems does not support stopping an app or running APK scripts. Reference: Cortex XDR documentation portal
Initiate a Live Terminal Session
Live Terminal Commands

NEW QUESTION: 23

Which statement is correct based on the report output below?



- 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: ([SHOW ANSWER](#))

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: 24

What does the following output tell us?

🔍 Top Hosts (Top 10 | Last 30 days)



HOST NAME

INCIDENTS BREAKDOWN

shpapy_win10

6 [5 1]

win7mickey

5 [5]

desktop-vjb9012

5 [4 1]

csp-enzo

4 [3 1]

win10-zb-thoma

3 [3]

pure_windows_10

3 [3]

lab1-8-csp

3 [3]

guru-pf

3 [3]

roneytestwindow

3 [3]

erikj-csp

3 [3]

- A. There is one low severity incident.
- B. Host shpapy_win10 had the most vulnerabilities.
- C. There is one informational severity alert.
- D. This is an actual output of the Top 10 hosts with the most malware.

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

The output shows the top 10 hosts with the most malware in the last 30 days, based on the Cortex XDR data. The output is sorted by the number of incidents, with the host with the most incidents at the top. The output also shows the number of alerts, the number of endpoints, and the percentage of endpoints for each host. The output is generated by using the ACC (Application Command

Center) feature of Cortex XDR, which provides a graphical representation of the network activity and threat landscape. The ACC allows you to view and analyze various widgets, such as the Top 10 hosts with the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more .

Reference:

Use the ACC to Analyze Network Activity

Top 10 Hosts with the Most Malware

NEW QUESTION: 25

When using the "File Search and Destroy" feature, which of the following search hash type is supported?

- A. SHA256 hash of the file
- B. AES256 hash of the file
- C. MD5 hash of the file
- D. SHA1 hash of the file

Answer: ([SHOW ANSWER](#))

The File Search and Destroy feature is a capability of Cortex XDR that allows you to search for and delete malicious or unwanted files across your endpoints. You can use this feature to quickly respond to incidents, remediate threats, and enforce compliance policies. To use the File Search and Destroy feature, you need to specify the file name and the file hash of the file you want to search for and delete. The file hash is a unique identifier of the file that is generated by a cryptographic hash function. The file hash ensures that you are targeting the exact file you want, and not a file with a similar name or a different version. The File Search and Destroy feature supports the SHA256 hash type, which is a secure hash algorithm that produces a 256-bit (32-byte) hash value. The SHA256 hash type is widely used for file integrity verification and digital signatures. The File Search and Destroy feature does not support other hash types, such as AES256, MD5, or SHA1, which are either encryption algorithms or less secure hash algorithms. Therefore, the correct answer is A, SHA256 hash of the file1234 Reference:

File Search and Destroy

What is a File Hash?

SHA-2 - Wikipedia

When using the "File Search and Destroy" feature, which of the following search hash type is supported?

NEW QUESTION: 26

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: 27

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

NEW QUESTION: 28

While working the alerts involved in a Cortex XDR incident, an analyst has found that every alert in this incident requires an exclusion. What will the Cortex XDR console automatically do to this incident if all alerts contained have exclusions?

- A. mark the incident as Unresolved
- B. create a BIOC rule excluding this behavior
- C. create an exception to prevent future false positives
- D. mark the incident as Resolved - False Positive

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

If all alerts contained in a Cortex XDR incident have exclusions, the Cortex XDR console will automatically mark the incident as Resolved - False Positive. This means that the incident was not a real threat, but a benign or legitimate activity that triggered an alert. By marking the incident as Resolved - False Positive, the Cortex XDR console removes the incident from the list of unresolved incidents and does not count it towards the incident statistics. This helps the analyst to focus on the true positive incidents that require further investigation and response¹.

An exclusion is a rule that hides an alert from the Cortex XDR console, based on certain criteria, such as the alert source, type, severity, or description. An exclusion does not change the security policy or prevent the alert from firing, it only suppresses the alert from the console. An exclusion is useful when the analyst wants to reduce the noise of false positive alerts that are not relevant or important².

An exception, on the other hand, is a rule that overrides the security policy and allows or blocks a process or file from running on an endpoint, based on certain attributes, such as the file hash, path, name, or signer. An exception is useful when the analyst wants to prevent false negative alerts that are caused by malicious or unwanted files or processes that are not detected by the security policy³.

A BIOC rule is a rule that creates an alert based on a custom XQL query that defines a specific behavior of interest or concern. A BIOC rule is useful when the analyst wants to detect and alert on anomalous or suspicious activities that are not covered by the default Cortex XDR rules⁴.

Reference:

Palo Alto Networks Cortex XDR Documentation, Resolve an Incident¹

Palo Alto Networks Cortex XDR Documentation, Alert Exclusions²

Palo Alto Networks Cortex XDR Documentation, Exceptions³

Palo Alto Networks Cortex XDR Documentation, BIOC Rules⁴

NEW QUESTION: 29

After scan, how does file quarantine function work on an endpoint?

- A.** Quarantine takes ownership of the files and folders and prevents execution through access control.
- B.** Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.
- C.** Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.
- D.** Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.

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

Quarantine is a feature of Cortex XDR that allows you to isolate a malicious file from its original location and prevent it from being executed. Quarantine works by moving the file to a protected folder on the endpoint and changing its permissions and attributes. Quarantine can be applied to files detected by periodic scans or by behavioral threat protection (BTP) rules. Quarantine is only supported for portable executable (PE) and dynamic link library (DLL) files. Quarantine does not affect the network connectivity or the communication of the endpoint with Cortex XDR. Reference:

Quarantine Malicious Files

Manage Quarantined Files

NEW QUESTION: 30

Where would you go to add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint?

- A.** Find the Malware profile attached to the endpoint, Under Portable Executable and DLL Examination add the hash to the allow list.
- B.** From the rules menu select new exception, fill out the criteria, choose the scope to apply it to, hit save.
- C.** Find the exceptions profile attached to the endpoint, under process exceptions select local analysis, paste the hash and save.

D. In the Action Center, choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it.

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

To add an exception to exclude a specific file hash from examination by the Malware profile for a Windows endpoint, you need to use the Action Center in Cortex XDR. The Action Center allows you to create and manage actions that apply to endpoints, such as adding files or processes to the allow list or block list, isolating or unisolating endpoints, or initiating live terminal sessions. To add a file hash to the allow list, you need to choose Allow list, select new action, select add to allow list, add your hash to the list, and apply it. This will prevent the Malware profile from scanning or blocking the file on the endpoints that match the scope of the action. Reference: Cortex XDR 3: Responding to Attacks¹, Action Center²

NEW QUESTION: 31

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

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

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

Malware Protection Profile

Endpoint Security Policy

Valid XDR-Analyst Dumps shared by BraindumpsPass.com for Helping Passing XDR-Analyst Exam! BraindumpsPass.com now offer the **newest XDR-Analyst exam dumps**, the BraindumpsPass.com XDR-Analyst exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com XDR-Analyst dumps with Test Engine here: <https://www.braindumpsPASS.com/Palo-Alto-Networks/XDR-Analyst-practice-exam-dumps.html> (93 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 32

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

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

Valid XDR-Analyst Dumps shared by BraindumpsPass.com for Helping Passing XDR-Analyst Exam! BraindumpsPass.com now offer the **newest XDR-Analyst exam dumps**, the BraindumpsPass.com XDR-Analyst exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com XDR-Analyst dumps with Test Engine here: <https://www.braindumpspass.com/Palo-Alto-Networks/XDR-Analyst-practice-exam-dumps.html> (**93** Q&As Dumps, **40%OFF**

Special Discount: Exam-Tests)