



"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks.com

Warning: Keep connected with our support team
for latest updates

Question: 1

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

Explanation:

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

Question: 2

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

Explanation:

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

Question: 3

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

Explanation:

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.

Question: 4

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

Explanation:

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 ...

Question: 5

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: D

Explanation:

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

Question: 6

What license would be required for ingesting external logs from various vendors?

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

Answer: C

Explanation:

To ingest external logs from various vendors, you need a Cortex XDR Pro per TB license. This license allows you to collect and analyze logs from Palo Alto Networks and third-party sources, such as firewalls, proxies, endpoints, cloud services, and more. You can use the Log Forwarding app to forward logs from the Logging Service to an external syslog receiver. The Cortex XDR Pro per Endpoint license only supports logs from Cortex XDR agents installed on endpoints. The Cortex XDR Vendor Agnostic Pro and Cortex XDR Cloud per Host licenses do not exist.

Reference: Features by Cortex XDR License Type

Log Forwarding App for Cortex XDR Analytics

SaaS Log Collection

Question: 7

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

Explanation:

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, Dyllib 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

Question: 8

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

Explanation:

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

Question: 9

Which Type of IOC can you define in Cortex XDR?

- A. destination port
- B. e-mail address
- C. full path
- D. App-ID

Answer: C

Explanation:

Cortex XDR allows you to define IOCs based on various criteria, such as file hashes, registry keys, IP addresses, domain names, and full paths. A full path IOC is a specific location of a file or folder on an endpoint, such as C:\Windows\System32\calc.exe. You can use full path IOCs to detect and respond to malicious files or folders that are located in known locations on your endpoints¹².

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

A. destination port: This is not the correct answer. Destination port is not a type of IOC that you can define in Cortex XDR. Destination port is a network attribute that indicates the port number to which a packet is sent.

Cortex XDR does not support defining IOCs based on destination ports, but you can use XQL queries to filter network events by destination ports³.

B. e-mail address: This is not the correct answer. E-mail address is not a type of IOC that you can define in Cortex XDR. E-mail address is an identifier that is used to send and receive e-mails. Cortex XDR does not support defining IOCs based on e-mail addresses, but you can use the Cortex XDR - IOC integration with Cortex XSOAR to ingest IOCs from various sources, including e-mail addresses⁴.

D. App-ID: This is not the correct answer. App-ID is not a type of IOC that you can define in Cortex XDR. App-ID is a feature of Palo Alto Networks firewalls that identifies and controls applications on the network. Cortex XDR does not support defining IOCs based on App-IDs, but you can use the Cortex XDR Analytics app to create custom rules that use App-IDs as part of the rule logic⁵.

In conclusion, full path is the type of IOC that you can define in Cortex XDR. By using full path IOCs, you can enhance your detection and response capabilities and protect your endpoints from malicious files or folders.

Reference:

Create an IOC Rule

XQL Reference Guide: Network Events Schema

Cortex XDR - IOC

Cortex XDR Analytics App

PCDRA: Which Type of IOC can define in Cortex XDR?

Question: 10

When viewing the incident directly, what is the "assigned to" field value of a new Incident that was just reported to Cortex?

- A. Pending
- B. It is blank

- C. Unassigned
- D. New

Answer: C

Explanation:

The "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This means that the incident has not been assigned to any analyst or group yet, and it is waiting for someone to take ownership of it. The "assigned to" field is one of the default fields that are displayed in the incident layout, and it can be used to filter and sort incidents in the incident list. The "assigned to" field can be changed manually by an analyst, or automatically by a playbook or a rule¹².

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

A . Pending: This is not the correct answer. Pending is not a valid value for the "assigned to" field. Pending is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"³.

B . It is blank: This is not the correct answer. The "assigned to" field is never blank for any incident. It always has a default value of "Unassigned" for new incidents, unless a playbook or a rule assigns it to a specific analyst or group¹².

D . New: This is not the correct answer. New is not a valid value for the "assigned to" field. New is a possible value for the "status" field, which indicates the current state of the incident. The status field can have values such as "New", "Active", "Done", "Closed", or "Pending"³.

In conclusion, the "assigned to" field value of a new incident that was just reported to Cortex is "Unassigned". This field can be used to manage the ownership and responsibility of incidents, and it can be changed manually or automatically.

Reference:

Cortex XDR Pro Admin Guide: Manage Incidents

Cortex XDR Pro Admin Guide: Assign Incidents

Cortex XDR Pro Admin Guide: Update Incident Status

Question: 11

In incident-related widgets, how would you filter the display to only show incidents that were "starred"?

- A. Create a custom XQL widget
- B. This is not currently supported
- C. Create a custom report and filter on starred incidents
- D. Click the star in the widget

Answer: D

Explanation:

To filter the display to only show incidents that were "starred", you need to click the star in the widget. This will apply a filter that shows only the incidents that contain a starred alert, which is an alert that matches a specific condition that you define in the incident starring configuration. You can use the incident starring feature to prioritize and focus on the most important or relevant incidents in your environment¹.

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

A . Create a custom XQL widget: This is not the correct answer. Creating a custom XQL widget is not necessary to filter the display to only show starred incidents. A custom XQL widget is a widget that you create by using the XQL

query language to define the data source and the visualization type. You can use custom XQL widgets to create your own dashboards or reports, but they are not required for filtering incidents by stars².

B . This is not currently supported: This is not the correct answer. Filtering the display to only show starred incidents is currently supported by Cortex XDR. You can use the star icon in the widget to apply this filter, or you can use the Filter Builder to create a custom filter based on the Starred field¹. C . Create a custom report and filter on starred incidents: This is not the correct answer. Creating a custom report and filtering on starred incidents is not the only way to filter the display to only show starred incidents. A custom report is a report that you create by using the Report Builder to define the data source, the layout, and the schedule. You can use custom reports to generate and share periodic reports on your Cortex XDR data, but they are not the only option for filtering incidents by stars³.

In conclusion, clicking the star in the widget is the simplest and easiest way to filter the display to

only show incidents that were "starred". By using this feature, you can quickly identify and focus on the most critical or relevant incidents in your environment.

Reference:

[Filter Incidents by Stars](#)

[Create a Custom XQL Widget](#)

[Create a Custom Report](#)

Question: 12

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

Explanation:

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

Question: 13

What does the following output tell us?

HOST NAME	INCIDENTS BREAKDOWN
shpapy_win10	6 [5 1]
win7mickey	5 [5]
desktop-vjb9012	5 [4 1]
csp-enzo	4 [3 1]
win10lab-thomas	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

Explanation:

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

the most malware, the Top 10 applications by bandwidth, the Top 10 threats by count, and more . Reference: Use the ACC to Analyze Network Activity

Top 10 Hosts with the Most Malware

Question: 14

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

Explanation:

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

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

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

C : Log Stitching Engine: This is not the correct answer. The Log Stitching Engine is not responsible for determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident. The Log Stitching Engine is the component that runs on the Cortex Data Lake, which is the cloud-based data storage and processing platform for Cortex XDR. The Log Stitching Engine normalizes and stitches together the data from different sources, such as firewalls, proxies, endpoints, and clouds. The Log Stitching Engine enables Cortex XDR to correlate and analyze data from multiple sources and provide a unified view of the network activity and threat landscape⁴.

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

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

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

Question: 15

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

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

Answer: B

Explanation:

The type of BIOC rule that is currently available in Cortex XDR is Discovery. A Discovery BIOC rule is a rule that detects suspicious or malicious behavior on endpoints based on the Cortex XDR data. A Discovery BIOC rule can use various event types, such as file, injection, load image, network, process, registry, or user, to define the criteria for the rule. A Discovery BIOC rule can also use operators, functions, and variables to create complex logic and conditions for the rule. A Discovery BIOC rule can generate alerts when the rule is triggered, and these alerts can be grouped into incidents for further investigation and response¹².

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

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

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

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

Reference:

Create a BIOC Rule
BIOC Rule Event Types
Threat Intelligence and Context

Malware Prevention

Question: 16

In Windows and macOS you need to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. What is one way to add an exception for the signer?

- A. In the Restrictions Profile, add the file name and path to the Executable Files allow list.
- B. Create a new rule exception and use the signer as the characteristic.
- C. Add the signer to the allow list in the malware profile.
- D. Add the signer to the allow list under the action center page.

Answer: C

Explanation:

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

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

A . In the Restrictions Profile, add the file name and path to the Executable Files allow list: This is not the correct answer. Adding the file name and path to the Executable Files allow list in the Restrictions Profile will not prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer. A Restrictions Profile is a profile that defines the settings and actions for restricting the execution of files or processes on the endpoints. A Restrictions Profile allows you to specify a list of executable files that you want to allow or block based on the file name and path. However, this method does not take into account the digital signer of the file, and it may not be effective if the file name or path changes².

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

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

In conclusion, to prevent the Cortex XDR Agent from blocking execution of a file based on the digital signer in Windows and macOS, one way to add an exception for the signer is to add the signer to the

allow list in the malware profile. By using this method, you can exclude the files that are signed by the trusted signer from the malware scanning and blocking.

Reference:

Add a New Malware Security Profile

Add a New Restrictions Security Profile
Create a Rule Exception
Action Center

Question: 17

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

Explanation:

To ensure that the same protection is extended to all your servers, you need to create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can use various operators, functions, and variables to define the criteria and the actions for the rules. By creating BTP rules that match the behaviors of the supply chain attack, you can prevent the attack from compromising your servers¹². Let's briefly discuss the other options to provide a comprehensive explanation:

B . Enable DLL Protection on all servers but there might be some false positives: This is not the correct answer. Enabling DLL Protection on all servers will not ensure that the same protection is extended to all your servers. DLL Protection is a feature of Cortex XDR that allows you to block the execution of unsigned or untrusted DLL files on your endpoints. DLL Protection can help to prevent some types of attacks that use malicious DLL files, but it may not be effective against the supply chain attack that used a Trojanized DLL file that was digitally signed by a trusted vendor. DLL Protection may also cause some false positives, as it may block some legitimate DLL files that are unsigned or untrusted³.

C . Create IOCs of the malicious files you have found to prevent their execution: This is not the correct answer. Creating IOCs of the malicious files you have found will not ensure that the same protection is extended to all your servers. IOCs are indicators of compromise that you can create to detect and respond to known threats on your endpoints, such as file hashes, registry keys, IP addresses, domain names, or full paths. IOCs can help to identify and block the malicious files that you have already discovered, but they may not be effective against the supply chain attack that used different variants of the malicious files with different hashes or names. IOCs may also become outdated, as the attackers may change or update their files to evade detection⁴.

D . Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading: This is not the correct answer. Enabling BTP with cytool will not ensure that the same protection is extended to all your servers. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can help to prevent the attack from spreading, but they need to be created and configured in the Cortex XDR app, not with cytool. Cytool is a command-line tool that allows you to perform various operations on the Cortex XDR agent, such as installing, uninstalling, upgrading, or troubleshooting. Cytool does not

have an option to enable or configure BTP rules.

In conclusion, to ensure that the same protection is extended to all your servers, you need to create BTP rules to recognize and prevent the activity. By using BTP rules, you can create custom and flexible prevention rules that match the behaviors of the supply chain attack.

Reference:

Behavioral Threat Protection

Create a BTP Rule

DLL Protection

Create an IOC Rule

[Cytool]

Question: 18

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

A Agent Auto Update Status



- A. There are a total of 689 Up To Date agents.
- B. Agent Auto Upgrade was enabled but not on all endpoints.
- C. Agent Auto Upgrade has not been enabled.
- D. There are more agents in Pending status than In Progress status.

Answer: B

Explanation:

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

Reference:

Cortex XDR Agent Auto Upgrade

PCDRA Study Guide

Question: 19

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

Explanation:

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

Question: 20

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

Explanation:

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

Question: 21

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

Explanation:

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

Question: 22

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: B

Explanation:

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

Question: 23

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

Explanation:

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

Question: 24

In the deployment of which Broker VM applet are you required to install a strong cipher SHA256based SSL certificate?

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

Answer: B

Explanation:

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

Question: 25

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

Explanation:

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.]

Question: 26

With a Cortex XDR Prevent license, which objects are considered to be sensors?

- A. Syslog servers
- B. Third-Party security devices
- C. Cortex XDR agents
- D. Palo Alto Networks Next-Generation Firewalls

Answer: C

Explanation:

The objects that are considered to be sensors with a Cortex XDR Prevent license are Cortex XDR agents and Palo Alto Networks Next-Generation Firewalls. These are the two sources of data that Cortex XDR can collect and analyze for threat detection and response. Cortex XDR agents are software components that run on endpoints, such as Windows, Linux, and Mac devices, and provide protection against malware, exploits, and fileless attacks. Cortex XDR agents also collect and send endpoint data, such as process activity, network traffic, registry changes, and user actions, to the Cortex Data Lake for analysis and correlation. Palo Alto Networks Next-Generation Firewalls are network security devices that provide visibility and control over network traffic, and enforce security policies based on applications, users, and content. Next-Generation Firewalls also collect and send network data, such as firewall logs, DNS logs, HTTP headers, and WildFire verdicts, to the Cortex Data Lake for analysis and correlation. By integrating data from both Cortex XDR agents and Next-Generation Firewalls, Cortex XDR can provide a comprehensive view of the attack surface and detect threats across the network and endpoint layers.

Reference:

- Cortex XDR Prevent License
- Cortex XDR Agent Features
- Next-Generation Firewall Features

Question: 27

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

Explanation:

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

Question: 28

What kind of the threat typically encrypts user files?

- A. ransomware
- B. SQL injection attacks
- C. Zero-day exploits
- D. supply-chain attacks

Answer: A

Explanation:

Ransomware is a type of malicious software, or malware, that encrypts user files and prevents them from accessing their data until they pay a ransom. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware attacks can cause costly disruptions, data loss, and reputational damage. 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 attack.

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](#)

Question: 29

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: A

Explanation:

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 file.

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?

Question: 30

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, which type of Broker VM setup can you use to facilitate the communication?

- A. Broker VM Pathfinder
- B. Local Agent Proxy
- C. Local Agent Installer and Content Caching
- D. Broker VM Syslog Collector

Answer: B

Explanation:

If you have an isolated network that is prevented from connecting to the Cortex Data Lake, you can use the Local Agent Proxy setup to facilitate the communication. The Local Agent Proxy is a type of Broker VM that acts as a proxy server for the Cortex XDR agents that are deployed on the isolated network. The Local Agent Proxy enables the Cortex XDR agents to communicate securely with the Cortex Data Lake and the Cortex XDR management console over the internet, without requiring direct access to the internet from the isolated network. The Local Agent Proxy also allows the Cortex XDR agents to download installation packages and content updates from the Cortex XDR management console. To use the Local Agent Proxy setup, you need to deploy a Broker VM on the isolated network and configure it as a Local Agent Proxy. You also need to deploy another Broker VM on a network that has internet access and configure it as a Remote Agent Proxy. The Remote Agent Proxy acts as a relay between the Local Agent Proxy and the Cortex Data Lake. You also need to install a strong cipher SHA256-based SSL certificate on both the Local Agent Proxy and the Remote Agent Proxy to ensure secure communication. You can read more about the Local Agent Proxy setup and how to configure it [here1](#) and [here2](#). Reference:

Local Agent Proxy

Configure the Local Agent Proxy Setup

Question: 31

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

Explanation:

Ransomware is a type of malicious software, or malware, that encrypts certain files or data on the victim's system or network and prevents them from accessing their data until they pay a ransom. This is by far the most common tactic used by ransomware to shut down a victim's operation, as it can cause costly disruptions, data loss, and

reputational damage. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks.

Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again. Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack¹²³⁴ 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]

Question: 32

Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques.

- A. Exfiltration, Command and Control, Collection
- B. Exfiltration, Command and Control, Privilege Escalation
- C. Exfiltration, Command and Control, Impact
- D. Exfiltration, Command and Control, Lateral Movement

Answer: D

Explanation:

Cortex XDR Analytics is a feature of Cortex XDR that leverages machine learning and behavioral analytics to detect and alert on malicious activity across the network and endpoint layers. Cortex XDR Analytics can alert when detecting activity matching the following MITRE ATT&CKTM techniques: Exfiltration, Command and Control, Lateral Movement, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, and Collection. However, among the options given in the question, the correct answer is D, Exfiltration, Command and Control, Lateral Movement. These are three of the most critical techniques that indicate an advanced and persistent threat (APT) in the environment. Exfiltration refers to the technique of transferring data or information from the compromised system or network to an external location controlled by the adversary. Command and Control refers to the technique of communicating with the compromised system or network to provide instructions, receive data, or update malware. Lateral Movement refers to the technique of moving from one system or network to another within the same environment, usually to gain access to more resources or data. Cortex XDR Analytics can alert on these techniques by analyzing various data sources, such as network traffic, firewall logs, endpoint events, and threat intelligence, and applying behavioral models, anomaly detection, and correlation rules. Cortex XDR Analytics can also map the alerts to the corresponding MITRE ATT&CKTM techniques and provide additional context and visibility into the attack chain¹²³⁴ Reference:

Cortex XDR Analytics MITRE ATT&CKTM

Cortex XDR Analytics MITRE ATT&CKTM Techniques

Cortex XDR Analytics Alert Categories

Question: 33

When selecting multiple Incidents at a time, what options are available from the menu when a user right-clicks the incidents? (Choose two.)

- A. Assign incidents to an analyst in bulk.
- B. Change the status of multiple incidents.
- C. Investigate several Incidents at once.
- D. Delete the selected Incidents.

Answer: A, B

Explanation:

When selecting multiple incidents at a time, the options that are available from the menu when a user right-clicks the incidents are: Assign incidents to an analyst in bulk and Change the status of multiple incidents. These options allow the user to perform bulk actions on the selected incidents, such as assigning them to a specific analyst or changing their status to open, in progress, resolved, or closed. These options can help the user to manage and prioritize the incidents more efficiently and effectively. To use these options, the user needs to select the incidents from the incident table, rightclick on them, and choose the desired option from the menu. The user can also use keyboard shortcuts to perform these actions, such as Ctrl+A to select all incidents, Ctrl+Shift+A to assign incidents to an analyst, and Ctrl+Shift+S to change the status of incidents¹²

Reference:

Assign Incidents to an Analyst in Bulk
Change the Status of Multiple Incidents

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

Explanation:

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 disregarded¹²³

Reference:

False positive (security) - Wikipedia

Local Analysis

WildFire Overview

Question: 35

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: B

Explanation:

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

Question: 36

Which statement is true for Application Exploits and Kernel Exploits?

- A. The ultimate goal of any exploit is to reach the application.
- B. Kernel exploits are easier to prevent than application exploits.
- C. The ultimate goal of any exploit is to reach the kernel.
- D. Application exploits leverage kernel vulnerability.

Answer: C

Explanation:

The ultimate goal of any exploit is to reach the kernel, which is the core component of the operating system that has the highest level of privileges and access to the hardware resources. Application exploits are attacks that target vulnerabilities in specific applications, such as web browsers, email clients, or office suites. Kernel exploits are attacks that target vulnerabilities in the kernel itself, such as memory corruption, privilege escalation, or code execution. Kernel exploits are more difficult to prevent and detect than

application exploits, because they can bypass security mechanisms and hide their presence from the user and the system. Reference:

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8
Palo Alto Networks Cortex XDR Documentation, Exploit Protection Overview

Question: 37

To create a BIOC rule with XQL query you must at a minimum filter on which field in order for it to be a valid BIOC rule?

- A. causality_chain
- B. endpoint_name
- C. threat_event
- D. event_type

Answer: D

Explanation:

To create a BIOC rule with XQL query, you must at a minimum filter on the event_type field in order for it to be a valid BIOC rule. The event_type field indicates the type of event that triggered the alert, such as PROCESS, FILE, REGISTRY, NETWORK, or USER_ACCOUNT. Filtering on this field helps you narrow down the scope of your query and focus on the relevant events for your use case. Other fields, such as causality_chain, endpoint_name, threat_event, are optional and can be used to further refine your query or display additional information in the alert. Reference:

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, BIOC Rule Query Syntax

Question: 38

Which of the following is an example of a successful exploit?

- A. connecting unknown media to an endpoint that copied malware due to Autorun.
- B. a user executing code which takes advantage of a vulnerability on a local service.
- C. identifying vulnerable services on a server.
- D. executing a process executable for well-known and signed software.

Answer: B

Explanation:

A successful exploit is a piece of software or code that takes advantage of a vulnerability and executes malicious actions on the target system. A vulnerability is a weakness or flaw in a software or hardware component that can be exploited by an attacker. A successful exploit is one that achieves its intended goal, such as gaining unauthorized access, executing arbitrary code, escalating privileges, or compromising data.

In the given options, only B is an example of a successful exploit, because it involves a user executing

code that exploits a vulnerability on a local service, such as a web server, a database, or a network protocol. This could allow the attacker to gain control over the service, access sensitive information, or perform other malicious actions.

Option A is not a successful exploit, because it involves connecting unknown media to an endpoint that copied malware due to Autorun. Autorun is a feature that automatically runs a program or script when a removable media, such as a USB drive, is inserted into a computer. This feature can be abused by malware authors to spread their malicious code, but it is not an exploit in itself. The malware still needs to exploit a vulnerability on the endpoint to execute its payload and cause damage.

Option C is not a successful exploit, because it involves identifying vulnerable services on a server. This is a step in the reconnaissance phase of an attack, where the attacker scans the target system for potential vulnerabilities that can be exploited. However, this does not mean that the attacker has successfully exploited any of the vulnerabilities, or that the vulnerabilities are even exploitable. Option D is not a successful exploit, because it involves executing a process executable for well-known and signed software. This is a legitimate action that does not exploit any vulnerability or cause any harm. Well-known and signed software are programs that are widely used and trusted, and have a digital signature that verifies their authenticity and integrity. Executing such software does not pose a security risk, unless the software itself is malicious or compromised.

Reference:

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8

What Is an Exploit? Definition, Types, and Prevention

Measures(<https://heimdalsecurity.com/blog/what-is-an-exploit/>)

Exploit Definition & Meaning - Merriam-Webster(<https://www.merriam-webster.com/dictionary/exploit>)

Question: 39

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

- A. Only alerts with the same host are grouped together into one Incident in a given time frame.
- B. Alerts that occur within a three-hour time frame are grouped together into one Incident.
- C. Alerts with same causality chains that occur within a given time frame are grouped together into an Incident.
- D. Every alert creates a new Incident.

Answer: C

Explanation:

The correct relation of alerts to incidents is that alerts with same causality chains that occur within a given time frame are grouped together into an incident. A causality chain is a sequence of events that are related to the same malicious activity, such as a malware infection, a lateral movement, or a data exfiltration. Cortex XDR uses a set of rules that take into account different attributes of the alerts, such as the alert source, type, and time period, to determine if they belong to the same causality chain. By grouping related alerts into incidents, Cortex XDR reduces the number of individual events to review and provides a complete picture of the attack with rich investigative details¹.

Option A is incorrect, because alerts with the same host are not necessarily grouped together into one incident in a given time frame. Alerts with the same host may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a malware infection and a network anomaly, these alerts may not be grouped into the same incident, unless they are part of the same attack. Option B is incorrect, because alerts that occur within a three hour time frame are not always grouped together into one incident. The time frame is not the only criterion for grouping alerts into incidents. Alerts that occur within a three hour time frame may belong to different causality chains, or may be unrelated to any malicious activity. For example, if a host has a file download and a registry modification within a three hour time frame, these alerts may not be grouped into the same incident, unless they are part of the same attack.

Option D is incorrect, because every alert does not create a new incident. Creating a new incident for every alert would result in alert fatigue and inefficient investigations. Cortex XDR aims to reduce the number of incidents by grouping related alerts into one incident, based on their causality chains and other attributes.

Reference:

Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 9 Palo Alto Networks Cortex XDR Documentation, Incident Management Overview2

Cortex XDR: Stop Breaches with AI-Powered Cybersecurity1

Question: 40

Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

- A. Hash Verdict Determination
- B. Behavioral Threat Protection
- C. Restriction Policy
- D. Child Process Protection

Answer: A

Explanation:

The first protection module that is checked in the Cortex XDR Windows agent malware protection flow is the Hash Verdict Determination. This module compares the hash of the executable file that is about to run on the endpoint with a list of known malicious hashes stored in the Cortex XDR cloud. If the hash matches a malicious hash, the agent blocks the execution and generates an alert. If the hash does not match a malicious hash, the agent proceeds to the next protection module, which is the Restriction Policy1.

The Hash Verdict Determination module is the first line of defense against malware, as it can quickly and efficiently prevent known threats from running on the endpoint. However, this module cannot protect against unknown or zero-day threats, which have no known hash signature. Therefore, the Cortex XDR agent relies on other protection modules, such as Behavioral Threat Protection, Child Process Protection, and Exploit Protection, to detect and block malicious behaviors and exploits that may occur during the execution of the file1.

Reference:

Palo Alto Networks Cortex XDR Documentation, File Analysis and Protection Flow

Question: 41

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

Explanation:

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

Question: 42

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: D

Explanation:

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]

Question: 43

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

Explanation:

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](#)

Question: 44

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

Explanation:

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](#)

Security Profiles

[Create an Agent Exception Profile](#)

[Create a Global Exception Profile](#)

Question: 45

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

Explanation:

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

Endpoint Security Policy

Question: 46

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

Explanation:

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

Question: 47

Which of the following is NOT a precanned script provided by Palo Alto Networks?

- A. delete_file
- B. quarantine_file
- C. process_kill_name
- D. list_directories

Answer: D

Explanation:

Palo Alto Networks provides a set of precanned scripts that you can use to perform various actions on your endpoints, such as deleting files, killing processes, or quarantining malware. The precanned scripts are written in Python and are available in the Agent Script Library in the Cortex XDR console. You can use the precanned scripts as they are, or you can customize them to suit your needs. The precanned scripts are:

`delete_file`: Deletes a specific file from a local or removable drive.

`quarantine_file`: Moves a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.

`process_kill_name`: Kills a process by its name on the endpoint.

`process_kill_pid`: Kills a process by its process ID (PID) on the endpoint.

`process_kill_tree`: Kills a process and all its child processes by its name on the endpoint. `process_kill_tree_pid`: Kills a process and all its child processes by its PID on the endpoint. `process_list`: Lists all the processes running on the endpoint, along with their names, PIDs, and command lines.

`process_list_tree`: Lists all the processes running on the endpoint, along with their names, PIDs, command lines, and parent processes.

`process_start`: Starts a process on the endpoint by its name or path.

`registry_delete_key`: Deletes a registry key and all its subkeys and values from the Windows registry.

`registry_delete_value`: Deletes a registry value from the Windows registry.

`registry_list_key`: Lists all the subkeys and values under a registry key in the Windows registry. `registry_list_value`:

Lists the value and data of a registry value in the Windows registry. `registry_set_value`: Sets the value and data of a registry value in the Windows registry.

The script `list_directories` is not a precanned script provided by Palo Alto Networks. It is a custom script that you can write yourself using Python commands.

Reference:

Run Scripts on an Endpoint

Agent Script Library Precanned Scripts

Question: 48

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: B

Explanation:

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

Question: 49

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

Explanation:

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

Question: 50

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

Explanation:

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

Question: 51

As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?

- A. Enable DLL Protection on all endpoints but there might be some false positives.
- B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- C. No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.
- D. No step is required because the malicious document is already stopped.

Answer: B

Explanation:

The correct answer is B, create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP rules are a powerful feature of Cortex XDR that allow you to define custom rules to detect and block malicious behaviors on endpoints. You can use BTP rules to create indicators of compromise (IOCs) based on file attributes, registry keys, processes, network connections, and other criteria. By creating BTP rules, you can prevent the same malicious Word document from being opened by other users in your organization, even if the document has a different name or hash value. BTP rules are updated through content updates and can be managed from the Cortex XDR console. The other options are incorrect for the following reasons:

A is incorrect because enabling DLL Protection on all endpoints is not a specific or effective way to prevent the malicious Word document. DLL Protection is a feature of Cortex XDR that prevents the loading of unsigned or untrusted DLLs by protected processes. However, this feature does not apply to Word documents or macros, and may cause false positives or compatibility issues with legitimate applications.

C is incorrect because relying on Cortex to share IOCs with the Cyber Threat Alliance members is not a proactive or sufficient way to prevent the malicious Word document. The Cyber Threat Alliance is a group of cybersecurity vendors that share threat intelligence and best practices to improve their products and services. However, not all vendors are members of the alliance, and not all IOCs are shared or updated in a timely manner. Therefore, you cannot assume that other users in your organization are protected by the same IOCs as Cortex XDR.

D is incorrect because doing nothing is not a responsible or secure way to prevent the malicious Word document. Even though Cortex XDR agent prevented the attempt to open the document on one endpoint, it does not mean that the document is no longer a threat. The document may still be circulating in your network or email system, and may be opened by other users who have different agent profiles or policies. Therefore, you should take steps to identify and block the document across your organization.

Reference:

Cortex XDR Agent Administrator Guide: Behavioral Threat Protection

Cortex XDR Agent Administrator Guide: DLL Protection

Palo Alto Networks: Cyber Threat Alliance

Question: 52

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

Explanation:

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

Question: 53

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: B

Explanation:

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

Question: 54

When creating a scheduled report which is not an option?

- A. Run weekly on a certain day and time.
- B. Run quarterly on a certain day and time.
- C. Run monthly on a certain day and time.
- D. Run daily at a certain time (selectable hours and minutes).

Answer: B

Explanation:

When creating a scheduled report in Cortex XDR, the option to run quarterly on a certain day and

time is not available. You can only schedule reports to run daily, weekly, or monthly. You can also specify the start and end dates, the time zone, and the recipients of the report. Scheduled reports are useful for generating regular reports on the security events, incidents, alerts, or endpoints in your network. You can create scheduled reports from the Reports page in the Cortex XDR console, or from the Query Center by saving a query as a report. Reference: Run or Schedule Reports Create a Scheduled Report

Question: 55

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

Explanation:

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

Question: 56

What is the function of WildFire for Cortex XDR?

- A. WildFire runs in the cloud and analyses alert data from the XDR agent to check for behavioural threats.
- B. WildFire is the engine that runs on the local agent and determines whether behavioural threats are occurring on the endpoint.
- C. WildFire accepts and analyses a sample to provide a verdict.
- D. WildFire runs entirely on the agent to quickly analyse samples and provide a verdict.

Answer: C

Explanation:

WildFire is a cloud-based service that accepts and analyses samples from various sources, including Cortex XDR, to provide a verdict of malware, benign, or grayware. WildFire also generates detailed analysis reports that show the behaviour and characteristics of the samples. Cortex XDR uses WildFire verdicts and reports to enhance its detection and prevention capabilities, as well as to provide more visibility and context into the threats.

Reference:

WildFire Analysis Concepts

WildFire Overview

Question: 57

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: C

Explanation:

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

Question: 58

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

Explanation:

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

Question: 59

Which statement best describes how Behavioral Threat Protection (BTP) works?

- A. BTP injects into known vulnerable processes to detect malicious activity.
- B. BTP runs on the Cortex XDR and distributes behavioral signatures to all agents.
- C. BTP matches EDR data with rules provided by Cortex XDR.
- D. BTP uses machine Learning to recognize malicious activity even if it is not known.

Answer: D

Explanation:

The statement that best describes how Behavioral Threat Protection (BTP) works is D, BTP uses machine learning to recognize malicious activity even if it is not known. BTP is a feature of Cortex XDR that allows you to define custom rules to detect and block malicious behaviors on endpoints. BTP uses machine learning to profile behavior and detect anomalies indicative of attack. BTP can recognize malicious activity based on file attributes, registry keys, processes, network connections, and other criteria, even if the activity is not associated with any known malware or threat. BTP rules are updated through content updates and can be managed from the Cortex XDR console.

The other statements are incorrect for the following reasons:

A is incorrect because BTP does not inject into known vulnerable processes to detect malicious activity. BTP does not rely on process injection, which is a technique used by some malware to hide or execute code within another process. BTP monitors the behavior of all processes on the endpoint, regardless of their vulnerability status, and compares them with the BTP rules.

B is incorrect because BTP does not run on the Cortex XDR and distribute behavioral signatures to all agents. BTP runs on the Cortex XDR agent, which is installed on the endpoint, and analyzes the endpoint data locally. BTP does not use behavioral signatures, which are predefined patterns of malicious behavior, but rather uses machine learning to identify anomalies and deviations from normal behavior.

C is incorrect because BTP does not match EDR data with rules provided by Cortex XDR. BTP is part of the EDR (Endpoint Detection and Response) capabilities of Cortex XDR, and uses the EDR data collected by the Cortex XDR agent to perform behavioral analysis. BTP does not match the EDR data with rules provided by Cortex XDR, but rather applies the BTP rules defined by the Cortex XDR administrator or the Palo Alto Networks threat research team.

Reference:

Cortex XDR Agent Administrator Guide: Behavioral Threat Protection
Cortex XDR: Stop Breaches with AI-Powered Cybersecurity

Question: 60

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

Explanation:

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

Question: 61

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

- A. The agent technical support file.
- B. The prevention archive from the alert.
- C. The distribution id of the agent.
- D. A list of all the current exceptions applied to the agent.
- E. The unique agent id.

Answer: A, B

Explanation:

When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:

The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself. The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself. The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:

The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.

A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.

The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The

unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.

Reference:

Generate and Download the Agent Technical Support File

Generate and Download the Prevention Archive

Cortex XDR Agent Administrator Guide: Agent Distribution ID

Cortex XDR Agent Administrator Guide: Exception Security Profiles

[Cortex XDR Agent Administrator Guide: Unique Agent ID]

Question: 62

What types of actions you can execute with live terminal session?

- A. Manage Network configurations, Quarantine Files, Run PowerShell scripts
- B. Manage Processes, Manage Files, Run Operating System Commands, Run Ruby Commands and Scripts
- C. Apply patches, Reboot System, send notification for end user, Run Python Commands and Scripts
- D. Manage Processes, Manage Files, Run Operating System Commands, Run Python Commands and Scripts

Answer: D

Explanation:

Live terminal session is a feature of Cortex XDR that allows you to remotely access and control endpoints from the Cortex XDR console. With live terminal session, you can execute various actions on the endpoints, such as:

Manage Processes: You can view, start, or kill processes on the endpoint, and monitor their CPU and memory usage.

Manage Files: You can view, create, delete, or move files and folders on the endpoint, and upload or download files to or from the endpoint.

Run Operating System Commands: You can run commands on the endpoint using the native command-line interface of the operating system, such as cmd.exe for Windows, bash for Linux, or zsh for macOS.

Run Python Commands and Scripts: You can run Python commands and scripts on the endpoint using the Python interpreter embedded in the Cortex XDR agent. You can use the Python commands and scripts to perform advanced tasks or automation on the endpoint.

Reference:

Initiate a Live Terminal Session

Manage Processes

Manage Files

Run Operating System Commands

Run Python Commands and Scripts

Question: 63

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

Explanation:

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

Question: 64

What kind of malware uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim?

- A. Ransomware
- B. Worm
- C. Keylogger
- D. Rootkit

Answer: A

Explanation:

The kind of malware that uses encryption, data theft, denial of service, and possibly harassment to take advantage of a victim is ransomware. Ransomware is a type of malware that encrypts the victim's files or blocks access to their system, and then demands a ransom for the decryption key or the restoration of access. Ransomware can also threaten to expose or delete the victim's data if the ransom is not paid. Ransomware can cause significant damage and disruption to individuals, businesses, and organizations, and can be difficult to remove or recover from. Some examples of ransomware are CryptoLocker, WannaCry, Ryuk, and REvil.

Reference:

12 Types of Malware + Examples That You Should Know - CrowdStrike [What is Malware? Malware Definition, Types and Protection](#) 12+ Types of Malware Explained with Examples (Complete List)

Question: 65

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

Explanation:

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

Question: 66

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

Explanation:

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

Question: 67

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: D

Explanation:

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

Question: 68

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: B

Explanation:

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

Question: 69

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: B

Explanation:

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: PCDDRA Study Guide, page 25
Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2
Cortex XDR Documentation, section "Create IOC Rules"

Question: 70

Which type of IOC can you define in Cortex XDR?

- A. Destination IP Address
- B. Source IP Address
- C. Source port
- D. Destination IP Address: Destination

Answer: A

Explanation:

Cortex XDR allows you to define IOC rules based on various types of indicators of compromise (IOC) that you can use to detect and respond to threats in your network. One of the types of IOC that you can define in Cortex XDR is destination IP address, which is the IP address of the remote host that a local endpoint is communicating with. You can use this type of IOC to identify malicious network activity, such as connections to command and control servers, phishing sites, or malware distribution hosts. You can also specify the direction of the network traffic (inbound or outbound) and the protocol (TCP or UDP) for the destination IP address IOC. Reference: Cortex XDR documentation portal

Is there a possibility to create an IOC list to employ it in a query?

Cortex XDR Datasheet

Question: 71

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: D

Explanation:

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

Question: 72

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

Explanation:

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

Question: 73

In the Cortex XDR console, from which two pages are you able to manually perform the agent upgrade action? (Choose two.)

- A. Asset Management
- B. Agent Installations
- C. Action Center
- D. Endpoint Administration

Answer: A, D

Explanation:

To manually upgrade the Cortex XDR agents, you can use the Asset Management page or the Endpoint Administration page in the Cortex XDR console. On the Asset Management page, you can select one or more endpoints and click Actions > Upgrade Agent. On the Endpoint Administration page, you can select one or more agent versions and click Upgrade. You can also schedule automatic agent upgrades using the Agent Installations page. Reference: Asset Management Endpoint Administration Agent Installations

Question: 74

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

Explanation:

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

Question: 75

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

Explanation:

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

Question: 76

Which Exploit Prevention Module (EPM) provides better entropy for randomization of memory locations?

- A. Memory Limit Heap spray check
- B. UASLR
- C. JIT Mitigation
- D. DLL Security

Answer: B

Explanation:

UASLR stands for User Address Space Layout Randomization, which is a feature of Exploit Prevention Module (EPM) that provides better entropy for randomization of memory locations. UASLR adds entropy to the base address of the executable image and the heap, making it harder for attackers to predict the memory layout of a process. UASLR is enabled by default for all processes, but can be disabled or customized for specific applications using the EPM policy settings. Reference:

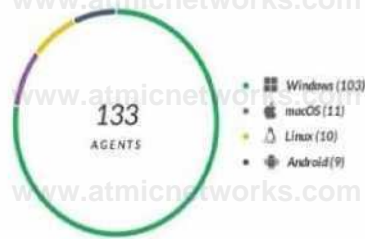
Exploit Prevention Module (EPM) entropy randomization memory locations

Exploit protection reference

Question: 77

Which statement is correct based on the report output below?

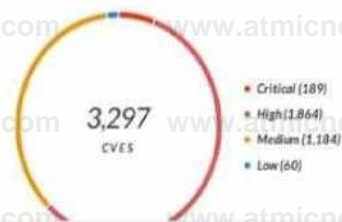
a Operating System Type Distribution



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

Explanation:

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

Question: 78

What contains a logical schema in an XQL query?

- A. Bin
- B. Array expand
- C. Field
- D. Dataset

Answer: C

Explanation:

A logical schema in an XQL query is a field, which is a named attribute of a dataset. A field can have a data type, such as string, integer, boolean, or array. A field can also have a modifier, such as bin or expand, that transforms the field value in the query output. A field can be used in the select, where, group by, order by, or having clauses of an XQL query. Reference:

XQL Syntax

XQL Data Types

XQL Field Modifiers

Question: 79

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

Explanation:

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

Question: 80

In Cortex XDR management console scheduled reports can be forwarded to which of the following applications/services?

- A. Salesforce
- B. Jira
- C. Service Now
- D. Slack

Answer: D

Explanation:

Cortex XDR allows you to schedule reports and forward them to Slack, a cloud-based collaboration platform. You can configure the Slack channel, frequency, and recipients of the scheduled reports. You can also view the report history and status in the Cortex XDR management console. Reference: Scheduled Queries: This document explains how to create, edit, and manage scheduled queries and reports in Cortex XDR.

Forward Scheduled Reports to Slack: This document provides the steps to configure Slack integration and forward scheduled reports to a Slack channel.

Question: 81

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

Explanation:

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

Question: 82

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

Explanation:

A common sequence of cyber-attack tactics is based on the Cyber Kill Chain model, which describes the stages of a cyber intrusion from the perspective of the attacker. The Cyber Kill Chain model consists of seven phases:

reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. These phases are briefly explained below: Reconnaissance: The attacker gathers information about the target, such as its network, systems, vulnerabilities, employees, and business operations. The attacker may use various methods, such as scanning, phishing, or searching open sources, to collect data that can help them plan the attack. Weaponization: The attacker creates or obtains a malicious payload, such as malware, exploit, or script, that can be used to compromise the target. The attacker may also embed the payload into a delivery mechanism, such as an email attachment, a web link, or a removable media.

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

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

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

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

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

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.

Question: 83

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

- A. 5,000
- B. 10,000
- C. 15,000
- D. 20,000

Answer: B

Explanation:

The Broker VM is a virtual machine that you can deploy in your network to provide various services and functionalities to the Cortex XDR agents. One of the services that the Broker VM offers is the Local Agent Settings applet, which allows you to configure the agent proxy, agent installer, and content caching settings for the agents.

The Local Agent Settings applet can support a maximum number of 10,000 agents per Broker VM. If you have more than 10,000 agents in your network, you need to deploy additional Broker VMs and distribute the load among them. Reference: Broker VM Overview: This document provides an overview of the Broker VM and its features, requirements, and deployment options.

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

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

Question: 84

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

- A. UASLR
- C. JIT Mitigation
- D. Memory Limit Heap Spray Check
- E. DLL Security

Answer: B

Explanation:

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

Palo Alto Networks. (2023). PCDRA Study Guide. PDF file. Retrieved from

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf

Palo Alto Networks. (2021). Exploit Protection Modules. Web page. Retrieved from

<https://docs.paloaltonetworks.com/traps/6-0/traps-endpoint-security-manager-admin/traps-endpoint-security-policies/exploit-protection-modules.html>

Question: 85

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

- A. To extort a payment from a victim or potentially embarrass the owners.
- B. To gain notoriety and potentially a consulting position.
- C. To better understand the underlying virtual infrastructure.
- D. To potentially perform a Distributed Denial of Attack.

Answer: A

Explanation:

Encrypting a hypervisor or a multiple number of virtual machines running on a server is a form of ransomware attack, which is a type of cyberattack that involves locking or encrypting the victim's data or system and demanding a ransom for its release. The attacker may threaten to encrypt the hypervisor or the virtual machines

to extort a payment from the victim or potentially embarrass the owners by exposing their sensitive or confidential information. Encrypting a hypervisor or a multiple number of virtual machines can have a severe impact on the victim's business operations, as it can affect the availability, integrity, and confidentiality of their data and applications. The attacker may also use the encryption as a leverage to negotiate a higher ransom or to coerce the victim into complying with their demands. Reference:

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

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

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

Question: 86

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

Explanation:

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

Anti-malware protection

Behavioral threat protection

Exploit protection

File integrity monitoring

Network security

Audit and remediation

Live terminal

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

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

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

Question: 87

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

Explanation:

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

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

In the Cortex XDR management console, go 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.

Question: 88

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: B

Explanation:

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

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

In the Cortex XDR management console, go 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.

Question: 89

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: C

Explanation:

An example of an attack vector for ransomware is phishing emails containing malicious attachments. Phishing is a technique that involves sending fraudulent emails that appear to come from a legitimate source, such as a bank, a company, or a government agency. The emails typically contain a malicious attachment, such as a PDF document, a ZIP archive, or a Microsoft Office document, that contains ransomware or a ransomware downloader. When the recipient opens or downloads the attachment, the ransomware is executed and encrypts the files or data on the victim's system. The attacker then demands a ransom for the decryption key, usually in cryptocurrency.

Phishing emails are one of the most common and effective ways of delivering ransomware, as they can bypass security measures such as firewalls, antivirus software, or URL filtering. Phishing emails can also exploit the human factor, as they can trick the recipient into opening the attachment by using social engineering techniques, such as impersonating a trusted sender, creating a sense of urgency, or appealing to curiosity or greed. Phishing emails can also target specific individuals or organizations, such as executives, employees, or customers, in a technique called spear phishing, which increases the chances of success.

According to various sources, phishing emails are the main vector of ransomware attacks, accounting for more than 90% of all ransomware infections¹². Some of the most notorious ransomware campaigns, such as CryptoLocker, Locky, and WannaCry, have used phishing emails as their primary delivery method³. Therefore, it is essential to educate users on how to recognize and avoid phishing emails, as well as to implement security solutions that can detect and block malicious attachments. Reference:

Top 7 Ransomware Attack Vectors & How to Avoid Becoming a Victim - Bitsight [What Is the Main Vector of Ransomware Attacks? A Definitive Guide](#) [CryptoLocker Ransomware Information Guide and FAQ](#) [[Locky Ransomware Information, Help Guide, and FAQ](#)] [[WannaCry ransomware attack](#)]

Question: 90

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

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

Answer: C

Explanation:

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

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

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.

Question: 91

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

- A. Using the Open Card Only
- B. Using the Open Card and Open Timeline actions respectively
- C. You can't pivot within a row to Causality view and Timeline views
- D. Using Open Timeline Actions Only

Answer: B

Explanation:

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

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

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