Exam Code: PCDRA

Exam Name: Palo Alto Networks Certified Detection and Remediation Analyst

$\mathcal{V}$dumps

Exam A

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

Correct Answer: D
Section:
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&CK1
Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK2
Phishing for information, Part 2: Tactics and techniques3
PHISHING AND THE MITREATT&CK FRAMEWORK - EnterpriseTalk4
Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK5

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'

Correct Answer: B
Section:
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.
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

Correct Answer: D
Section:
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.

Correct Answer: B, D
Section:
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.
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.

Correct Answer: D
Section:
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

Correct Answer: C
Section:
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

Correct Answer: D
Section:
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, Dylib Hijacking is the Cortex XDR module that specifically addresses the prevention of attackers loading dynamic libraries from unsecure locations on macOS. By leveraging this module, organizations can enhance their security posture and protect against this specific attack vector.
Endpoint Protection Modules

DDL Security
Hot Patch Protection
Kernel Integrity Monitor

QUESTION 8
What is the purpose of the Unit42 team?

A. Unit42 is responsible for automation and orchestration of products
B. Unit42 is responsible for the configuration optimization of the Cortex XDR server
C. Unit42 is responsible for threat research, malware analysis and threat hunting
D. Unit42 is responsible for the rapid deployment of Cortex XDR agents

Correct Answer: C
Section:
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 agents5 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.
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

Correct Answer: C
Section:
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.

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

Correct Answer: C

Section:

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.

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

Correct Answer: D

Section:

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.

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

Correct Answer: A
Section:
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.

View Incident Details
View WildFire Reports
Action Center
Agent Audit Logs
HUB

QUESTION 13
What does the following output tell us?

Top Hosts (Top 10 | Last 30 days) ★

HOST NAME	INCIDENTS BREAKDOWN	
shpapy_win10	**6**	[• 5 • 1]
win7mickey	**5**	[• 5]
desktop-vjb9012	**5**	[• 4 • 1]
cpsp-enzo	**4**	[• 3 • 1]
win10lab-thomas	**3**	[• 3]
pure_windows_10	**3**	[• 3]
lab1-8-cpsp	**3**	[• 3]
guru-pf	**3**	[• 3]
roneytestwindow	**3**	[• 3]
erikj-cpsp	**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.

Correct Answer: D

Section:

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 .

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

Correct Answer: B
Section:
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.
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

Correct Answer: B
Section:
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.

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 singer?

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 singer 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.

Correct Answer: C
Section:
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.

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.

Correct Answer: A
Section:
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.
Behavioral Threat Protection
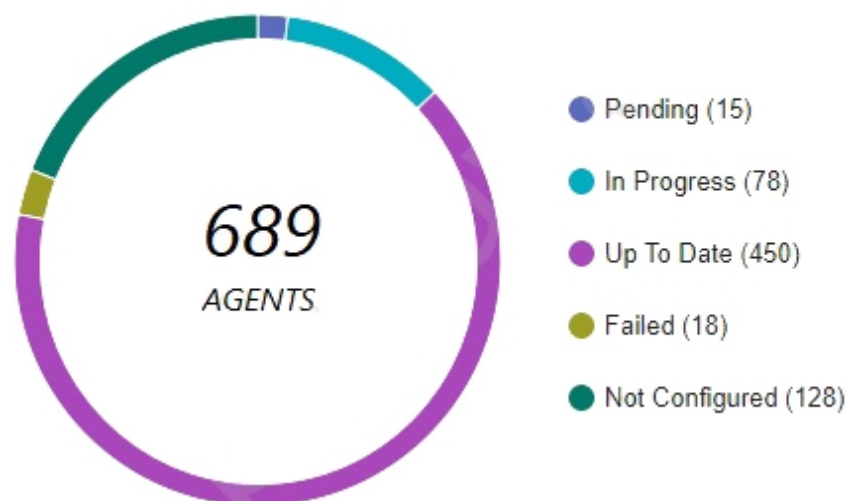Create a BTP Rule
DLL Protection
Create an IOC Rule
[Cytool]

QUESTION 18
Which statement is true based on the following Agent Auto Upgrade widget?

⚸ Agent Auto Update Status

689
AGENTS

● Pending (15)
● In Progress (78)
● Up To Date (450)
● Failed (18)
● Not Configured (128)

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.

Correct Answer: B
Section:
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.

Correct Answer: A
Section:
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

Correct Answer: D
Section:
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.

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

Correct Answer: D
Section:
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.

Correct Answer: B
Section:
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

Correct Answer: B
Section:
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 SHA256-based SSL certificate?

A. Agent Proxy

B. Agent Installer and Content Caching

C. Syslog Collector

D. CSV Collector

Correct Answer: B
Section:
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

Correct Answer: D
Section:
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

Correct Answer: C
Section:
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

Correct Answer: D
Section:
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 here1and 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

Correct Answer: A
Section:
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 attack123456
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

Correct Answer: A
Section:
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 file1234
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

Correct Answer: B
Section:
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 here1and 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

Correct Answer: D
Section:
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
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

Correct Answer: D
Section:
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
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.

Correct Answer: A, B
Section:
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, right-click 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
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.

Correct Answer: B
Section:
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

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.

Correct Answer: B
Section:
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

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 then application exploits.

C. The ultimate goal of any exploit is to reach the kernel.

D. Application exploits leverage kernel vulnerability.

Correct Answer: C
Section:
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

Correct Answer: D
Section:
Explanation:
To create a BIOC rule with XQL query, you must at a minimum filter on theevent_typefield 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.

Correct Answer: B
Section:
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.
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.

Correct Answer: C
Section:
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.
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

Correct Answer: A
Section:
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.
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

Correct Answer: D
Section:
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.

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