Vendor: Palo Alto Networks

Exam Code: XDR-Analyst

Exam Name: Palo Alto Networks XDR Analyst

Version: DEMO

QUESTION 1
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.

QUESTION 2
Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

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

Answer: D
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.

QUESTION 3
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.

QUESTION 4
What functionality of the Broker VM would you use to ingest third-party firewall logs to the Cortex Data Lake?

A. Netflow Collector
B. Syslog Collector
C. DB Collector
D. Pathfinder

Answer: B
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.

QUESTION 5
In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

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

Answer: B
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.

QUESTION 6
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.

QUESTION 7
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.

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.

QUESTION 8
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.

QUESTION 9
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.

QUESTION 10
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 details.

QUESTION 11
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 Policy.
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 file.

QUESTION 12
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 response. 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 important.
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 policy. 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 rules.

QUESTION 13
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.

QUESTION 14
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.

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**