Reliable XDR-Analyst Test Sample & Updated XDR-Analyst CBT

Constantly updated multiple mock exams with a great number of questions that will help you in better self-assessment. Memorize all your previous Palo Alto Networks XDR Analyst (XDR-Analyst) exam questions attempts and display all the changes in your results at the end of each Palo Alto Networks XDR-Analyst Practice Exam attempt. Users will be able to customize the XDR-Analyst practice test software by time or question types. Supported on all Windows-based PCs.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Analysis: This domain encompasses querying data with XQL language, utilizing query templates and libraries, working with lookup tables, hunting for IOCs, using Cortex XDR dashboards, and understanding data retention and Host Insights.
Topic 2	• Incident Handling and Response: This domain focuses on investigating alerts using forensics, causality chains and timelines, analyzing security incidents, executing response actions including automated remediation, and managing exclusions.
Topic 3	• Endpoint Security Management: This domain addresses managing endpoint prevention profiles and policies, validating agent operational states, and assessing the impact of agent versions and content updates.
Topic 4	• Alerting and Detection Processes: This domain covers identifying alert types and sources, prioritizing alerts through scoring and custom configurations, creating incidents, and grouping alerts with data stitching techniques.

>> Reliable XDR-Analyst Test Sample <<

Get Latest Reliable XDR-Analyst Test Sample and High Hit Rate Updated XDR-Analyst CBT

We provide first-rate service on the XDR-Analyst learning prep to the clients and they include the service before and after the sale, 24-hours online customer service and long-distance assistance, the refund service and the update service. The client can try out our and download XDR-Analyst guide materials freely before the sale and if the client have problems about our product after the sale they can contact our customer service at any time. We provide 24-hours online customer service which replies the client's questions and doubts about our XDR-Analyst training quiz and solve their problems.

Palo Alto Networks XDR Analyst Sample Questions (Q40-Q45):

NEW QUESTION # 40
What should you do to automatically convert leads into alerts after investigating a lead?

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

Answer: A

Explanation:
To automatically convert leads into alerts after investigating a lead, you should create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting. IOC rules are used to detect known threats based on indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, etc. By creating IOC rules from the leads, you can prevent future occurrences of the same threats and generate alerts for them. Reference:
PCDRA Study Guide, page 25
Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2
Cortex XDR Documentation, section "Create IOC Rules"

NEW QUESTION # 41
What are two purposes of "Respond to Malicious Causality Chains" in a Cortex XDR Windows Malware profile? (Choose two.)

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

Answer: B,D

NEW QUESTION # 42
Which module provides the best visibility to view vulnerabilities?

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

Answer: B

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

threats and improve your security posture. Reference:
Host Insights
Vulnerability Management

NEW QUESTION # 43
What is the standard installation disk space recommended to install a Broker VM?

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

Answer: A

Explanation:
The Broker VM for Cortex XDR is a virtual machine that serves as the central communication hub for all Cortex XDR agents deployed in your organization. It enables agents to communicate with the Cortex XDR cloud service and allows you to manage and monitor the agents' activities from a centralized location. The system requirements for the Broker VM are as follows:
CPU: 4 cores
RAM: 8 GB
Disk space: 256 GB
Network: Internet access and connectivity to all Cortex XDR agents
The disk space requirement is based on the number of agents and the frequency of content updates. The Broker VM stores the content updates locally and distributes them to the agents. The disk space also depends on the retention period of the content updates, which can be configured in the Broker VM settings. The default retention period is 30 days.
Reference:
Broker VM for Cortex XDR
PCDRA Study Guide

NEW QUESTION # 44
Which of the following represents a common sequence of cyber-attack tactics?

- A. Installation - Reconnaissance - Weaponization & Delivery - Exploitation - Command & Control - Actions on the objective
- B. Actions on the objective - Reconnaissance - Weaponization & Delivery - Exploitation - Installation - Command & Control
- C. Reconnaissance - Weaponization & Delivery - Exploitation - Installation - Command & Control - Actions on the objective
- D. Reconnaissance - Installation - Weaponization & Delivery -Exploitation - Command & Control - Actions on the objective

Answer: C

Explanation:
A common sequence of cyber-attack tactics is based on the Cyber Kill Chain model, which describes the stages of a cyber intrusion from the perspective of the attacker. The Cyber Kill Chain model consists of seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. These phases are briefly explained below:
Reconnaissance: The attacker gathers information about the target, such as its network, systems, vulnerabilities, employees, and business operations. The attacker may use various methods, such as scanning, phishing, or searching open sources, to collect data that can help them plan the attack.
Weaponization: The attacker creates or obtains a malicious payload, such as malware, exploit, or script, that can be used to compromise the target. The attacker may also embed the payload into a delivery mechanism, such as an email attachment, a web link, or a removable media.
Delivery: The attacker sends or delivers the weaponized payload to the target, either directly or indirectly. The attacker may use various channels, such as email, web, or physical access, to reach the target's network or system.
Exploitation: The attacker exploits a vulnerability or weakness in the target's network or system to execute the payload. The vulnerability may be technical, such as a software flaw, or human, such as a social engineering trick.
Installation: The attacker installs or drops additional malware or tools on the target's network or system to establish a foothold and maintain persistence. The attacker may use various techniques, such as registry modification, file manipulation, or process injection, to hide their presence and evade detection.
Command and Control: The attacker establishes a communication channel between the compromised target and a remote server or controller. The attacker may use various protocols, such as HTTP, DNS, or IRC, to send commands and receive data from the target.

Actions on the objective: The attacker performs the final actions that achieve their goal, such as stealing data, destroying files, encrypting systems, or disrupting services. The attacker may also try to move laterally within the target's network or system to access more resources or data.
Reference:
Cyber Kill Chain: This document explains the Cyber Kill Chain model and how it can be used to analyze and respond to cyberattacks.
Cyber Attack Tactics: This document provides an overview of some common cyber attack tactics and examples of how they are used by threat actors.

NEW QUESTION # 45
.....