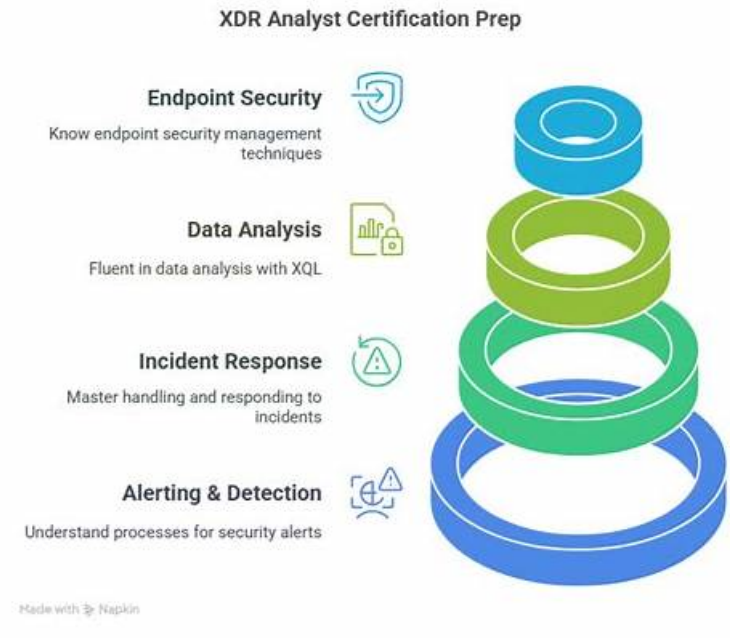
XDR-Analyst Regualer Update - Visual XDR-Analyst Cert Exam



TroytecDumps's expert team use their experience and knowledge to study the examinations of past years and finally have developed the best training materials about Palo Alto Networks certification XDR-Analyst exam. Our Palo Alto Networks certification XDR-Analyst exam training materials are very popular among customers and this is the result ofTroytecDumps's expert team industrious labor. The simulation test and the answer of their research have a high quality and have 95% similarity with the true examination questions. TroytecDumps is well worthful for you to rely on. If you use TroytecDumps's training tool, you can 100% pass your first time to attend Palo Alto Networks Certification XDR-Analyst Exam.

How can our XDR-Analyst study questions are so famous and become the leader in the market? Because our XDR-Analyst learning braindumps comprise the most significant questions and answers that have every possibility to be the part of the real exam. As you study with our XDR-Analyst Practice Guide, you will find the feeling that you are doing the real exam. Especially if you choose the Software version of our XDR-Analyst training engine, which can simulate the real exam.

>> XDR-Analyst Regualer Update <<

Visual XDR-Analyst Cert Exam, XDR-Analyst Exam Assessment

After you practice our XDR-Analyst study materials, you can master the examination point from the XDR-Analyst exam torrent. Then, you will have enough confidence to pass your XDR-Analyst exam. We can succeed so long as we make efforts for one thing. As for the safe environment and effective product, why don't you have a try for our XDR-Analyst Test Question, never let you down! Before your purchase, there is a free demo of our XDR-Analyst training material for you. You can know the quality of our XDR-Analyst guide question earlier before your purchase.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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.
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	• 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.

Palo Alto Networks XDR Analyst Sample Questions (Q83-Q88):

NEW QUESTION # 83
What should you do to automatically convert leads into alerts after investigating a lead?

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

Answer: D

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 # 84
What does the following output tell us?

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

Answer: B

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

NEW QUESTION # 85
In the deployment of which Broker VM applet are you required to install a strong cipher SHA256-based SSL certificate?

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

Answer: A

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

NEW QUESTION # 86
What is the maximum number of agents one Broker VM local agent applet can support?

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

Answer: A

Explanation:
The Broker VM is a virtual machine that you can deploy in your network to provide various services and functionalities to the Cortex XDR agents. One of the services that the Broker VM offers is the Local Agent Settings applet, which allows you to configure the agent proxy, agent installer, and content caching settings for the agents. The Local Agent Settings applet can support a maximum number of 10,000 agents per Broker VM. If you have more than 10,000 agents in your network, you need to deploy additional Broker VMs and distribute the load among them. Reference:
Broker VM Overview: This document provides an overview of the Broker VM and its features, requirements, and deployment options.
Configure the Broker VM: This document explains how to install, set up, and configure the Broker VM in an ESXi environment.
Manage Broker VM from the Cortex XDR Management Console: This document describes how to activate and manage the Broker VM applets from the Cortex XDR management console.

NEW QUESTION # 87
An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

- A. Dylib Hijacking
- B. Kernel Integrity Monitor (KIM)
- C. Hot Patch Protection
- D. DDL Security

Answer: A

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.
Reference:
Endpoint Protection Modules
DDL Security
Hot Patch Protection
Kernel Integrity Monitor

NEW QUESTION # 88
.....

There is no doubt that obtaining this XDR-Analyst certification is recognition of their ability so that they can find a better job and gain the social status that they want. Most people are worried that it is not easy to obtain the certification of XDR-Analyst, so they dare not choose to start. We are willing to appease your troubles and comfort you. We are convinced that our XDR-Analyst test material can help you solve your problems. Compared to other learning materials, our XDR-Analyst exam qeustions are of higher quality and can give you access to the XDR-Analyst certification that you have always dreamed of.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes