Real Downloadable XDR-Analyst PDF, Latest Test XDR-Analyst Discount

The exam questions and answers of general Palo Alto Networks certification exams are produced by the Palo Alto Networks specialist professional experience. TroytecDumps just have these Palo Alto Networks experts to provide you with practice questions and answers of the exam to help you pass the exam successfully. Our TroytecDumps's practice questions and answers have 100% accuracy. Purchasing products of TroytecDumps you can easily obtain Palo Alto Networks certification and so that you will have a very great improvement in XDR-Analyst area.

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	• 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 3	• 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 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.

>> Downloadable XDR-Analyst PDF <<

Pass XDR-Analyst Exam with Newest Downloadable XDR-Analyst PDF by TroytecDumps

As is known to us, there are best sale and after-sale service of the XDR-Analyst study materials all over the world in our company. Our company has employed a lot of excellent experts and professors in the field in the past years, in order to design the best and most suitable XDR-Analyst study materials for all customers. More importantly, it is evident to all that the XDR-Analyst study materials from our company have a high quality, and we can make sure that the quality of our products will be higher than other study materials in the market. If you want to pass the XDR-Analyst Exam and get the related certification in the shortest time, choosing the XDR-Analyst study materials from our company will be in the best interests of all people. We can make sure that it will

be very easy for you to pass your exam and get the related certification in the shortest time that beyond your imagination.

Palo Alto Networks XDR Analyst Sample Questions (Q23-Q28):

NEW QUESTION # 23
When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

- A. Machine Remediation
- B. Automatic Remediation
- C. Remediation Suggestions
- D. Remediation Automation

Answer: C

Explanation:
When investigating security events, the feature in Cortex XDR that is useful for reverting the changes on the endpoint is Remediation Suggestions. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR. Reference:
Remediation Suggestions
Apply Remediation Suggestions

NEW QUESTION # 24
Which of the following policy exceptions applies to the following description?
'An exception allowing specific PHP files'

- A. Process exception
- B. Behavioral threat protection rule exception
- C. Local file threat examination exception
- D. Support exception

Answer: C

Explanation:
The policy exception that applies to the following description is B, local file threat examination exception. A local file threat examination exception is an exception that allows you to exclude specific files or folders from being scanned by the Cortex XDR agent for malware or threats. You can use this exception to prevent false positives, performance issues, or compatibility problems with legitimate files or applications. You can define the local file threat examination exception by file name, file path, file hash, or digital signer. For example, you can create a local file threat examination exception for specific PHP files by entering their file names or paths in the exception configuration. Reference:
Local File Threat Examination Exceptions
Create a Local File Threat Examination Exception

NEW QUESTION # 25
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 allows to interfere with the pattern as soon as it is observed on the endpoint.
- C. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.
- D. 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.

Answer: B

Explanation:
Cortex XDR Analytics is a cloud-based service that uses machine learning and artificial intelligence to detect and prevent network

attacks. Cortex XDR Analytics can interfere with the attack pattern as soon as it is observed on the endpoint by applying protection policies that block malicious processes, files, or network connections. This way, Cortex XDR Analytics can stop the attack before it causes any damage or compromises the system. Reference:
[Cortex XDR Analytics Overview]
[Cortex XDR Analytics Protection Policies]

NEW QUESTION # 26
Which statement best describes how Behavioral Threat Protection (BTP) works?

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

Answer: A

Explanation:
The statement that best describes how Behavioral Threat Protection (BTP) works is D, BTP uses machine learning to recognize malicious activity even if it is not known. BTP is a feature of Cortex XDR that allows you to define custom rules to detect and block malicious behaviors on endpoints. BTP uses machine learning to profile behavior and detect anomalies indicative of attack. BTP can recognize malicious activity based on file attributes, registry keys, processes, network connections, and other criteria, even if the activity is not associated with any known malware or threat. BTP rules are updated through content updates and can be managed from the Cortex XDR console.
The other statements are incorrect for the following reasons:
A is incorrect because BTP does not inject into known vulnerable processes to detect malicious activity. BTP does not rely on process injection, which is a technique used by some malware to hide or execute code within another process. BTP monitors the behavior of all processes on the endpoint, regardless of their vulnerability status, and compares them with the BTP rules.
B is incorrect because BTP does not run on the Cortex XDR and distribute behavioral signatures to all agents. BTP runs on the Cortex XDR agent, which is installed on the endpoint, and analyzes the endpoint data locally. BTP does not use behavioral signatures, which are predefined patterns of malicious behavior, but rather uses machine learning to identify anomalies and deviations from normal behavior.
C is incorrect because BTP does not match EDR data with rules provided by Cortex XDR. BTP is part of the EDR (Endpoint Detection and Response) capabilities of Cortex XDR, and uses the EDR data collected by the Cortex XDR agent to perform behavioral analysis. BTP does not match the EDR data with rules provided by Cortex XDR, but rather applies the BTP rules defined by the Cortex XDR administrator or the Palo Alto Networks threat research team.
Reference:
Cortex XDR Agent Administrator Guide: Behavioral Threat Protection
Cortex XDR: Stop Breaches with AI-Powered Cybersecurity

NEW QUESTION # 27
Which minimum Cortex XDR agent version is required for Kubernetes Cluster?

- A. Cortex XDR 6.1
- B. Cortex XDR 5.0
- C. Cortex XDR 7.4
- D. Cortex XDR 7.5

Answer: D

Explanation:
The minimum Cortex XDR agent version required for Kubernetes Cluster is Cortex XDR 7.5. This version introduces the Cortex XDR agent for Kubernetes hosts, which provides protection and visibility for Linux hosts that run on Kubernetes clusters. The Cortex XDR agent for Kubernetes hosts supports the following features:
Anti-malware protection
Behavioral threat protection
Exploit protection
File integrity monitoring
Network security
Audit and remediation

Live terminal
To install the Cortex XDR agent for Kubernetes hosts, you need to deploy the Cortex XDR agent as a DaemonSet on your Kubernetes cluster. You also need to configure the agent settings profile and the agent installer in the Cortex XDR management console. Reference:
Cortex XDR Agent Release Notes: This document provides the release notes for Cortex XDR agent versions, including the new features, enhancements, and resolved issues.
Install the Cortex XDR Agent for Kubernetes Hosts: This document explains how to install and configure the Cortex XDR agent for Kubernetes hosts using the Cortex XDR management console and the Kubernetes command-line tool.

NEW QUESTION # 28
.....

Buying any product should choose a trustworthy company. Our TroytecDumps can give you the promise of the highest pass rate of XDR-Analyst exam; we can give you a promise to try our XDR-Analyst software for free, and the promise of free updates within a year after purchase. To resolve your doubts, we assure you that if you regrettably fail the XDR-Analyst Exam, we will full refund all the cost you buy our study materials. TroytecDumps is your best partners in your preparation for XDR-Analyst exam.