Palo Alto Networks XDR-Analyst Exam Dumps - Get Success In First Attempt [2026]

Practice materials are typically seen as the tools of reviving, practicing and remembering necessary exam questions for the exam, spending much time on them you may improve the chance of winning. However, our XDR-Analyst training materials can offer better condition than traditional practice materials and can be used effectively. We treat it as our major responsibility to offer help so our XDR-Analyst Practice Guide can provide so much help, the most typical one is the efficiency of our XDR-Analyst exam questions, which can help you pass the XDR-Analyst exam only after studying for 20 to 30 hours.

Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 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	• 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	• 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.

Free XDR-Analyst Brain Dumps | Free XDR-Analyst Pdf Guide

There are rare products which can rival with our products and enjoy the high recognition and trust by the clients like our products. Our products provide the XDR-Analyst study materials to clients and help they pass the test XDR-Analyst certification which is highly authorized and valuable. Our company is a famous company which bears the world-wide influences and our XDR-Analyst Study Materials are recognized as the most representative and advanced study materials among the same kinds of products.

Palo Alto Networks XDR Analyst Sample Questions (Q19-Q24):

NEW QUESTION # 19
What is the action taken out by Managed Threat Hunting team for Zero Day Exploits?

- A. MTH pushes content updates to prevent against the zero-day exploits.
- B. MTH runs queries and investigative actions and no further action is taken.
- C. MTH researches for threats in the tenant and generates a report with the findings.
- D. MTH researches for threats in the logs and reports to engineering.

Answer: C

Explanation:
The Managed Threat Hunting (MTH) team is a group of security experts who proactively hunt for threats in the Cortex XDR tenant and generate a report with the findings. The MTH team uses advanced queries and investigative actions to identify and analyze potential threats, such as zero-day exploits, that may have bypassed the prevention and detection capabilities of Cortex XDR. The MTH team also provides recommendations and best practices to help customers remediate the threats and improve their security posture. Reference:
Managed Threat Hunting Service
Managed Threat Hunting Report

NEW QUESTION # 20
Which minimum Cortex XDR agent version is required for Kubernetes Cluster?

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

Answer: B

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 # 21

Phishing belongs to which of the following MITRE ATT&CK tactics?

- A. Initial Access, Persistence
- B. Persistence, Command and Control
- C. Reconnaissance, Initial Access
- D. Reconnaissance, Persistence

Answer: C

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&CK 1
Phishing for Information, Technique T1598 - Enterprise | MITRE ATT&CK 2 Phishing for information, Part 2: Tactics and techniques 3 PHISHING AND THE MITREATT&CK FRAMEWORK - EnterpriseTalk 4 Initial Access, Tactic TA0001 - Enterprise | MITRE ATT&CK 5

NEW QUESTION # 22
Which Exploit Protection Module (EPM) can be used to prevent attacks based on OS function?

- A. UASLR
- B. JIT Mitigation
- C. Memory Limit Heap Spray Check
- D. DLL Security

Answer: B

Explanation:
JIT Mitigation is an Exploit Protection Module (EPM) that can be used to prevent attacks based on OS function. JIT Mitigation protects against exploits that use the Just-In-Time (JIT) compiler of the OS to execute malicious code. JIT Mitigation monitors the memory pages that are allocated by the JIT compiler and blocks any attempts to execute code from those pages. This prevents attackers from using the JIT compiler as a way to bypass other security mechanisms such as Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR). Reference:
Palo Alto Networks. (2023). PCDRA Study Guide. PDF file. Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcdra-study-guide.pdf Palo Alto Networks. (2021). Exploit Protection Modules. Web page. Retrieved from https://docs.paloaltonetworks.com/traps/6-0/traps-endpoint-security-manager-admin/traps-endpoint-security-policies/exploit-protection-modules.html

NEW QUESTION # 23
Which statement best describes how Behavioral Threat Protection (BTP) works?

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

Answer: C

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 # 24
.....

Success in the test of the Palo Alto Networks XDR Analyst (XDR-Analyst) certification proves your technical knowledge and skills. The XDR-Analyst exam credential paves the way toward landing high-paying jobs or promotions in your organization. Many people who attempt the Palo Alto Networks XDR Analyst (XDR-Analyst) exam questions don't find updated practice questions. Due to this they don't prepare as per the current XDR-Analyst examination content and fail the final test.

www.stes.tyc.edu.tw, Disposable vapes