# XDR-Analyst Demo Test | New XDR-Analyst Test Questions


Prep4King XDR-Analyst exam dumps offer a full refund if you cannot pass XDR-Analyst certification on your first try. This is a risk-free guarantee currently enjoyed by our more than 90,000 clients. We can assure that you can always count on our braindumps material. We are proud to say that our XDR-Analyst Exam Dumps material to reduce your chances of failing the XDR-Analyst certification. Therefore, you are not only saving a lot of time but money as well.

## Palo Alto Networks XDR-Analyst Exam Syllabus Topics:

| Topic | Details |
|---|---|
| Topic 1 | • 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 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 | • 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 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. |

**>> XDR-Analyst Demo Test <<**

# New XDR-Analyst Test Questions & XDR-Analyst Materials

Professional certification can not only improve staff's technical level but also enhance enterprise's competition. Valid Palo Alto Networks XDR-Analyst latest exam cram pdf will be necessary for every candidate since it can point out key knowledge and most of the real test question. XDR-Analyst Latest Exam Cram pdf provides you the simplest way to clear exam with little cost.

# Palo Alto Networks XDR Analyst Sample Questions (Q14-Q19):

**NEW QUESTION # 14**
What is the maximum number of agents one Broker VM local agent applet can support?

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

**Answer: B**

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 # 15**
With a Cortex XDR Prevent license, which objects are considered to be sensors?

- A. Cortex XDR agents
- B. Syslog servers
- C. Palo Alto Networks Next-Generation Firewalls
- D. Third-Party security devices

**Answer: A**

Explanation:
The objects that are considered to be sensors with a Cortex XDR Prevent license are Cortex XDR agents and Palo Alto Networks Next-Generation Firewalls. These are the two sources of data that Cortex XDR can collect and analyze for threat detection and response. Cortex XDR agents are software components that run on endpoints, such as Windows, Linux, and Mac devices, and provide protection against malware, exploits, and fileless attacks. Cortex XDR agents also collect and send endpoint data, such as process activity, network traffic, registry changes, and user actions, to the Cortex Data Lake for analysis and correlation. Palo Alto Networks Next-Generation Firewalls are network security devices that provide visibility and control over network traffic, and enforce security policies based on applications, users, and content. Next-Generation Firewalls also collect and send network data, such as firewall logs, DNS logs, HTTP headers, and WildFire verdicts, to the Cortex Data Lake for analysis and correlation. By integrating data from both Cortex XDR agents and Next-Generation Firewalls, Cortex XDR can provide a comprehensive view of the attack surface and detect threats across the network and endpoint layers. Reference:
Cortex XDR Prevent License
Cortex XDR Agent Features
Next-Generation Firewall Features

**NEW QUESTION # 16**
When reaching out to TAC for additional technical support related to a Security Event; what are two critical pieces of information you need to collect from the Agent? (Choose Two)

- A. The agent technical support file.
- B. The distribution id of the agent.
- C. The prevention archive from the alert.
- D. A list of all the current exceptions applied to the agent.
- E. The unique agent id.

**Answer: A,C**

Explanation:
When reaching out to TAC for additional technical support related to a security event, two critical pieces of information you need to collect from the agent are:
The agent technical support file. This is a file that contains diagnostic information about the agent, such as its configuration, status, logs, and system information. The agent technical support file can help TAC troubleshoot and resolve issues with the agent or the endpoint. You can generate and download the agent technical support file from the Cortex XDR console, or from the agent itself.
The prevention archive from the alert. This is a file that contains forensic data related to the alert, such as the process tree, the network activity, the registry changes, and the files involved. The prevention archive can help TAC analyze and understand the alert and the malicious activity. You can generate and download the prevention archive from the Cortex XDR console, or from the agent itself.
The other options are not critical pieces of information for TAC, and may not be available or relevant for every security event. For example:
The distribution id of the agent is a unique identifier that is assigned to the agent when it is installed on the endpoint. The distribution id can help TAC identify the agent and its profile, but it is not sufficient to provide technical support or forensic analysis. The distribution id can be found in the Cortex XDR console, or in the agent installation folder.
A list of all the current exceptions applied to the agent is a set of rules that define the files, processes, or behaviors that are excluded from the agent's security policies. The exceptions can help TAC understand the agent's configuration and behavior, but they are not essential to provide technical support or forensic analysis. The exceptions can be found in the Cortex XDR console, or in the agent configuration file.
The unique agent id is a unique identifier that is assigned to the agent when it registers with Cortex XDR. The unique agent id can help TAC identify the agent and its endpoint, but it is not sufficient to provide technical support or forensic analysis. The unique agent id can be found in the Cortex XDR console, or in the agent log file.
Reference:
Generate and Download the Agent Technical Support File
Generate and Download the Prevention Archive
Cortex XDR Agent Administrator Guide: Agent Distribution ID
Cortex XDR Agent Administrator Guide: Exception Security Profiles
[Cortex XDR Agent Administrator Guide: Unique Agent ID]

**NEW QUESTION # 17**
What kind of the threat typically encrypts user files?

- A. supply-chain attacks
- B. SQL injection attacks
- C. Zero-day exploits
- D. ransomware

**Answer: D**

Explanation:
Ransomware is a type of malicious software, or malware, that encrypts user files and prevents them from accessing their data until they pay a ransom. Ransomware can affect individual users, businesses, and organizations of all kinds. Ransomware attacks can cause costly disruptions, data loss, and reputational damage. Ransomware can spread through various methods, such as phishing emails, malicious attachments, compromised websites, or network vulnerabilities. Some ransomware variants can also self-propagate and infect other devices or networks. Ransomware authors typically demand payment in cryptocurrency or other untraceable methods, and may threaten to delete or expose the encrypted data if the ransom is not paid within a certain time frame. However, paying the ransom does not guarantee that the files will be decrypted or that the attackers will not target the victim again. Therefore, the best way to protect against ransomware is to prevent infection in the first place, and to have a backup of the data in case of an attack123456 Reference:
What is Ransomware? | How to Protect Against Ransomware in 2023
Ransomware - Wikipedia
What is ransomware? | Ransomware meaning | Cloudflare

What Is Ransomware? | Ransomware.org
Ransomware - FBI

**NEW QUESTION # 18**
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

- A. UDP and a random port
- B. NetBIOS over TCP
- C. WebSocket
- D. TCP, over port 80

**Answer: C**

Explanation:
Live Terminal uses the WebSocket protocol to communicate with the agent on the endpoint. WebSocket is a full-duplex communication protocol that enables bidirectional data exchange between a client and a server over a single TCP connection. WebSocket is designed to be implemented in web browsers and web servers, but it can be used by any client or server application. WebSocket provides a persistent connection between the Cortex XDR console and the endpoint, allowing you to execute commands and receive responses in real time. Live Terminal uses port 443 for WebSocket communication, which is the same port used for HTTPS traffic. Reference:
Initiate a Live Terminal Session
WebSocket

**NEW QUESTION # 19**
.....

- XDR-Analyst Study Dumps □ Reliable XDR-Analyst Exam Review □ XDR-Analyst Dumps Guide □ 「 www.examcollectionpass.com 」 is best website to obtain （ XDR-Analyst ） for free download □Practice XDR-Analyst Exams Free
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, interncorp.in, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes