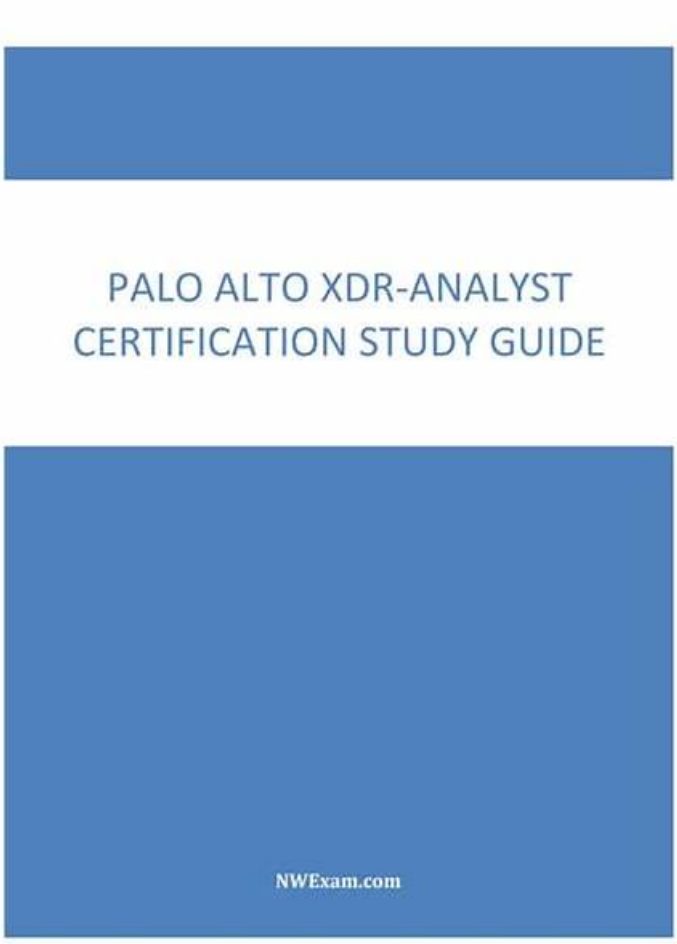
Exam XDR-Analyst Braindumps - Palo Alto Networks XDR Analyst Realistic Reliable Test Preparation Free PDF Quiz



BTW, DOWNLOAD part of FreeCram XDR-Analyst dumps from Cloud Storage: https://drive.google.com/open?id=1KqW2iqT_1tHHQ2HEIQL0R688Wx9n3c5J

The education level of the country has been continuously improved. At present, there are more and more people receiving higher education, and even many college graduates still choose to continue studying in school. Getting the test XDR-Analyst certification maybe they need to achieve the goal of the learning process, have been working for the workers, have more qualifications can they provide wider space for development. The XDR-Analyst Actual Exam guide can provide them with efficient and convenient learning platform so that they can get the certification as soon as possible in the shortest possible time. A high degree may be a sign of competence, getting the test XDR-Analyst certification is also a good choice. When we get enough certificates, we have more options to create a better future.

The FreeCram offers desktop Palo Alto Networks XDR-Analyst Practice Exam software for students to practice for the XDR-Analyst exam. This software mimics the actual Palo Alto Networks XDR Analyst (XDR-Analyst) exam and tracks the student's progress, records grades, and compares results. Available for Windows computers, it requires an internet connection only for license validation.

>> Exam XDR-Analyst Braindumps <<

XDR-Analyst Reliable Test Preparation - Test XDR-Analyst Free

With vast experience in this field, FreeCram always comes forward to provide its valued customers with authentic, actual, and genuine XDR-Analyst exam dumps at an affordable cost. All the Palo Alto Networks XDR Analyst (XDR-Analyst) questions given in the product are based on actual examination topics. FreeCram provides three months of free updates if you purchase the Palo Alto Networks XDR-Analyst Questions and the content of the examination changes after that.

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.

Palo Alto Networks XDR Analyst Sample Questions (Q16-Q21):

NEW QUESTION # 16
After scan, how does file quarantine function work on an endpoint?

- A. Quarantine disables the network adapters and locks down access preventing any communications with the endpoint.
- B. Quarantine takes ownership of the files and folders and prevents execution through access control.
- C. Quarantine prevents an endpoint from communicating with anything besides the listed exceptions in the agent profile and Cortex XDR.
- D. Quarantine removes a specific file from its location on a local or removable drive to a protected folder and prevents it from being executed.

Answer: D

Explanation:
Quarantine is a feature of Cortex XDR that allows you to isolate a malicious file from its original location and prevent it from being executed. Quarantine works by moving the file to a protected folder on the endpoint and changing its permissions and attributes. Quarantine can be applied to files detected by periodic scans or by behavioral threat protection (BTP) rules. Quarantine is only supported for portable executable (PE) and dynamic link library (DLL) files. Quarantine does not affect the network connectivity or the communication of the endpoint with Cortex XDR. Reference:
Quarantine Malicious Files
Manage Quarantined Files

NEW QUESTION # 17
Which type of IOC can you define in Cortex XDR?

- A. Source port
- B. Destination IP Address
- C. Source IP Address
- D. Destination IP Address: Destination

Answer: B

Explanation:
Cortex XDR allows you to define IOC rules based on various types of indicators of compromise (IOC) that you can use to detect and respond to threats in your network. One of the types of IOC that you can define in Cortex XDR is destination IP address, which is the IP address of the remote host that a local endpoint is communicating with. You can use this type of IOC to identify malicious network activity, such as connections to command and control servers, phishing sites, or malware distribution hosts. You can also specify the direction of the network traffic (inbound or outbound) and the protocol (TCP or UDP) for the destination IP address IOC. Reference:
Cortex XDR documentation portal
Is there a possibility to create an IOC list to employ it in a query?
Cortex XDR Datasheet

NEW QUESTION # 18
Which type of BIOC rule is currently available in Cortex XDR?

- A. Network
- B. Discovery
- C. Dropper
- D. Threat Actor

Answer: B

Explanation:
The type of BIOC rule that is currently available in Cortex XDR is Discovery. A Discovery BIOC rule is a rule that detects suspicious or malicious behavior on endpoints based on the Cortex XDR data. A Discovery BIOC rule can use various event types, such as file, injection, load image, network, process, registry, or user, to define the criteria for the rule. A Discovery BIOC rule can also use operators, functions, and variables to create complex logic and conditions for the rule. A Discovery BIOC rule can generate alerts when the rule is triggered, and these alerts can be grouped into incidents for further investigation and response12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Threat Actor: This is not the correct answer. Threat Actor is not a type of BIOC rule that is currently available in Cortex XDR. Threat Actor is a term that refers to an individual or a group that is responsible for a cyberattack or a threat campaign. Cortex XDR does not support creating BIOC rules based on threat actors, but it can provide threat intelligence and context from various sources, such as Unit 42, AutoFocus, or Cortex XSOAR3.
C . Network: This is not the correct answer. Network is not a type of BIOC rule that is currently available in Cortex XDR. Network is an event type that can be used in a Discovery BIOC rule to define the criteria based on network attributes, such as source IP, destination IP, source port, destination port, protocol, or domain. Network is not a standalone type of BIOC rule, but a part of the Discovery BIOC rule2.
D . Dropper: This is not the correct answer. Dropper is not a type of BIOC rule that is currently available in Cortex XDR. Dropper is a term that refers to a type of malware that is designed to download and install other malicious files or programs on a compromised system. Cortex XDR does not support creating BIOC rules based on droppers, but it can detect and prevent droppers using various methods, such as behavioral threat protection, exploit prevention, or WildFire analysis4.
In conclusion, the type of BIOC rule that is currently available in Cortex XDR is Discovery. By using Discovery BIOC rules, you can create custom detection rules that match your specific use cases and scenarios.
Reference:
Create a BIOC Rule
BIOC Rule Event Types
Threat Intelligence and Context
Malware Prevention

NEW QUESTION # 19
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

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

Answer: A

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 # 20
Which statement is true for Application Exploits and Kernel Exploits?

- A. The ultimate goal of any exploit is to reach the application.
- B. The ultimate goal of any exploit is to reach the kernel.
- C. Application exploits leverage kernel vulnerability.
- D. Kernel exploits are easier to prevent then application exploits.

Answer: B

Explanation:
The ultimate goal of any exploit is to reach the kernel, which is the core component of the operating system that has the highest level of privileges and access to the hardware resources. Application exploits are attacks that target vulnerabilities in specific applications, such as web browsers, email clients, or office suites. Kernel exploits are attacks that target vulnerabilities in the kernel itself, such as memory corruption, privilege escalation, or code execution. Kernel exploits are more difficult to prevent and detect than application exploits, because they can bypass security mechanisms and hide their presence from the user and the system. Reference:
Palo Alto Networks Certified Detection and Remediation Analyst (PCDRA) Study Guide, page 8 Palo Alto Networks Cortex XDR Documentation, Exploit Protection Overview

NEW QUESTION # 21
.....

www.dumpsmaterials.com □✔□ enter （ XDR-Analyst ） and obtain a free download □Real XDR-Analyst Torrent

- Free PDF The Best Palo Alto Networks - XDR-Analyst - Exam Palo Alto Networks XDR Analyst Braindumps □ Search on □ www.pdfvce.com □ for ▸ XDR-Analyst ◂ to obtain exam materials for free download □Top XDR-Analyst Dumps
- Trustworthy XDR-Analyst Practice □ Trustworthy XDR-Analyst Practice □ XDR-Analyst Dump Check □ Copy URL “ www.dumpsmaterials.com ” open and search for ✔ XDR-Analyst □✔□ to download for free □Top XDR-Analyst Dumps
- en-web-directory.com, nellsdgx839323.goabroadblog.com, inespdca011030.blogsvirals.com, diegoyeuz678284.topbloghub.com, joanhvsj412662.wikifordummies.com, www.callcentersindia.co.in, www.stes.tyc.edu.tw, theresayyxe401098.wikikali.com, nicolehwzd711705.bloggazza.com, maximusbookmarks.com, Disposable vapes

What's more, part of that FreeCram XDR-Analyst dumps now are free: https://drive.google.com/open?id=1KqW2iqT_1tHHQ2HEIQL0R688Wx9n3c5J