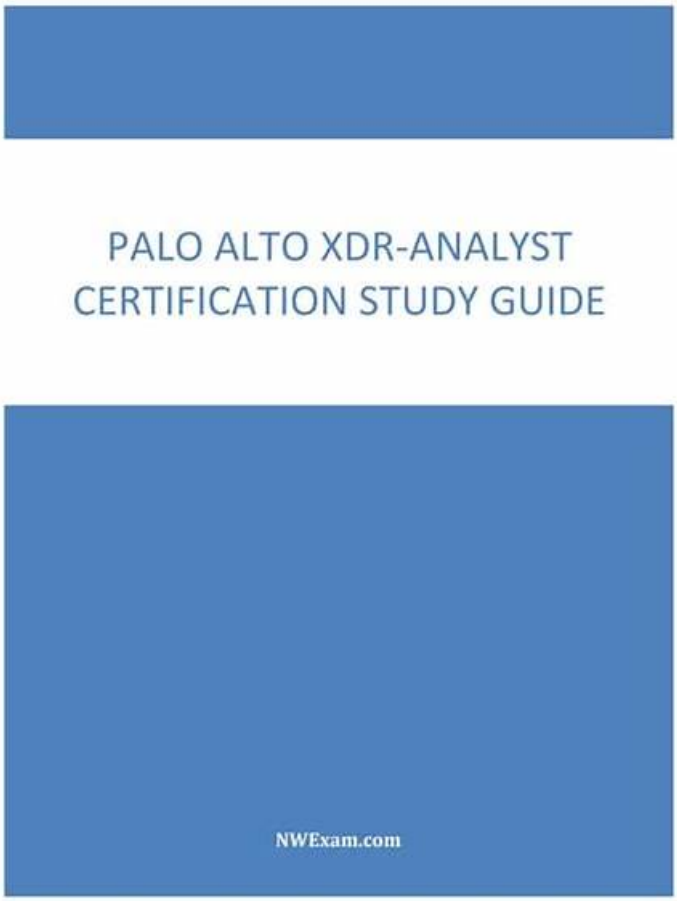
XDR-Analyst New APP Simulations, XDR-Analyst Valid Study Materials



With limited time for your preparation, many exam candidates can speed up your pace of making progress. Our XDR-Analyst practice materials will remedy your faults of knowledge understanding. Many customers get manifest improvement and lighten their load. As we know, some people failed the exam before, and lost confidence in this agonizing exam before purchasing XDR-Analyst Training Materials. We are here divide grieves with you. You can abandon the time-consuming thought from now on. In contrast, they will inspire your potential without obscure content to feel. After getting our XDR-Analyst exam prep, you will not live under great stress during the exam period.

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	• 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 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	• 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.

XDR-Analyst Valid Study Materials - XDR-Analyst New Study Guide

Our company is a professional certification exam materials provider. We have occupied in this field more than ten years, therefore we have rich experiences in providing valid exam dumps. XDR-Analyst training materials cover most of knowledge points for the exam, and you can improve your professional ability in the process of learning. XDR-Analyst Exam Materials are high-quality, and you can improve your efficiency while preparing for the exam. We offer you free demo for XDR-Analyst exam dumps, you can have a try before buying, so that you can have a deeper understanding of what you are going to buy.

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

NEW QUESTION # 14
As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to download Cobalt Strike on one of your servers. Days later, you learn about a massive ongoing supply chain attack. Using Cortex XDR you recognize that your server was compromised by the attack and that Cortex XDR prevented it. What steps can you take to ensure that the same protection is extended to all your servers?

- A. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.
- B. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.
- C. Create IOCs of the malicious files you have found to prevent their execution.
- D. Enable DLL Protection on all servers but there might be some false positives.

Answer: B

Explanation:
To ensure that the same protection is extended to all your servers, you need to create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can use various operators, functions, and variables to define the criteria and the actions for the rules. By creating BTP rules that match the behaviors of the supply chain attack, you can prevent the attack from compromising your servers12.
Let's briefly discuss the other options to provide a comprehensive explanation:
B . Enable DLL Protection on all servers but there might be some false positives: This is not the correct answer. Enabling DLL Protection on all servers will not ensure that the same protection is extended to all your servers. DLL Protection is a feature of Cortex XDR that allows you to block the execution of unsigned or untrusted DLL files on your endpoints. DLL Protection can help to prevent some types of attacks that use malicious DLL files, but it may not be effective against the supply chain attack that used a Trojanized DLL file that was digitally signed by a trusted vendor. DLL Protection may also cause some false positives, as it may block some legitimate DLL files that are unsigned or untrusted3.
C . Create IOCs of the malicious files you have found to prevent their execution: This is not the correct answer. Creating IOCs of the malicious files you have found will not ensure that the same protection is extended to all your servers. IOCs are indicators of compromise that you can create to detect and respond to known threats on your endpoints, such as file hashes, registry keys, IP addresses, domain names, or full paths. IOCs can help to identify and block the malicious files that you have already discovered, but they may not be effective against the supply chain attack that used different variants of the malicious files with different hashes or names. IOCs may also become outdated, as the attackers may change or update their files to evade detection4.
D . Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading: This is not the correct answer. Enabling BTP with cytool will not ensure that the same protection is extended to all your servers. BTP is a feature of Cortex XDR that allows you to create custom rules that detect and block malicious or suspicious behaviors on your endpoints, such as file execution, process injection, network connection, or registry modification. BTP rules can help to prevent the attack from spreading, but they need to be created and configured in the Cortex XDR app, not with cytool. Cytool is a command-line tool that allows you to perform various operations on the Cortex XDR agent, such as installing, uninstalling, upgrading, or troubleshooting. Cytool does not have an option to enable or configure BTP rules.
In conclusion, to ensure that the same protection is extended to all your servers, you need to create BTP rules to recognize and prevent the activity. By using BTP rules, you can create custom and flexible prevention rules that match the behaviors of the supply

chain attack.
Reference:
Behavioral Threat Protection
Create a BTP Rule
DLL Protection
Create an IOC Rule
[Cytool]

NEW QUESTION # 15
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. TCP, over port 80
- D. WebSocket

Answer: D

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 # 16
Which Exploit Protection Module (EPM) can be used to prevent attacks based on OS function?

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

Answer: D

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 # 17
You can star security events in which two ways? (Choose two.)

- A. Create an Incident-starring configuration.
- B. Create an alert-starring configuration.
- C. Manually star an Incident.
- D. Manually star an alert.

Answer: C,D

Explanation:
You can star security events in Cortex XDR in two ways: manually star an alert or an incident, or create an alert-starring or incident-starring configuration. Starring security events helps you prioritize and track the events that are most important to you. You can also filter and sort the events by their star status in the Cortex XDR console.
To manually star an alert or an incident, you can use the star icon in the Alerts table or the Incidents table. You can also star an alert from the Causality View or the Query Center Results table. You can star an incident from the Incident View or the Query Center Results table. You can also unstar an event by clicking the star icon again.
To create an alert-starring or incident-starring configuration, you can use the Alert Starring Configuration or the Incident Starring Configuration pages in the Cortex XDR console. You can define the criteria for starring alerts or incidents based on their severity, category, source, or other attributes. You can also enable or disable the configurations as needed.
Reference:
Star Security Events
Create an Alert Starring Configuration
Create an Incident Starring Configuration

NEW QUESTION # 18
Which of the following represents a common sequence of cyber-attack tactics?

- A. Reconnaissance - Weaponization & Delivery - Exploitation - Installation - Command & Control - Actions on the objective
- B. Installation - Reconnaissance - Weaponization & Delivery - Exploitation - Command & Control - Actions on the objective
- C. Actions on the objective - Reconnaissance - Weaponization & Delivery - Exploitation - Installation - Command & Control
- D. Reconnaissance - Installation - Weaponization & Delivery -Exploitation - Command & Control - Actions on the objective

Answer: A

Explanation:
A common sequence of cyber-attack tactics is based on the Cyber Kill Chain model, which describes the stages of a cyber intrusion from the perspective of the attacker. The Cyber Kill Chain model consists of seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on the objective. These phases are briefly explained below:
Reconnaissance: The attacker gathers information about the target, such as its network, systems, vulnerabilities, employees, and business operations. The attacker may use various methods, such as scanning, phishing, or searching open sources, to collect data that can help them plan the attack.
Weaponization: The attacker creates or obtains a malicious payload, such as malware, exploit, or script, that can be used to compromise the target. The attacker may also embed the payload into a delivery mechanism, such as an email attachment, a web link, or a removable media.
Delivery: The attacker sends or delivers the weaponized payload to the target, either directly or indirectly. The attacker may use various channels, such as email, web, or physical access, to reach the target's network or system.
Exploitation: The attacker exploits a vulnerability or weakness in the target's network or system to execute the payload. The vulnerability may be technical, such as a software flaw, or human, such as a social engineering trick.
Installation: The attacker installs or drops additional malware or tools on the target's network or system to establish a foothold and maintain persistence. The attacker may use various techniques, such as registry modification, file manipulation, or process injection, to hide their presence and evade detection.
Command and Control: The attacker establishes a communication channel between the compromised target and a remote server or controller. The attacker may use various protocols, such as HTTP, DNS, or IRC, to send commands and receive data from the target.
Actions on the objective: The attacker performs the final actions that achieve their goal, such as stealing data, destroying files, encrypting systems, or disrupting services. The attacker may also try to move laterally within the target's network or system to access more resources or data.
Reference:
Cyber Kill Chain: This document explains the Cyber Kill Chain model and how it can be used to analyze and respond to cyberattacks.
Cyber Attack Tactics: This document provides an overview of some common cyber attack tactics and examples of how they are used by threat actors.

NEW QUESTION # 19
.....

You can try our XDR-Analyst study demo for free. There is no any personal information required from your side. The XDR-Analyst complete study material contains comprehensive test information than the demo. So if you are interested with our XDR-Analyst free demo then go for the XDR-Analyst complete questions & answers. We will give you the best offer for the XDR-Analyst practice dumps. 100% pass with XDR-Analyst training dumps at first time is our guarantee.

XDR-Analyst Valid Study Materials: https://www.vcedumps.com/XDR-Analyst-examcollection.html

- Reliable XDR-Analyst Test Sample □ XDR-Analyst Reliable Test Forum □ XDR-Analyst Exam Dumps Provider □ Search for " XDR-Analyst " and download exam materials for free through " www.torrentvce.com " □XDR-Analyst PDF VCE
- Reliable XDR-Analyst Test Sample □ New XDR-Analyst Exam Book □ Reliable XDR-Analyst Exam Voucher □ Open ☀ www.pdfvce.com □☀□ and search for □ XDR-Analyst □ to download exam materials for free □Reliable XDR-Analyst Test Sample
- XDR-Analyst Test Papers □ XDR-Analyst Flexible Testing Engine □ XDR-Analyst Reliable Test Sample □ Search for □ XDR-Analyst □ and download exam materials for free through " www.testkingpass.com " □XDR-Analyst Reliable Test Sample
- Palo Alto Networks XDR-Analyst Web-Based Practice Exam Questions □ Search for " XDR-Analyst " and obtain a free download on ⇛ www.pdfvce.com ⇚ □XDR-Analyst Reliable Test Sample
- XDR-Analyst Exam Guide □ XDR-Analyst Authorized Exam Dumps □ Latest XDR-Analyst Test Format □ The page for free download of ➡ XDR-Analyst □□□ on { www.examcollectionpass.com } will open immediately □XDR-Analyst Reliable Test Forum
- XDR-Analyst Flexible Testing Engine □ Reliable XDR-Analyst Exam Voucher □ XDR-Analyst Test Registration □ Easily obtain ➡ XDR-Analyst □□□ for free download through ➤ www.pdfvce.com □ □XDR-Analyst PDF VCE
- Palo Alto Networks XDR-Analyst Practice Exams Questions □ Open □ www.examcollectionpass.com □ and search for □ XDR-Analyst □ to download exam materials for free □XDR-Analyst Latest Test Labs
- XDR-Analyst Reliable Test Forum □ XDR-Analyst PDF VCE □ XDR-Analyst Test Quiz □ Open ➡ www.pdfvce.com □□□ enter ➥ XDR-Analyst □ and obtain a free download □XDR-Analyst Reliable Test Cost
- Exam XDR-Analyst Exercise □ XDR-Analyst Exam Guide □ XDR-Analyst Exam Dumps Provider □ Download [XDR-Analyst] for free by simply searching on □ www.easy4engine.com □ ☃New XDR-Analyst Exam Book
- The Best XDR-Analyst - Palo Alto Networks XDR Analyst New APP Simulations □ Open ➤ www.pdfvce.com □ enter " XDR-Analyst " and obtain a free download □XDR-Analyst Flexible Testing Engine
- XDR-Analyst Flexible Testing Engine □ XDR-Analyst Reliable Test Forum □ New XDR-Analyst Exam Book □ Search for ✔ XDR-Analyst □✔□ and download exam materials for free through 「 www.vce4dumps.com 」 □XDR-Analyst Authorized Exam Dumps
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, Disposable vapes