XDR-Analyst퍼펙트덤프문제 & XDR-Analyst인증덤프문제

Pass4Test는Palo Alto Networks XDR-Analyst시험을 패스할 수 있는 아주 좋은 사이트입니다. Pass4Test은 아주 알맞게 최고의Palo Alto Networks XDR-Analyst시험문제와 답 내용을 만들어 냅니다. 덤프는 기존의 시험문제와 답과 시험문제분석 등입니다. Pass4Test에서 제공하는Palo Alto Networks XDR-Analyst시험자료의 문제와 답은 실제시험의 문제와 답과 아주 비슷합니다.

Palo Alto Networks XDR-Analyst 시험요강:

주제	소개
주제 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.
주제 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.

주제 3	• 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.
주제 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.

최신 Security Operations XDR-Analyst 무료샘플문제 (Q16-Q21):

질문 # 16
Under which conditions is Local Analysis evoked to evaluate a file before the file is allowed to run?

- A. The endpoint is disconnected or the verdict from WildFire is of a type malware.
- B. The endpoint is disconnected or the verdict from WildFire is of a type grayware.
- C. The endpoint is disconnected or the verdict from WildFire is of a type benign.
- D. The endpoint is disconnected or the verdict from WildFire is of a type unknown.

정답：D

설명:
Local Analysis is a feature of Cortex XDR that allows the agent to evaluate files locally on the endpoint, without sending them to WildFire for analysis. Local Analysis is evoked when the following conditions are met:
The endpoint is disconnected from the internet or the Cortex XDR management console, and therefore cannot communicate with WildFire.
The verdict from WildFire is of a type unknown, meaning that WildFire has not yet analyzed the file or has not reached a conclusive verdict.
Local Analysis uses machine learning models to assess the behavior and characteristics of the file and assign it a verdict of either benign, malware, or grayware. If the verdict is malware or grayware, the agent will block the file from running and report it to the Cortex XDR management console. If the verdict is benign, the agent will allow the file to run and report it to the Cortex XDR management console. Reference:
Local Analysis
WildFire File Verdicts

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

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

정답：B

설명:
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

질문 # 18
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 does not have to interfere with the pattern as soon as it is observed on the endpoint in order to prevent the attack.
- B. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the firewall.
- C. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.
- D. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.

정답：C

설명:
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]

질문 # 19
Which engine, of the following, in Cortex XDR determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident?

- A. Causality Analysis Engine
- B. Log Stitching Engine
- C. Sensor Engine
- D. Causality Chain Engine

정답：A

설명:
The engine that determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident is the Causality Analysis Engine. The Causality Analysis Engine is one of the core components of Cortex XDR that performs advanced analytics on the data collected from various sources, such as endpoints, networks, and clouds. The Causality Analysis Engine uses machine learning and behavioral analysis to identify the root cause, the attack chain, and the impact of each alert. It also groups related alerts into incidents based on the temporal and logical relationships among the alerts. The Causality Analysis Engine helps to reduce the noise and complexity of alerts and incidents, and provides a clear and concise view of the attack story12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Sensor Engine: This is not the correct answer. The Sensor Engine is not responsible for determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident. The Sensor Engine is the component that runs on the Cortex XDR agents installed on the endpoints. The Sensor Engine collects and analyzes endpoint data, such as processes, files, registry keys, network connections, and user activities. The Sensor Engine also enforces the endpoint security policies and performs prevention and response actions3.
C . Log Stitching Engine: This is not the correct answer. The Log Stitching Engine is not responsible for determining the most relevant artifacts in each alert and aggregating all alerts related to an event into an incident. The Log Stitching Engine is the component that runs on the Cortex Data Lake, which is the cloud-based data storage and processing platform for Cortex XDR. The Log Stitching Engine normalizes and stitches together the data from different sources, such as firewalls, proxies, endpoints, and clouds. The Log Stitching Engine enables Cortex XDR to correlate and analyze data from multiple sources and provide a unified view of the network activity and threat landscape4.
D . Causality Chain Engine: This is not the correct answer. Causality Chain Engine is not a valid name for any of the Cortex XDR engines. There is no such engine in Cortex XDR that performs the function of determining the most relevant artifacts in each alert and

aggregating all alerts related to an event into an incident.
In conclusion, the Causality Analysis Engine is the engine that determines the most relevant artifacts in each alert and aggregates all alerts related to an event into an incident. By using the Causality Analysis Engine, Cortex XDR can provide a comprehensive and accurate detection and response capability for security analysts.
Reference:
Cortex XDR Pro Admin Guide: Causality Analysis Engine
Cortex XDR Pro Admin Guide: View Incident Details
Cortex XDR Pro Admin Guide: Sensor Engine
Cortex XDR Pro Admin Guide: Log Stitching Engine

질문 # 20
What is an example of an attack vector for ransomware?

- A. Performing SSL Decryption on an endpoint
- B. Phishing emails containing malicious attachments
- C. A URL filtering feature enabled on a firewall
- D. Performing DNS queries for suspicious domains

정답：B

설명:
An example of an attack vector for ransomware is phishing emails containing malicious attachments. Phishing is a technique that involves sending fraudulent emails that appear to come from a legitimate source, such as a bank, a company, or a government agency. The emails typically contain a malicious attachment, such as a PDF document, a ZIP archive, or a Microsoft Office document, that contains ransomware or a ransomware downloader. When the recipient opens or downloads the attachment, the ransomware is executed and encrypts the files or data on the victim's system. The attacker then demands a ransom for the decryption key, usually in cryptocurrency.
Phishing emails are one of the most common and effective ways of delivering ransomware, as they can bypass security measures such as firewalls, antivirus software, or URL filtering. Phishing emails can also exploit the human factor, as they can trick the recipient into opening the attachment by using social engineering techniques, such as impersonating a trusted sender, creating a sense of urgency, or appealing to curiosity or greed. Phishing emails can also target specific individuals or organizations, such as executives, employees, or customers, in a technique called spear phishing, which increases the chances of success.
According to various sources, phishing emails are the main vector of ransomware attacks, accounting for more than 90% of all ransomware infections12. Some of the most notorious ransomware campaigns, such as CryptoLocker, Locky, and WannaCry, have used phishing emails as their primary delivery method3 . Therefore, it is essential to educate users on how to recognize and avoid phishing emails, as well as to implement security solutions that can detect and block malicious attachments. Reference:
Top 7 Ransomware Attack Vectors & How to Avoid Becoming a Victim - Bitsight What Is the Main Vector of Ransomware Attacks? A Definitive Guide CryptoLocker Ransomware Information Guide and FAQ
[Locky Ransomware Information, Help Guide, and FAQ]
[WannaCry ransomware attack]

질문 # 21
.....

- XDR-Analyst시험패스 가능한 공부 □ XDR-Analyst시험문제집 □ XDR-Analyst최신 업데이트버전 덤프공부 □ ➥ www.dumptop.com □웹사이트를 열고 （ XDR-Analyst ）를 검색하여 무료 다운로드XDR-Analyst유효한 최신덤프공부
- XDR-Analyst최신 업데이트버전 덤프공부 □ XDR-Analyst시험대비 최신 덤프공부자료 □ XDR-Analyst유효한 최신덤프공부 □ ⇛ www.itdumpskr.com ⇚웹사이트에서▸ XDR-Analyst ◂를 열고 검색하여 무료 다운로드XDR-Analyst퍼펙트 덤프데모문제 보기
- XDR-Analyst인증시험 인기 시험자료 □ XDR-Analyst시험대비 최신 덤프자료 ⊷ XDR-Analyst덤프최신버전 □ □ 무료 다운로드를 위해 지금☀ www.itdumpskr.com □☀□에서「 XDR-Analyst 」검색XDR-Analyst최신 업데이트버전 덤프공부
- XDR-Analyst시험패스 가능한 공부 □ XDR-Analyst완벽한 덤프문제자료 □ XDR-Analyst덤프데모문제 다운 □ ➥ www.itdumpskr.com □웹사이트에서□ XDR-Analyst □를 열고 검색하여 무료 다운로드XDR-Analyst인증시험 인기 시험자료
- XDR-Analyst인증시험 인기 시험자료 □ XDR-Analyst최신버전 인기 덤프문제 □ XDR-Analyst높은 통과율 시험대비 덤프공부 □ 검색만 하면【 www.passtip.net 】에서▷ XDR-Analyst ◁무료 다운로드XDR-Analyst최신 업데이트버전 덤프공부
- XDR-Analyst퍼펙트 덤프문제 최신덤프자료 □ [www.itdumpskr.com]의 무료 다운로드“ XDR-Analyst ”페이지가 지금 열립니다XDR-Analyst인증시험 인기 시험자료
- XDR-Analyst완벽한 덤프문제자료 □ XDR-Analyst높은 통과율 시험대비 덤프공부 □ XDR-Analyst최고품질 덤프샘플문제 다운 □ 지금➡ www.koreadumps.com □□□에서⇛ XDR-Analyst ⇚를 검색하고 무료로 다운로드하세요XDR-Analyst인증시험 인기 시험자료
- 퍼펙트한 XDR-Analyst퍼펙트 덤프문제 최신버전 덤프샘플 문제 □ 지금“ www.itdumpskr.com ”을(를) 열고 무료 다운로드를 위해✔ XDR-Analyst □✔□를 검색하십시오XDR-Analyst최고품질 덤프샘플문제 다운
- 적중율 좋은 XDR-Analyst퍼펙트 덤프문제 시험공부자료 □ □ www.passtip.net □을 통해 쉽게（ XDR-Analyst ）무료 다운로드 받기XDR-Analyst최고품질 덤프샘플문제 다운
- 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, pct.edu.pk, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 47.121.119.212, myportal.utt.edu.tt, Disposable vapes