Palo Alto Networks XDR-Analyst資料 & XDR-Analyst考古題

從Google Drive中免費下載最新的PDFExamDumps XDR-Analyst PDF版考試題庫：https://drive.google.com/open?id=13lA9Of5dJ_9yM_F0dp_L_L9rRqIVrzUF

你買了PDFExamDumps的產品，我們會全力幫助你通過認證考試，而且還有免費的一年更新升級服務。如果官方改變了認證考試的大綱，我們會立即通知客戶。如果有我們的軟體有任何更新版本，都會立即推送給客戶。PDFExamDumps是可以承諾幫你成功通過你的第一次Palo Alto Networks XDR-Analyst 認證考試。

Palo Alto Networks XDR-Analyst 考試大綱：

主題	簡介
主題 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.
主題 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.
主題 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.
主題 4	• Endpoint Security Management:
主題 5	• 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考古題 & XDR-Analyst更新

選擇捷徑、使用技巧是為了更好地獲得成功。如果你想獲得一次就通過XDR-Analyst認證考試的保障，那麼PDFExamDumps的XDR-Analyst考古題是你唯一的、也是最好的選擇。這絕對是一個讓你禁不住讚美的考古題。你不可能找到比它更好的考試相關的資料了。這個考古題可以讓你更準確地瞭解考試的出題點，從而讓你更有目的地學習相關知識。另外，如果你實在沒有準備考試的時間，那麼你只需要記好這個考古題裏的試題和答案。因為這個考古題包括了真實考試中的所有試題，所以只是這樣你也可以通過考試。

最新的 Security Operations XDR-Analyst 免費考試真題 (Q11-Q16):

問題 #11
Live Terminal uses which type of protocol to communicate with the agent on the endpoint?

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

答案：B

解題說明：
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

問題 #12
What contains a logical schema in an XQL query?

- A. Field
- B. Bin
- C. Dataset
- D. Array expand

答案：A

解題說明：
A logical schema in an XQL query is a field, which is a named attribute of a dataset. A field can have a data type, such as string, integer, boolean, or array. A field can also have a modifier, such as bin or expand, that transforms the field value in the query output. A field can be used in the select, where, group by, order by, or having clauses of an XQL query. Reference:
XQL Syntax
XQL Data Types
XQL Field Modifiers

問題 #13
To stop a network-based attack, any interference with a portion of the attack pattern is enough to prevent it from succeeding. Which statement is correct regarding the Cortex XDR Analytics module?

- A. It does not need to interfere with the any portion of the pattern to prevent the attack.
- B. It interferes with the pattern as soon as it is observed by the firewall.
- C. It interferes with the pattern as soon as it is observed on the endpoint.

- D. It does not interfere with any portion of the pattern on the endpoint.

答案：C

解題說明：
The correct statement regarding the Cortex XDR Analytics module is D, it interferes with the pattern as soon as it is observed on the endpoint. The Cortex XDR Analytics module is a feature of Cortex XDR that uses machine learning and behavioral analytics to detect and prevent network-based attacks on endpoints. The Cortex XDR Analytics module analyzes the network traffic and activity on the endpoint, and compares it with the attack patterns defined by Palo Alto Networks threat research team. The Cortex XDR Analytics module interferes with the attack pattern as soon as it is observed on the endpoint, by blocking the malicious network connection, process, or file. This way, the Cortex XDR Analytics module can stop the attack before it causes any damage or compromise.
The other statements are incorrect for the following reasons:
A is incorrect because the Cortex XDR Analytics module does interfere with the attack pattern on the endpoint, by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on the firewall or any other network device to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.
B is incorrect because the Cortex XDR Analytics module does not interfere with the attack pattern as soon as it is observed by the firewall. The Cortex XDR Analytics module does not depend on the firewall or any other network device to detect or prevent the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the analysis and interference. The firewall may not be able to observe or block the attack pattern if it is encrypted, obfuscated, or bypassed by the attacker.
C is incorrect because the Cortex XDR Analytics module does need to interfere with the attack pattern to prevent the attack. The Cortex XDR Analytics module does not only detect the attack pattern, but also prevents it from succeeding by blocking the malicious network connection, process, or file. The Cortex XDR Analytics module does not rely on any other response mechanism or human intervention to stop the attack, but rather uses the Cortex XDR agent installed on the endpoint to perform the interference.
Reference:
Cortex XDR Analytics Module
Cortex XDR Analytics Module Detection and Prevention

問題 #14
Where can SHA256 hash values be used in Cortex XDR Malware Protection Profiles?

- A. in the Windows Malware Protection Profile to indicate allowed executables
- B. in the Linux Malware Protection Profile to indicate allowed Java libraries
- C. SHA256 hashes cannot be used in Cortex XDR Malware Protection Profiles
- D. in the macOS Malware Protection Profile to indicate allowed signers

答案：A

解題說明：
Cortex XDR Malware Protection Profiles allow you to configure the malware prevention settings for Windows, Linux, and macOS endpoints. You can use SHA256 hash values in the Windows Malware Protection Profile to indicate allowed executables that you want to exclude from malware scanning. This can help you reduce false positives and improve performance by skipping the scanning of known benign files. You can add up to 1000 SHA256 hash values per profile. You cannot use SHA256 hash values in the Linux or macOS Malware Protection Profiles, but you can use other criteria such as file path, file name, or signer to exclude files from scanning. Reference:
Malware Protection Profiles
Configure a Windows Malware Protection Profile
PCDRA Study Guide

問題 #15
What is the purpose of the Unit 42 team?

- A. Unit 42 is responsible for threat research, malware analysis and threat hunting
- B. Unit 42 is responsible for the rapid deployment of Cortex XDR agents
- C. Unit 42 is responsible for the configuration optimization of the Cortex XDR server
- D. Unit 42 is responsible for automation and orchestration of products

答案：A

解題說明：
Unit 42 is the threat intelligence and response team of Palo Alto Networks. The purpose of Unit 42 is to collect and analyze the most up-to-date threat intelligence and apply it to respond to cyberattacks. Unit 42 is composed of world-renowned threat researchers, incident responders and security consultants who help organizations proactively manage cyber risk. Unit 42 is responsible for threat research, malware analysis and threat hunting, among other activities12.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . Unit 42 is not responsible for automation and orchestration of products. Automation and orchestration are capabilities that are provided by Palo Alto Networks products such as Cortex XSOAR, which is a security orchestration, automation and response platform that helps security teams automate tasks, coordinate actions and manage incidents3.
B . Unit 42 is not responsible for the configuration optimization of the Cortex XDR server. The Cortex XDR server is the cloud-based platform that provides detection and response capabilities across network, endpoint and cloud data sources. The configuration optimization of the Cortex XDR server is the responsibility of the Cortex XDR administrators, who can use the Cortex XDR app to manage the settings and policies of the Cortex XDR server4.
C . Unit 42 is not responsible for the rapid deployment of Cortex XDR agents. The Cortex XDR agents are the software components that are installed on endpoints to provide protection and visibility. The rapid deployment of Cortex XDR agents is the responsibility of the Cortex XDR administrators, who can use various methods such as group policy objects, scripts, or third-party tools to deploy the Cortex XDR agents to multiple endpoints5.
In conclusion, Unit 42 is the threat intelligence and response team of Palo Alto Networks that is responsible for threat research, malware analysis and threat hunting. By leveraging the expertise and insights of Unit 42, organizations can enhance their security posture and protect against the latest cyberthreats.
Reference:
About Unit 42: Our Mission and Team
Unit 42: Threat Intelligence & Response
Cortex XSOAR
Cortex XDR Pro Admin Guide: Manage Cortex XDR Settings and Policies
Cortex XDR Pro Admin Guide: Deploy Cortex XDR Agents

問題 #16
.....

- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.188ym.cc, 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, www.dahanyijing.com, www.fuxinwang.com, 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.maoyestudio.com, Disposable vapes

順便提一下，可以從雲存儲中下載PDFExamDumps XDR-Analyst考試題庫的完整版：https://drive.google.com/open?id=13lA9Of5dJ_9yM_F0dp_L_L9rRqIVrzUF