XDR-Analyst試験の準備方法｜最高のXDR-Analyst最新テスト試験｜一番優秀なPalo Alto Networks XDR Analystウェブトレーニング

Palo Alto NetworksのXDR-Analystの認定試験に受かることはIT業種に従事している皆さんの夢です。あなたは夢を実現したいのなら、プロなトレーニングを選んだらいいです。Jpshikenは専門的にIT認証トレーニング資料を提供するサイトです。Jpshikenはあなたのそばにいてさしあげて、あなたの成功を保障します。あなたの目標はどんなに高くても、Jpshikenはその目標を現実にすることができます。

Palo Alto Networks XDR-Analyst 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• アラートおよび検出プロセス: このドメインでは、アラートの種類とソースの識別、スコアリングとカスタム構成によるアラートの優先順位付け、インシデントの作成、データステッチング手法によるアラートのグループ化について説明します。
トピック 2	• エンドポイント セキュリティ管理: このドメインでは、エンドポイント防止プロファイルとポリシーの管理、エージェントの動作状態の検証、エージェントのバージョンとコンテンツの更新の影響の評価について説明します。
トピック 3	• インシデントの処理と対応: このドメインは、フォレンジック、因果関係の連鎖、タイムラインを使用したアラートの調査、セキュリティ インシデントの分析、自動修復などの対応アクションの実行、除外の管理に重点を置いています。
トピック 4	• データ分析: このドメインには、XQL 言語を使用したデータのクエリ、クエリ テンプレートとライブラリの利用、ルックアップ テーブルの操作、IOC の検索、Cortex XDR ダッシュボードの使用、データ保持とホスト インサイトの理解が含まれます。

>> XDR-Analyst最新テスト <<

認定する-100％合格率のXDR-Analyst最新テスト試験-試験の準備方法 XDR-Analystウェブトレーニング

JpshikenのXDR-Analyst試験トレントの合格率は、効果的で有用を証明する唯一の基準であるというのは常識です。 XDR-Analyst試験問題の利点についての一般的な考えは既にお持ちのことと思いますが、XDR-Analystガイドトレントの最大の強みである最高の合格率をお見せしたいと思います。 Palo Alto Networks統計によると、XDR-Analystガイドトレントのガイダンスに従って試験を準備したお客様の合格率は、98〜100％に達し、XDR-Analyst試験トレントを20〜30時間しか練習していません。

Palo Alto Networks XDR Analyst 認定 XDR-Analyst 試験問題 (Q71-Q76):

質問 # 71
Which of the following policy exceptions applies to the following description?
'An exception allowing specific PHP files'

- A. Support exception
- B. Process exception
- C. Local file threat examination exception
- D. Behavioral threat protection rule exception

正解：C

解説：
The policy exception that applies to the following description is B, local file threat examination exception. A local file threat examination exception is an exception that allows you to exclude specific files or folders from being scanned by the Cortex XDR agent for malware or threats. You can use this exception to prevent false positives, performance issues, or compatibility problems with legitimate files or applications. You can define the local file threat examination exception by file name, file path, file hash, or digital signer. For example, you can create a local file threat examination exception for specific PHP files by entering their file names or paths in the exception configuration. Reference:
Local File Threat Examination Exceptions
Create a Local File Threat Examination Exception

質問 # 72
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 allows to interfere with the pattern as soon as it is observed on the firewall.
- B. Cortex XDR Analytics does not interfere with the pattern as soon as it is observed on the endpoint.
- C. 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.
- D. Cortex XDR Analytics allows to interfere with the pattern as soon as it is observed on the endpoint.

正解：D

解説：
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]

質問 # 73
As a Malware Analyst working with Cortex XDR you notice an alert suggesting that there was a prevented attempt to open a malicious Word document. You learn from the WildFire report and AutoFocus that this document is known to have been used in Phishing campaigns since 2018. What steps can you take to ensure that the same document is not opened by other users in your organization protected by the Cortex XDR agent?

- A. Enable DLL Protection on all endpoints but there might be some false positives.
- B. No step is required because Cortex shares IOCs with our fellow Cyber Threat Alliance members.
- C. No step is required because the malicious document is already stopped.
- D. Create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity.

正解：D

解説：
The correct answer is B, create Behavioral Threat Protection (BTP) rules to recognize and prevent the activity. BTP rules are a powerful feature of Cortex XDR that allow you to define custom rules to detect and block malicious behaviors on endpoints. You

can use BTP rules to create indicators of compromise (IOCs) based on file attributes, registry keys, processes, network connections, and other criteria. By creating BTP rules, you can prevent the same malicious Word document from being opened by other users in your organization, even if the document has a different name or hash value. BTP rules are updated through content updates and can be managed from the Cortex XDR console.
The other options are incorrect for the following reasons:
A is incorrect because enabling DLL Protection on all endpoints is not a specific or effective way to prevent the malicious Word document. DLL Protection is a feature of Cortex XDR that prevents the loading of unsigned or untrusted DLLs by protected processes. However, this feature does not apply to Word documents or macros, and may cause false positives or compatibility issues with legitimate applications.
C is incorrect because relying on Cortex to share IOCs with the Cyber Threat Alliance members is not a proactive or sufficient way to prevent the malicious Word document. The Cyber Threat Alliance is a group of cybersecurity vendors that share threat intelligence and best practices to improve their products and services. However, not all vendors are members of the alliance, and not all IOCs are shared or updated in a timely manner. Therefore, you cannot assume that other users in your organization are protected by the same IOCs as Cortex XDR.
D is incorrect because doing nothing is not a responsible or secure way to prevent the malicious Word document. Even though Cortex XDR agent prevented the attempt to open the document on one endpoint, it does not mean that the document is no longer a threat. The document may still be circulating in your network or email system, and may be opened by other users who have different agent profiles or policies. Therefore, you should take steps to identify and block the document across your organization.
Reference:
Cortex XDR Agent Administrator Guide: Behavioral Threat Protection
Cortex XDR Agent Administrator Guide: DLL Protection
Palo Alto Networks: Cyber Threat Alliance

質問 # 74
Which function describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed?

- A. Isolation
- B. Quarantine
- C. Search & destroy
- D. Flag for removal

正解：B

解説：
The function that describes the removal of a specific file from its location on a local or removable drive to a protected folder to prevent the file from being executed is quarantine. Quarantine is a feature of Cortex XDR that allows you to isolate malicious or suspicious files from the endpoint and prevent them from running or spreading. You can quarantine files manually from the Cortex XDR console, or automatically based on the malware analysis profile or the remediation suggestions. When you quarantine a file, the Cortex XDR agent encrypts the file and moves it to a hidden folder under the agent installation directory. The file is also renamed with a random string and a .quarantine extension. You can view, restore, or delete the quarantined files from the Cortex XDR console. Reference:
Quarantine Files
Manage Quarantined Files

質問 # 75
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

正解：D

解説：
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

質問 # 76
......