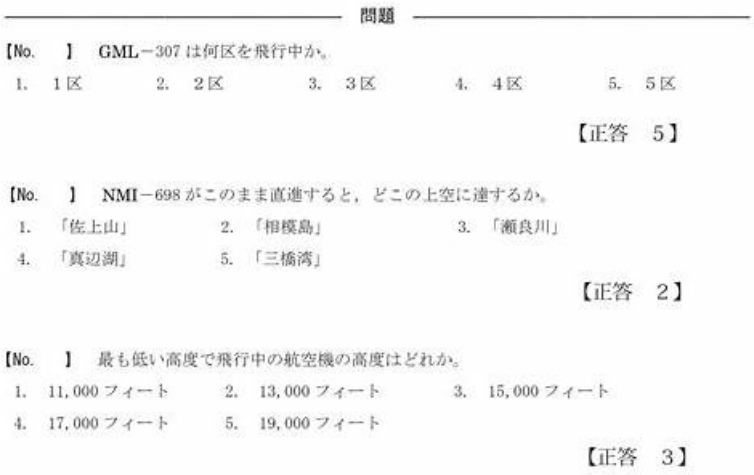
試験の準備方法-ユニークなXDR-Analystサンプル問題集試験-最新のXDR-Analyst日本語受験教科書



問題

【No. 】 GML－307は何区を飛行中か。

1. 1区　2. 2区　3. 3区　4. 4区　5. 5区

【正答 5】

【No. 】 NMI－698がこのまま直進すると，どこの上空に達するか。

1. 「佐上山」　2. 「相模島」　3. 「瀬良川」
4. 「真辺湖」　5. 「三橋湾」

【正答 2】

【No. 】 最も低い高度で飛行中の航空機の高度はどれか。

1. 11,000フィート　2. 13,000フィート　3. 15,000フィート
4. 17,000フィート　5. 19,000フィート

【正答 3】

It-PassportsのXDR-Analyst 問題集はあなたがXDR-Analyst認定試験に準備するときに最も欠かせない資料です。この問題集の価値は試験に関連する他の参考書の総合の価値に相当します。このアサーションは過言ではありません。It-Passportsの問題集を利用してからこのすべてが真であることがわかります。

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	• 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 2	• 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 3	• 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。
トピック 4	• 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。

>> XDR-Analystサンプル問題集 <<

信頼的なXDR-Analystサンプル問題集 & 合格スムーズXDR-Analyst日本語受験教科書 | ハイパスレートのXDR-Analyst過去問

人生はさまざまな試しがある、人生の頂点にかからないけど、刺激のない生活に変化をもたらします。あなたは我々社の提供する質高いPalo Alto Networks　XDR-Analyst問題集を使用して、試験に参加します。もし無事にXDR-Analyst試験に合格したら、あなたはもっと自信になって、更なる勇気でやりたいことをしています。

Palo Alto Networks XDR Analyst 認定 XDR-Analyst 試験問題 (Q92-Q97):

質問 # 92

When investigating security events, which feature in Cortex XDR is useful for reverting the changes on the endpoint?

- A. Remediation Automation
- B. Remediation Suggestions
- C. Automatic Remediation
- D. Machine Remediation

正解：B

解説：
When investigating security events, the feature in Cortex XDR that is useful for reverting the changes on the endpoint is Remediation Suggestions. Remediation Suggestions are a feature of Cortex XDR that provide you with recommended actions to undo the effects of malicious activity on your endpoints. You can view the remediation suggestions for each alert or incident in the Cortex XDR console, and decide whether to apply them or not. Remediation Suggestions can help you restore the endpoint to its original state, remove malicious files or processes, or fix registry or system settings. Remediation Suggestions are based on the forensic data collected by the Cortex XDR agent and the analysis performed by Cortex XDR. Reference:
Remediation Suggestions
Apply Remediation Suggestions

質問 # 93
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 automation and orchestration of products
- C. Unit 42 is responsible for the rapid deployment of Cortex XDR agents
- D. Unit 42 is responsible for the configuration optimization of the Cortex XDR server

正解：A

解説：
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

質問 # 94
Which statement regarding scripts in Cortex XDR is true?

- A. The level of risk is assigned to the script upon import.
- B. The script is run on the machine uploading the script to ensure that it is operational.
- C. Any version of Python script can be run.
- D. Any script can be imported including Visual Basic (VB) scripts.

正解：A

解説：
The correct answer is B, the level of risk is assigned to the script upon import. When you import a script to the Agent Script Library in Cortex XDR, you need to specify the level of risk associated with the script. The level of risk determines the permissions and restrictions for running the script on endpoints. The levels of risk are:
Low: The script can be run on any endpoint without requiring approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.
Medium: The script can be run on any endpoint, but requires approval from the Cortex XDR administrator. The script can also be used in remediation suggestions or automation actions.
High: The script can only be run on isolated endpoints, and requires approval from the Cortex XDR administrator. The script cannot be used in remediation suggestions or automation actions.
The other options are incorrect for the following reasons:
A is incorrect because not any version of Python script can be run in Cortex XDR. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. For example, the scripts must not exceed 64 KB in size, must not use external libraries or modules, and must not contain malicious or harmful code.
C is incorrect because not any script can be imported to Cortex XDR, including Visual Basic (VB) scripts. The scripts must be written in Python 2.7, and must follow the guidelines and limitations described in the Cortex XDR documentation. VB scripts are not supported by Cortex XDR, and will not run on the endpoints.
D is incorrect because the script is not run on the machine uploading the script to ensure that it is operational. The script is only validated for syntax errors and size limitations when it is imported to the Agent Script Library. The script is not executed or tested on the machine uploading the script, and the script may still fail or cause errors when it is run on the endpoints.
Reference:
Agent Script Library
Import a Script
Run Scripts on an Endpoint

質問 # 95
Which of the following best defines the Windows Registry as used by the Cortex XDR agent?

- A. a central system, available via the internet, for registering officially licensed versions of software to prove ownership
- B. a hierarchical database that stores settings for the operating system and for applications
- C. a ledger for maintaining accurate and up-to-date information on total disk usage and disk space remaining available to the operating system
- D. a system of files used by the operating system to commit memory that exceeds the available hardware resources. Also known as the "swap"

正解：B

解説：
The Windows Registry is a hierarchical database that stores settings for the operating system and for applications that run on Windows. The registry contains information, settings, options, and other values for programs and hardware installed on all versions of Microsoft Windows operating systems. The registry is organized into five main sections, called hives, each of which contains keys, subkeys, and values. The Cortex XDR agent uses the registry to store its configuration, status, and logs, as well as to monitor and control the endpoint's security features. The Cortex XDR agent also allows you to run scripts that can read, write, or delete registry keys and values on the endpoint. Reference:
Windows Registry - Wikipedia
Registry Operations

質問 # 96
An attacker tries to load dynamic libraries on macOS from an unsecure location. Which Cortex XDR module can prevent this attack?

- A. Hot Patch Protection

- B. DDL Security
- C. Dylib Hijacking
- D. Kernel Integrity Monitor (KIM)

正解：C

解説：
The correct answer is D. Dylib Hijacking. Dylib Hijacking, also known as Dynamic Library Hijacking, is a technique used by attackers to load malicious dynamic libraries on macOS from an unsecure location. This technique takes advantage of the way macOS searches for dynamic libraries to load when an application is executed. To prevent such attacks, Palo Alto Networks offers the Dylib Hijacking prevention capability as part of their Cortex XDR platform. This capability is designed to detect and block attempts to load dynamic libraries from unauthorized or unsecure locations1.
Let's briefly discuss the other options to provide a comprehensive explanation:
A . DDL Security: This is not the correct answer. DDL Security is not specifically designed to prevent dynamic library loading attacks on macOS. DDL Security is focused on protecting against DLL (Dynamic Link Library) hijacking on Windows systems2.
B . Hot Patch Protection: Hot Patch Protection is not directly related to preventing dynamic library loading attacks. It is a security feature that protects against runtime patching or modification of code in memory, often used by advanced attackers to bypass security measures3. While Hot Patch Protection is a valuable security feature, it is not directly relevant to the scenario described.
C . Kernel Integrity Monitor (KIM): Kernel Integrity Monitor is also not the correct answer. KIM is a module in Cortex XDR that focuses on monitoring and protecting the integrity of the macOS kernel. It detects and prevents unauthorized modifications to critical kernel components4. While KIM plays an essential role in overall macOS security, it does not specifically address the prevention of dynamic library loading attacks.
In conclusion, Dylib Hijacking is the Cortex XDR module that specifically addresses the prevention of attackers loading dynamic libraries from unsecure locations on macOS. By leveraging this module, organizations can enhance their security posture and protect against this specific attack vector.
Reference:
Endpoint Protection Modules
DDL Security
Hot Patch Protection
Kernel Integrity Monitor

質問 # 97
.....

Palo Alto NetworksのXDR-Analyst試験のために不安なのですか。弊社のソフトは買うたるかどうかまだ疑問がありますか。そうであれば、無料で弊社の提供するPalo Alto NetworksのXDR-Analystのデモをダウンロードしてみよう。我々提供する資料はあなたの需要だと知られています。あなたのPalo Alto NetworksのXDR-Analyst試験に参加する圧力を減ってあなたの効率を高めるのは我々の使命だと思います。

過去問 ❣ 検索するだけで□ www.goshiken.com □から[XDR-Analyst]を無料でダウンロードXDR-Analyst模擬試験問題集

- 検証するXDR-Analystサンプル問題集 - 合格スムーズXDR-Analyst日本語受験教科書 | 信頼できるXDR-Analyst過去問 □ ウェブサイト{ www.passtest.jp }を開き、□ XDR-Analyst □を検索して無料でダウンロードしてくださいXDR-Analyst資格準備
- 試験の準備方法-ユニークなXDR-Analystサンプル問題集試験-完璧なXDR-Analyst日本語受験教科書 □（ www.goshiken.com ）の無料ダウンロード▶ XDR-Analyst ◀ページが開きますXDR-Analyst受験練習参考書
- 一番優秀XDR-Analyst丨権威のあるXDR-Analystサンプル問題集試験丨試験の準備方法Palo Alto Networks XDR Analyst日本語受験教科書 □⇛ www.japancert.com ⇚に移動し、▷ XDR-Analyst ◁を検索して無料でダウンロードしてくださいXDR-Analyst最新受験攻略
- academy.dfautomation.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.mixcloud.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.medicalup.net, behindvlsi.com, www.stes.tyc.edu.tw, whatoplay.com, Disposable vapes