Palo Alto Networks XDR-Analyst関連日本語版問題集 & XDR-Analyst全真問題集

ShikenPASSのPalo Alto NetworksのXDR-Analyst問題集を買う前に、一部の問題と解答を無料に試用することができます。そうすると、ShikenPASSのPalo Alto NetworksのXDR-Analystトレーニング資料の品質をよく知っています。ShikenPASSのPalo Alto NetworksのXDR-Analyst問題集は絶対あなたの最良の選択です。

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	• 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.
トピック 2	• 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.
トピック 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.
トピック 4	• 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.

>> Palo Alto Networks XDR-Analyst関連日本語版問題集 <<

Palo Alto Networks XDR-Analyst全真問題集 & XDR-Analyst基礎問題集

弊社のPalo Alto Networks問題集を購入するなら、あなたは必ず後悔しません。我々は自分の商品に自信があります。お客様は我々の商品を利用したら、XDR-Analyst試験に合格できます。もしXDR-Analyst試験に落ちるなら、我々は返金できます。それとも、お客様はほかの試験に対応する問題集を交換するのを選ぶことができます。

Palo Alto Networks XDR Analyst 認定 XDR-Analyst 試験問題 (Q55-Q60):

質問 # 55
What is the purpose of targeting software vendors in a supply-chain attack?

- A. to take advantage of a trusted software delivery method.
- B. to steal users' login credentials.

- C. to report Zero-day vulnerabilities.
- D. to access source code.

正解：A

解説：
A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain. Software supply chain attacks inject malicious code into an application in order to infect all users of an app. The purpose of targeting software vendors in a supply-chain attack is to take advantage of a trusted software delivery method, such as an update or a download, that can reach a large number of potential victims. By compromising a software vendor, an attacker can bypass the security measures of the downstream organizations and gain access to their systems, data, or networks. Reference: What Is a Supply Chain Attack? - Definition, Examples & More | Proofpoint US What Is a Supply Chain Attack? - CrowdStrike What Is a Supply Chain Attack? | Zscaler What Is a Supply Chain Attack? Definition, Examples & Prevention

質問 # 56
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. Kernel Integrity Monitor (KIM)
- D. Dylib Hijacking

正解：D

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 # 57
What is the maximum number of agents one Broker VM local agent applet can support?

- A. 10,000
- B. 5,000
- C. 15,000
- D. 20,000

正解：A

解説：
The Broker VM is a virtual machine that you can deploy in your network to provide various services and functionalities to the Cortex XDR agents. One of the services that the Broker VM offers is the Local Agent Settings applet, which allows you to configure the agent proxy, agent installer, and content caching settings for the agents. The Local Agent Settings applet can support a maximum number of 10,000 agents per Broker VM. If you have more than 10,000 agents in your network, you need to deploy additional Broker VMs and distribute the load among them. Reference:
Broker VM Overview: This document provides an overview of the Broker VM and its features, requirements, and deployment options.
Configure the Broker VM: This document explains how to install, set up, and configure the Broker VM in an ESXi environment.
Manage Broker VM from the Cortex XDR Management Console: This document describes how to activate and manage the Broker VM applets from the Cortex XDR management console.

質問 # 58
What should you do to automatically convert leads into alerts after investigating a lead?

- A. Lead threats can't be prevented in the future because they already exist in the environment.
- B. Create BIOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.
- C. Build a search query using Query Builder or XQL using a list of IOCs.
- D. Create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting.

正解：D

解説：
To automatically convert leads into alerts after investigating a lead, you should create IOC rules based on the set of the collected attribute-value pairs over the affected entities concluded during the lead hunting. IOC rules are used to detect known threats based on indicators of compromise (IOCs) such as file hashes, IP addresses, domain names, etc. By creating IOC rules from the leads, you can prevent future occurrences of the same threats and generate alerts for them. Reference:
PCDRA Study Guide, page 25
Cortex XDR 3: Handling Cortex XDR Alerts, section 3.2
Cortex XDR Documentation, section "Create IOC Rules"

質問 # 59
Where would you view the WildFire report in an incident?

- A. under Response --> Action Center
- B. under the gear icon --> Agent Audit Logs
- C. on the HUB page at apps.paloaltonetworks.com
- D. next to relevant Key Artifacts in the incidents details page

正解：D

解説：
To view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. A key artifact is a piece of evidence that is associated with an alert or an incident, such as a file hash, a registry key, an IP address, a domain name, or a full path. If a key artifact is related to a WildFire analysis, you will see a WildFire icon next to it, indicating that there is a WildFire report available for that artifact. You can click on the WildFire icon to view the report, which will show you the detailed information about the artifact, such as the verdict, the behavior, the severity, the signatures, and the screenshots12.
Let's briefly discuss the other options to provide a comprehensive explanation:
B . under Response --> Action Center: This is not the correct answer. The Action Center is a feature that allows you to create and manage actions that you can perform on your endpoints, such as isolating, scanning, collecting files, or executing scripts. The Action Center does not show you the WildFire reports for the incidents, but it can help you to remediate the incidents by applying the appropriate actions3.
C . under the gear icon --> Agent Audit Logs: This is not the correct answer. The Agent Audit Logs are logs that show you the activities and events that occurred on the Cortex XDR agents, such as installation, upgrade, connection, policy update, or prevention. The Agent Audit Logs do not show you the WildFire reports for the incidents, but they can help you to troubleshoot the agent issues or verify the agent status4.

D . on the HUB page at apps.paloaltonetworks.com: This is not the correct answer. The HUB page is a web portal that allows you to access and manage your Palo Alto Networks applications, such as Cortex XDR, Cortex XSOAR, Prisma Cloud, or AutoFocus. The HUB page does not show you the WildFire reports for the incidents, but it can help you to navigate to the different applications or view the notifications and alerts5.
In conclusion, to view the WildFire report in an incident, you need to go to the incident details page and look for the relevant key artifacts that are related to the WildFire analysis. By viewing the WildFire report, you can gain more insights and context about the incident and the artifact.
Reference:
View Incident Details
View WildFire Reports
Action Center
Agent Audit Logs
HUB

質問 # 60
.....

Palo Alto NetworksのXDR-Analyst認定試験に受かるためにがんばって勉強していれば、ShikenPASSはあなたにヘルプを与えます。ShikenPASS が提供したPalo Alto NetworksのXDR-Analyst問題集は実践の検査に合格したもので、最も良い品質であなたがPalo Alto NetworksのXDR-Analyst認定試験に合格することを保証します。

XDR-Analyst全真問題集: https://www.shikenpass.com/XDR-Analyst-shiken.html

- 更新するXDR-Analyst関連日本語版問題集試験-試験の準備方法-権威のあるXDR-Analyst全真問題集 □ ☀ jp.fast2test.com □☀□を開いて☀ XDR-Analyst □☀□を検索し、試験資料を無料でダウンロードしてくださいXDR-Analyst復習時間
- XDR-Analyst合格率書籍 □ XDR-Analyst全真模擬試験 □ XDR-Analyst全真模擬試験 □ ➡ www.goshiken.com □□□サイトにて最新➽ XDR-Analyst □問題集をダウンロードXDR-Analyst最新受験攻略
- XDR-Analystサンプル問題集 ↕ XDR-Analyst参考書 □ XDR-Analystサンプル問題集 □ URL ➡ www.mogiexam.com □□□をコピーして開き、➤ XDR-Analyst □を検索して無料でダウンロードしてくださいXDR-Analyst復習時間
- XDR-Analystテスト参考書 □ XDR-Analystトレーニング ☑ XDR-Analyst受験資料更新版 □□ ➠ XDR-Analyst □□を無料でダウンロード「 www.goshiken.com 」ウェブサイトを入力するだけXDR-Analystサンプル問題集
- もしあなたはまだPalo Alto NetworksのXDR-Analyst試験に合格するのために悩まれば □□ www.japancert.com □で▶ XDR-Analyst ◀を検索し、無料でダウンロードしてくださいXDR-Analyst最新テスト
- XDR-Analyst模試エンジン □ XDR-Analyst最新受験攻略 □ XDR-Analyst過去問無料 □ ウェブサイト「 www.goshiken.com 」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認証pdf資料
- XDR-Analyst最新テスト □ XDR-Analyst復習時間 □ XDR-Analyst合格率書籍 □ 今すぐ□ www.goshiken.com □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試験過去問
- XDR-Analyst試験の準備方法｜信頼的なXDR-Analyst関連日本語版問題集試験｜有効的なPalo Alto Networks XDR Analyst全真問題集 ✔□ ➥ XDR-Analyst □の試験問題は □ www.goshiken.com □で無料配信中XDR-Analyst受験資料更新版
- XDR-Analyst最新テスト □ XDR-Analystサンプル問題集 □ XDR-Analystテスト参考書 □ ➥ www.mogiexam.com □から⇒ XDR-Analyst ⇐を検索して、試験資料を無料でダウンロードしてくださいXDR-Analystトレーニング
- もしあなたはまだPalo Alto NetworksのXDR-Analyst試験に合格するのために悩まれば □ ウェブサイト✔ www.goshiken.com □✔□から□ XDR-Analyst □を開いて検索し、無料でダウンロードしてくださいXDR-Analystトレーニング
- XDR-Analyst試験の準備方法｜ハイパスレートのXDR-Analyst関連日本語版問題集試験｜素敵なPalo Alto Networks XDR Analyst全真問題集 □ ⇒ www.mogiexam.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技術内容
- 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.stes.tyc.edu.tw, ycs.instructure.com, 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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes