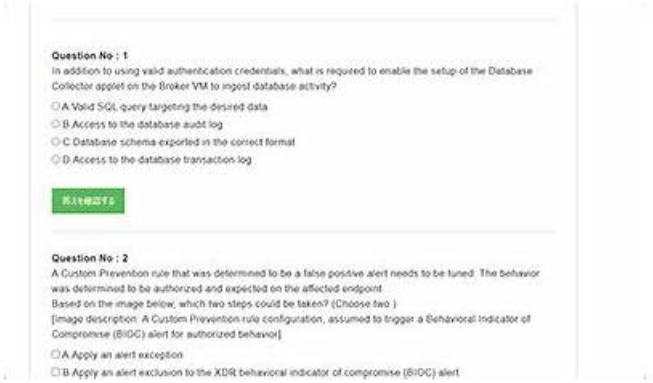
更新するXDR-Analyst日本語版問題集 &合格スムーズXDR-Analyst資格模擬 |一番優秀なXDR-Analyst参考書内容


Question No : 1
In addition to using valid authentication credentials, what is required to enable the setup of the Database Collector applet on the Broker VM to ingest database activity?
A Valid SQL query targeting the desired data
B Access to the database audit log
C Database schema exported in the correct format
D Access to the database transaction log
Question No : 2
A Custom Prevention rule that was determined to be a false positive alert needs to be tuned. The behavior was determined to be authorized and expected on the affected endpoint.
Based on the image below, which two steps could be taken? (Choose two.)
[image description: A Custom Prevention rule configuration, assumed to trigger a Behavioral Indicator of Compromise (BIOC) alert for authorized behavior.]
A Apply an alert exception
B Apply an alert exclusion to the XDR behavioral indicator of compromise (BIOC) alert

P.S. CertJukenがGoogle Driveで共有している無料かつ新しいXDR-Analystダンプ：https://drive.google.com/open?id=1ZaE94T9JDv8kc2QUQj9J5HcdEAstcKkH

CertJukenのXDR-Analystスタディガイドには、さまざまなニーズを満たすことができる3つの形式があります。PDFバージョン、ソフトウェアバージョン、オンラインバージョンです。 PDFバージョンを選択した場合は、XDR-Analyst学習資料をダウンロードして、どこでも学習できるように印刷できます。新しいバージョンがリリースされた場合は、電子メールボックスへの新しいリンクが送信され、再度ダウンロードできます。ソフトウェアバージョンのXDR-Analyst試験教材を使用すると、実際のPalo Alto Networks XDR Analyst試験と同じような環境で練習できます。また、XDR-Analyst実践ガイドのAPPバージョンは、あらゆる種類の電子機器で利用できます。

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	• Endpoint Security Management:
トピック 2	• 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 3	• 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.
トピック 4	• 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 5	• 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.

>> XDR-Analyst日本語版問題集 <<

ハイパスレート-権威のあるXDR-Analyst日本語版問題集試験-試験の準

備方法XDR-Analyst資格模擬

一般的には、IT技術会社ではPalo Alto Networks XDR-Analyst資格認定を持つ職員の給料は持たない職員の給料に比べ、15%より高いです。これなので、IT技術職員としてのあなたはCertJukenのPalo Alto Networks XDR-Analyst問題集デモを参考し、試験の準備に速く行動しましょう。我々社はあなたがPalo Alto Networks XDR-Analyst試験に一発的に合格するために、最新版の備考資料を提供します。

Palo Alto Networks XDR Analyst 認定 XDR-Analyst 試験問題 (Q66-Q71):

質問 # 66
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 unknown.
- 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 malware.

正解：A

解説：
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

質問 # 67
Which Exploit Prevention Module (EPM) provides better entropy for randomization of memory locations?

- A. UASLR
- B. JIT Mitigation
- C. DLL Security
- D. Memory Limit Heap spray check

正解：A

解説：
UASLR stands for User Address Space Layout Randomization, which is a feature of Exploit Prevention Module (EPM) that provides better entropy for randomization of memory locations. UASLR adds entropy to the base address of the executable image and the heap, making it harder for attackers to predict the memory layout of a process. UASLR is enabled by default for all processes, but can be disabled or customized for specific applications using the EPM policy settings. Reference:
Exploit Prevention Module (EPM) entropy randomization memory locations
Exploit protection reference

質問 # 68
A file is identified as malware by the Local Analysis module whereas WildFire verdict is Benign, Assuming WildFire is accurate. Which statement is correct for the incident?

- A. It is true positive.
- B. It is true negative.
- C. It is false positive.

- D. It is a false negative.

正解：C

解説：
A false positive is a situation where a file or activity is incorrectly identified as malicious by a security tool, when in fact it is benign or harmless. A false positive can cause unnecessary alerts, disruptions, or remediation actions, and reduce the confidence and efficiency of the security system. In this question, a file is identified as malware by the Local Analysis module, whereas WildFire verdict is Benign, assuming WildFire is accurate. This means that the Local Analysis module has made a mistake and flagged a legitimate file as malicious, while WildFire has correctly determined that the file is safe. Therefore, this is an example of a false positive. The Local Analysis module is a feature of the Cortex XDR agent that uses a static set of pattern-matching rules and a statistical model to determine if an unknown file is likely to be malware. The Local Analysis module can provide a fast and offline verdict for files that are not yet analyzed by WildFire, but it is not as accurate or comprehensive as WildFire, which uses dynamic analysis and machine learning to examine the behavior and characteristics of files in a sandbox environment. WildFire verdicts are considered more reliable and authoritative than Local Analysis verdicts, and can override them in case of a discrepancy. Therefore, if a file is identified as malware by the Local Analysis module, but as Benign by WildFire, the WildFire verdict should be trusted and the Local Analysis verdict should be disregarded123 Reference:
False positive (security) - Wikipedia
Local Analysis
WildFire Overview

質問 # 69
Cortex XDR is deployed in the enterprise and you notice a cobalt strike attack via an ongoing supply chain compromise was prevented on 1 server. What steps can you take to ensure the same protection is extended to all your servers?

- A. Create IOCs of the malicious files you have found to prevent their execution.
- B. Conduct a thorough Endpoint Malware scan.
- C. Enable Behavioral Threat Protection (BTP) with cytool to prevent the attack from spreading.
- D. Enable DLL Protection on all servers but there might be some false positives.

正解：A

解説：
The best step to ensure the same protection is extended to all your servers is to create indicators of compromise (IOCs) of the malicious files you have found to prevent their execution. IOCs are pieces of information that indicate a potential threat or compromise on an endpoint, such as file hashes, IP addresses, domain names, or registry keys. You can create IOCs in Cortex XDR to block or alert on any file or network activity that matches the IOCs. By creating IOCs of the malicious files involved in the cobalt strike attack, you can prevent them from running or spreading on any of your servers.
The other options are not the best steps for the following reasons:
A is not the best step because conducting a thorough Endpoint Malware scan may not detect or prevent the cobalt strike attack if the malicious files are obfuscated, encrypted, or hidden. Endpoint Malware scan is a feature of Cortex XDR that allows you to scan endpoints for known malware and quarantine any malicious files found. However, Endpoint Malware scan may not be effective against unknown or advanced threats that use evasion techniques to avoid detection.
B is not the best step because enabling DLL Protection on all servers may cause some false positives and disrupt legitimate applications. DLL Protection is a feature of Cortex XDR that allows you to block or alert on any DLL loading activity that matches certain criteria, such as unsigned DLLs, DLLs loaded from network locations, or DLLs loaded by specific processes. However, DLL Protection may also block or alert on benign DLL loading activity that is part of normal system or application operations, resulting in false positives and performance issues.
C is not the best step because enabling Behavioral Threat Protection (BTP) with cytool may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection. Behavioral Threat Protection is a feature of Cortex XDR that allows you to block or alert on any endpoint behavior that matches certain patterns, such as ransomware, credential theft, or lateral movement. Cytool is a command-line tool that allows you to configure and manage the Cortex XDR agent on the endpoint. However, Behavioral Threat Protection may not prevent the attack from spreading if the malicious files are already on the endpoints or if the attack uses other methods to evade detection, such as encryption, obfuscation, or proxy servers.
Reference:
Create IOCs
Scan an Endpoint for Malware
DLL Protection
Behavioral Threat Protection

質問 # 70
Which of the following protection modules is checked first in the Cortex XDR Windows agent malware protection flow?

- A. Behavioral Threat Protection
- B. Restriction Policy
- C. Child Process Protection
- D. Hash Verdict Determination

正解：D

解説：
The first protection module that is checked in the Cortex XDR Windows agent malware protection flow is the Hash Verdict Determination. This module compares the hash of the executable file that is about to run on the endpoint with a list of known malicious hashes stored in the Cortex XDR cloud. If the hash matches a malicious hash, the agent blocks the execution and generates an alert. If the hash does not match a malicious hash, the agent proceeds to the next protection module, which is the Restriction Policy1.
The Hash Verdict Determination module is the first line of defense against malware, as it can quickly and efficiently prevent known threats from running on the endpoint. However, this module cannot protect against unknown or zero-day threats, which have no known hash signature. Therefore, the Cortex XDR agent relies on other protection modules, such as Behavioral Threat Protection, Child Process Protection, and Exploit Protection, to detect and block malicious behaviors and exploits that may occur during the execution of the file1.
Reference:
Palo Alto Networks Cortex XDR Documentation, File Analysis and Protection Flow

質問 # 71
.....

何千人ものお客様がXDR-Analyst試験に合格し、関連する認定を取得しています。その後、XDR-Analyst試験トレントはすべて、当社のWebサイトで購入されました。業界の動向に加えて、XDR-Analystテストガイドは、過去の多くの資料の厳密な分析によって書かれています。 XDR-Analyst学習教材の言語は理解しやすいものであり、厳密な学習を行った場合のみ、最新の専門的なXDR-Analyst学習教材を作成します。私たちはあなたに最高のサービスを提供し、あなたが満足できることを願っています。

でダウンロード【 www.goshiken.com 】で検索するだけXDR-Analystテスト対策書

- emiliahmit570601.iamthewiki.com, heidifwpp271453.therainblog.com, thefairlist.com, laytnhqmi020776.mywikiparty.com, yesbookmarks.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, keybookmarks.com, www.stes.tyc.edu.tw, jessejrej176288.cosmicwiki.com, barbaramwxi747445.bloggerchest.com, Disposable vapes

P.S. CertJukenがGoogle Driveで共有している無料かつ新しいXDR-Analystダンプ：https://drive.google.com/open?id=1ZaE94T9JDv8kc2QUQj9J5HcdEAstcKkH