Exam : **CAS-005-JPN**

Title : CompTIA SecurityX Certification Exam (CAS-005日本語版)

Vendor : CompTIA

Version : DEMO

QUESTION NO: 1
ある企業では、他のシステムと比較してタイムスタンプが変更されたログを発見しました。セキュリティチームは、インシデント対応のためのログ記録と監査を改善することを決定しました。この目標を最も効果的に達成するために、セキュリティチームは以下のどれを実施すべきでしょうか？
A. ファイル監視ツールを SIEM と統合します。
B. ログ ソリューションを変更し、既存の SIEM と統合します。
C. ログの取り込みのみを許可する中央ログサーバーを実装します。
D. 24
時間ごとにログをローテーションしてバックアップし、バックアップを暗号化します。
Answer: C
Explanation:
A central logging server ensures logs are collected in a tamper-proof manner and only ingested (not modified). This prevents attackers from altering logs locally.
Key concepts:
Logs should be centrally stored to prevent tampering.
Enabling log forwarding to a secure SIEM improves integrity.
Other options:
A (File monitoring tool) helps detect file changes but doesn't prevent log tampering.
B (Changing log solutions) does not inherently improve security.
D (Log rotation and encryption) is best practice but does not prevent modification before transmission.
Reference: CASP+ CAS-005 Official Study Guide -Security Operations and Logging

QUESTION NO: 2
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実施しています。標準ユーザーとしてテストを行ったところ、以下のエラーログが表示されました。
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
後でもう一度リクエストをお試しください。
アナリストの調査結果と潜在的な対策を最も適切に説明しているのは、次のうちどれですか？
A.
調査結果は、安全でない参照を示しています。すべての潜在的なユーザー入力は適切にサニタイズする必要があります。
B.調査結果はSQLインジェクションを示しています。データベースのアップグレードが必要です。
C. 調査結果は、安全でないプロトコルを示しています。すべてのクッキーは HttpOnly としてマークする必要があります。
D. 情報漏洩の疑いがあります。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。
Answer: D

QUESTION NO: 3
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.第三者リスクレビュー
B.事業影響分析
C.危機管理計画
D. インシデント対応プレイブック
Answer: B

QUESTION NO: 4
ある組織が、複数のアプリケーションからのレコードを一元管理する新しいデータレイクを導入しようとしています。設計段階で、セキュリティアーキテクトは以下の要件を特定しました。
* データの感度レベルが異なります。
* 認証後、ステートレスなAPI呼び出しを通じてデータにアクセスする必要があります。
* ユーザーによってアクセスできるデータセットは異なります。
これらの要件を最適に満たすために、建築家は以下のうちどれを実施すべきでしょうか？
A. CASB
B. EAP-TLS を使用した 802.1X
C. ディレクトリサービス
D. OpenID Connect
Answer: D

QUESTION NO: 5
最高情報セキュリティ責任者（CISO）は、企業の現在のデータ廃棄手順ではデータが残留してしまう可能性があることを懸念しています。同社はSSDのみを使用しています。CISOの懸念を考慮すると、SSDを廃棄する最も安全な方法は次のうちどれでしょうか？
A. 消磁
B. 上書き
C. シュレッディング
D. 書式設定
E. 焼却
Answer: E
Explanation:
For SSDs,incinerationis considered the most secure method of physical destruction, ensuring no data remanence. SSDs store data differently compared to traditional spinning disks, making degaussing ineffective.
Overwriting and formatting may not reliably erase all storage cells due to wear-leveling technologies.
Shredding may work if the granularity is extremely fine, but incineration guarantees complete

destruction beyond recovery.
Reference:CompTIA SecurityX CAS-005, Domain 2.0: Apply secure media sanitization methods appropriate for device types such as SSDs.

QUESTION NO: 6
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	10.200.4.139/24	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。
Answer: C
Explanation:
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.

QUESTION NO: 7
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

Answer: D

Explanation:

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.

QUESTION NO: 8

ゲストネットワークに接続する際に、ユーザーはキャプティブペタル（花びら）に表示される利用規約に同意する必要があります。最近、ネットワークに接続した後にインターネットにアクセスできないという報告がユーザーから寄せられています。あるネットワークエンジニアは、次のような状況に気づきました。

* ユーザーはキャプティブ ポータルにリダイレクトされる必要があります。
* MotivePortalはTl. S 1 2で実行されます
* 新しいブラウザバージョンでは、回避できないセキュリティエラーが発生します
* 特定のウェブサイトは予期しないリダイレクトを引き起こします

この行動を説明する可能性のあるのは次のどれでしょうか?

A. キャプティブポータルでサポートされているTLS暗号は非推奨です

B. HSTS 設定の採用が急速に増加しています。

C. 許可されたトラフィックルールにより、NIPS
が正当なトラフィックをドロップしています

D. 攻撃者はサプリカントを悪意のある双子の WLAN にリダイレクトしています。

Answer: A

Explanation:

The most likely explanation for the issues encountered with the captive portal is that the TLS ciphers supported by the captive portal are deprecated. Here's why:

TLS Cipher Suites: Modern browsers are continuously updated to support the latest security standards and often drop support for deprecated and insecure cipher suites. If the captive portal uses outdated TLS ciphers, newer browsers may refuse to connect, causing security errors.

HSTS and Browser Security: Browsers with HTTP Strict Transport Security (HSTS) enabled will not allow connections to sites with weak security configurations. Deprecated TLS ciphers would cause these browsers to block the connection.

References:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations OWASP Transport LayerProtection Cheat Sheet By updating the TLS ciphers to modern, supported ones, the security engineer can ensure compatibility with newer browser versions and resolve the connectivity issues reported by users.

QUESTION NO: 9
セキュリティ管理者が特定のOSベンチマークに対するギャップ評価を実施しています。このベンチマークでは、エンドポイントに以下の構成を適用する必要があります。
* フルディスク暗号化
ホストベースのファイアウォール
* 時刻同期
* パスワードポリシー
* アプリケーションがリスト掲載を許可する
* ゼロトラストアプリケーションへのアクセス
以下の解決策のうち、要件に最も適しているのはどれですか？(2つ選択してください。)
A. CASB
B. SBoM
C. SCAP
D. SASE
E. HIDS
Answer: C D
Explanation:
To address the specific OS benchmark configurations, the following solutions are most appropriate:
C). SCAP (Security Content Automation Protocol): SCAP helps in automating vulnerability management and policy compliance, including configurations like full disk encryption, host-based firewalls, and password policies.
D). SASE (Secure Access Service Edge): SASE provides a framework for Zero Trust network access and application allow listing, ensuring secure and compliant access to applications and data.
These solutions together cover the comprehensive security requirements specified in the OS benchmark, ensuring a robust security posture for endpoints.
References:
CompTIA SecurityX Study Guide: Discusses SCAP and SASE as part of security configuration management and Zero Trust architectures.
NIST Special Publication 800-126, " The Technical Specification for the Security Content Automation Protocol (SCAP) " : Details SCAP ' s role in security automation.
" Zero Trust Networks: Building Secure Systems in Untrusted Networks " by Evan Gilman and Doug Barth:
Covers the principles of Zero Trust and how SASE can implement them.
By implementing SCAP and SASE, the organization ensures that all the specified security configurations are applied and maintainedeffectively.

QUESTION NO: 10
ある組織は最近、組織環境における情報セキュリティ管理体制の監査を第三者機関に依頼しました。監査結果を検討した後、最高情報セキュリティ責任者(CISO)は、ネットワークセキュリティのための包括的な防御戦略の予算を承認しました。CISOが追加予算を承認した最も可能性の高い理由は次のうちどれでしょうか？
A. 他の部署には未使用の予算があり、それがITセキュリティに振り替えられました。
B.潜在顧客からセキュリティコンプライアンスレポートを求める声がますます増えている。
C.
以前のネットワークアーキテクチャには、簡単に回避できる制御機能が含まれていました。
D.監査担当者は、PCI DSS自己評価アンケートで低いスコアを報告しました。
Answer: C
Explanation:
The most likely driver for approving additional network security budget is that the audit revealed that the existing architecture contained security controls that could be easily bypassed. This indicates fundamental weaknesses in defense-in-depth and suggests that attackers could gain access to sensitive systems or data despite the presence of controls.
Option A (unused budgets) is not a strategic reason for approving security investment. Option B (compliance reports requested by customers) may influence investment in compliance initiatives, but it does not explain the need for an in-depth defense architecture. Option D (PCI DSS low score) is a compliance-specific issue but would not, on its own, drive a broad architectural budget approval unless PCI was the only focus.
Security audits often uncover systemic flaws-such as flat networks, insufficient segmentation, or single points of failure-that create the conditions for bypassing controls. Addressing these issues requires rearchitecting the environment, introducing layered defenses, and strengthening monitoring capabilities, all of which demand significant budget. Thus, option C aligns with the decision to invest in robust defense-in-depth strategies.

QUESTION NO: 11
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
Answer: C
Explanation:
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.

QUESTION NO: 12
ネットワーク設計者がすべての VPN
トンネルで前方秘匿性を有効にする理由を最もよく説明しているのは次のうちどれですか?
A. このプロセスは、ハードウェア
アクセラレーションによる暗号化を有効にするための要件です。
B. このプロセスにより、攻撃者が暗号解読を行う成功率が低下します。
C. ビジネス要件では、機密性が重要な成功要因であるとされています。
D. 最新の暗号化プロトコルでは、このプロセスを使用の前提条件として挙げています。
Answer: B
Explanation:
Forward secrecy (also known as perfect forward secrecy, PFS) ensures that session keys used in a VPN tunnel are ephemeral, meaning that even if an attacker compromises a long-term private key, past sessions cannot be decrypted. According to the CompTIA SecurityX CAS-005 study guide (Domain 3: Cybersecurity Technology, 3.1), enabling forward secrecy on VPN tunnels reduces the risk of cryptanalysis by ensuring that each session's encryption key is unique and not derived from a single compromised key. This directly mitigates the impact of attacks like key theft or future decryption attempts.
Option A:Forward secrecy is not required for hardware-accelerated cryptography, which depends on processor capabilities, not key management.
Option C:While confidentiality is important, this is too vague and does not specifically explain why forward secrecy is chosen.
Option D:Modern protocols (e.g., TLS 1.3, IPsec with ECDHE) support forward secrecy but donot mandate it as a prerequisite for use.
Option B:This is the most precise, as forward secrecy directly reduces the success of cryptanalysis by limiting the scope of key compromise.
Reference:
CompTIA SecurityX CAS-005 Official Study Guide, Domain 3: Cybersecurity Technology, Section 3.1: " Explain cryptographic techniques, including perfect forward secrecy. " CAS-005 Exam Objectives, 3.1: " Evaluate the impact of cryptographic configurations on security. "

QUESTION NO: 13
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. EDR
B. HIDS
C. Webアプリケーションファイアウォール
D. 中央ログ
E. ホストベースのファイアウォール

F. TPM

Answer: A D

QUESTION NO: 14

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

Answer: A

Explanation:

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

QUESTION NO: 15

クラウドエンジニアは、以下の点について適切な解決策を特定する必要があります。

* 内部および外部のクラウド リソースへの安全なアクセスを提供する。

* トンネルの分岐による交通の流れをなくす。

*IDおよびアクセス管理機能を有効にする。

以下の解決策のうち、最も適切なものはどれですか？(2つ選択してください。)

A. フェデレーション

B. マイクロセグメンテーション

C. CASB

D. PAM

E. SD-WAN

F. SASE

Answer: C F

Explanation:

To provide secure access tointernal and external cloud resources, eliminate split-tunnel traffic flows, and enable identity and access management capabilities, the most appropriate

solutions are CASB (Cloud Access Security Broker) and SASE (Secure Access Service Edge).
Why CASB and SASE?
CASB (Cloud Access Security Broker):
Secure Access: CASB solutions provide secure access to cloud resources by enforcing security policies and monitoring user activities.
Identity and Access Management: CASBs integrate with identity and access management (IAM) systems to ensure that only authorized users can access cloud resources.
Visibility and Control: They offer visibility into cloud application usage and control over data sharing and access.
SASE (Secure Access Service Edge):
Eliminate Split-Tunnel Traffic: SASE integrates network security functions with WAN capabilities to ensure secure access without the need for split-tunnel configurations.
Comprehensive Security: SASE provides a holistic security approach, including secure web gateways, firewalls, and zero trust network access (ZTNA).
Identity-Based Access: SASE leverages IAM to enforce access controls based on user identity and context.
Other options, while useful, do not comprehensively address all the requirements:
A). Federation: Useful for identity management but does not eliminate split-tunnel traffic or provide comprehensive security.
B). Microsegmentation: Enhances security within the network but does not directly address secure access to cloud resources or split-tunnel traffic.
D). PAM (Privileged Access Management): Focuses on managing privileged accounts and does not provide comprehensive access control for internal and external resources.
E). SD-WAN: Enhances WAN performance but does not inherently provide the identity and access management capabilities or eliminate split-tunnel traffic.
References:
CompTIA SecurityX Study Guide
" CASB: Cloud Access Security Broker, " Gartner Research

QUESTION NO: 16
ある企業が、インバウンド接続に関連する不審なアクティビティを検出しました。セキュリティ検出ツールではこのアクティビティを分類できません。この課題を克服するために、企業が最適なソリューションは次のうちどれですか？
A. インタラクティブなハニーポットを実装します。
B. ネットワーク トラフィックを既知の IoC にマップします。
C. ダークウェブを監視します。
D. UEBA を実装します。
Answer: A
Explanation:
The best solution is to implement an interactive honeypot (A). Honeypots are decoy systems designed to attract and observe adversary behavior in real time. When security tools cannot categorize suspicious inbound traffic, a honeypot provides an isolated environment where the suspicious activity can be redirected and monitored without risking production systems. By deploying an interactive honeypot, analysts can study attacker tactics, techniques, and

procedures (TTPs), extract Indicators of Compromise (IoCs), and improve defensive controls. Option B (mapping to known IoCs) fails because the activity cannot be categorized, implying it is novel or not yet identified in threat intelligence feeds. Option C (monitoring the dark web) provides intelligence about potential threats but does not address real-time inbound suspicious activity. Option D (UEBA) focuses on analyzing user and entity behaviors but is less effective for categorizing inbound external traffic.
By using honeypots, organizations gain visibility into new, unknown, or advanced attack techniques, which helps improve detection capabilities, enrich threat intelligence, and strengthen incident response.

QUESTION NO: 17
ある組織が、資本計画と報告機能をサポートする社内ソフトウェアプラットフォームを開発しています。製品マネージャーは、ロールベースのアクセス制御と監査 / ログ機能に加えて、データのアーカイブと変更不可能なバックアップに関する要件も考慮する必要があります。この要件に関連する組織上の考慮事項として最も可能性が高いのはどれですか（2つ選択してください）。
A. 暗号輸出管理制御
B. サプライチェーンの弱点
C. デバイスの認証
D. 品質保証
E. 法的保留コンプライアンス
F. ランサムウェア耐性
Answer: E F
Explanation:
The requirements for archiving data and immutable backups directly align with legal hold compliance (E) and ransomware resilience (F).
Legal hold compliance ensures that organizations can retain data in a tamper-proof manner when required for litigation, regulatory mandates, or audits. Immutable backups satisfy this by preventing unauthorized changes or deletion, ensuring evidence and records are preserved.
Ransomware resilience is also a key factor. Immutable backups allow recovery from ransomware attacks, as attackers cannot encrypt or delete data stored in read-only or write-once media. This reduces downtime and supports business continuity.
Options A (crypto-export), B (supply chain), C (device attestation), and D (quality assurance) do not relate directly to data archiving or immutable storage.
CAS-005 stresses aligning security controls with business continuity and compliance requirements. By focusing on legal and ransomware-related considerations, the organization ensures both regulatory and operational resilience.

QUESTION NO: 18
最高情報セキュリティ責任者（CIO）は、ランサムウェアによる業務への影響を懸念しています。ランサムウェア攻撃が発生した場合、データの整合性を維持し、RPO（目標復旧時点）を1時間未満に抑える必要があります。以下のストレージ戦略のうち、このビジネス要件を最もよく満たすものはどれですか？
A. フルディスク暗号化
B. リモートジャーナリング

C. 不変
D. RAID 10
Answer: B
Explanation:
Remote journaling continuously sends log updates to a remote system, ensuring near-real-time backup and an RPO (Recovery Point Objective) under one hour.
Key concepts:
RPO under one hour means minimal data loss.
Remote journaling provides rapid recovery by keeping near-live backups.
Other options:
A(Full disk encryption) protects against unauthorized access but does not aid recovery.
C (Immutable storage) prevents modification but does not ensure real-time backups.
D (RAID 10) improves redundancy but does not help against ransomware.
Reference: CASP+ CAS-005 - Business Continuity and Disaster Recovery Planning

QUESTION NO: 19
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。
Answer: B
Explanation:
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.

QUESTION NO: 20
ある企業は、業界標準に準拠するために、クラウド環境のコンプライアンスを向上・自動化したいと考えています。この目標を達成するために、企業は以下のどのリソースを活用すべきでしょうか？
A. ジェンキンス
B. パイソン
C. アンシブル
D. PowerShell
Answer: C
Explanation:
Automating compliance in cloudenvironments requires a tool that can enforce configurations, manage infrastructure as code, and align with industry standards (e.g., NIST, ISO). Let's evaluate:
A). Jenkins:A CI/CD tool for automating software builds and deployments. It's not designed for compliance enforcement or infrastructure management.
B). Python:A programming language that can be scripted for automation but lacks built-in compliance-focused features without significant custom development.
C). Ansible:An automation tool for configuration management, application deployment, and compliance enforcement. It uses playbooks to define desired states, making it ideal for automating compliance checks and remediation in cloud environments (e.g., AWS, Azure). CAS-005 emphasizes automation tools for security and compliance, and Ansible fits perfectly.
Reference:CompTIA SecurityX (CAS-005) objectives, Domain 3: Security Engineering and Cryptography, focusing on automation for compliance in cloud environments.

QUESTION NO: 21

セキュリティアナリストは、レビューのために以下のSIEMアラートを受け取ります。
時間 | イベント
2025/03/07 UTC 13:54:06 | マシン: hr_talent_01.corp.local " cd " 成功
2025/03/07 UTC 13:54:07 | マシン: hr_talent_01.corp.local " cd ../../ " 成功
2025/03/07 UTC 13:54:08 | マシン: hr_talent_01.corp.local " sudo cat /etc/shadow " 成功
デバイスで発生した事象を最もよく表しているのは次のうちどれですか?
A. デバイスに対してファイルインジェクション攻撃が発生しました。
B. 攻撃者がデバイス上のパスワードハッシュを閲覧しました。
C. デバイスから機密ファイルが流出しました。
D. デバイス上でディレクトリトラバーサル攻撃が発生しました。
Answer: B
Explanation:
The best answer is B. An attacker viewed password hashes on the device . The decisive event is sudo cat /etc
/shadow SUCCESS . On Linux systems, /etc/shadow stores password hashes and related account password data. The log therefore indicates successful privileged access to that file and successful viewing of its contents. CompTIA's SecurityX Security Operations domain includes analysis of indicators of malicious activity and investigation of suspicious system behavior; this command sequence is consistent with credential- access activity.
Why the other options are not best:
A is incorrect because there is no evidence of file injection. C is not supported because the logs show file access, not confirmed data transfer or exfiltration. D is tempting because of cd ../../ , but that is only navigation. The key security-relevant action is the successful reading of /etc/shadow , which means password hashes were viewed.
References:
CompTIA SecurityX official exam objectives summary, Security Operations domain.

QUESTION NO: 22
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
Answer: A B
Explanation:
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. "

QUESTION NO: 23
以下のテストのうち、AIの出力が不正確になる理由を説明できるのはどれですか？
A.モデル中毒
B.ソーシャルエンジニアリング
C. 出力処理
D. 即時注射
Answer: A
Explanation:
Model poisoning occurs when an attacker manipulates the training data or the training process of an AI model so that its predictions are deliberately inaccurate or biased. In the SecurityX CAS-005 objectives, this is part of understanding emerging technology threats, specifically AI/ML vulnerabilities. This differs from:
* Social engineering, which manipulates humans rather than AI models.
* Output handling, which deals with how outputs are processed but doesn't cause inaccuracy at the model level.
* Prompt injections, which manipulate the model at query time, not during training.Because model poisoning directly corrupts the AI model itself, it is the clearest reason AI outputs could be inaccurate.

QUESTION NO: 24
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
Answer: C
Explanation:

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.

QUESTION NO: 25
ある組織の脆弱性管理チームは、本番サーバーのスキャン結果から以下の出力結果をレビューしています。
ID検索 | 概要
脆弱な暗号ライブラリ | このデバイスは脆弱な暗号ライブラリの使用を許可します。
サポート終了済みのサードパーティライブラリ |
稼働中のサービスには、サポート終了済みのサードパーティライブラリが含まれています。
リモートサービスが検出されました | デバイスはTCPポート21でFTPを実行しています。
サポート終了となったオペレーティングシステム |
オペレーティングシステムはサポート終了状態になりました。
データベースが検出されました |
このデバイスにはデータベースがインストールされています。
チームはまず、次のうちどれを行うべきでしょうか？
A. デバイスの前に踏み台ホストを配置します。
B. データベースサービスへのポートを閉じます。
C. メーカーがサポートするオペレーティングシステムにアップグレードしてください。
D. 実行中のFTPサービスを無効にします。
Answer: C
Explanation:
The best answer is C. Upgrade to a manufacturer-supported operating system . The end-of-life operating system is the highest-priority foundational issue because it affects the overall security posture of the host. An unsupported OS no longer receives vendor security updates, which increases exposure across the entire system, including services and libraries running on it. From a SecurityX perspective, vulnerability management and asset lifecycle issues are part of security operations and enterprise resilience. Resolving the unsupported platform first addresses the broadest root problem. CompTIA's SecurityX exam coverage includes security operations, vulnerability management activities, and proper hardware/software asset management as core skills.
Why the other options are weaker as the first step:
A adds a compensating control but leaves the unsupported server in place. B may be appropriate later, but the prompt does not indicate the database service is the primary exposed weakness. D disabling FTP would remove an insecure service and is a good hardening step, but it still leaves the system on an unsupported operating system with broader unpatched risk. The first action should address the most systemic weakness, which

is the end-of-life OS.
References:
CompTIA SecurityX official certification page.
CompTIA blog summary of current security operations topics including vulnerability management and asset management.

QUESTION NO: 26
ある大規模組織が、世界中のユーザーが利用できる生成AIプラットフォームを導入しました。ベータテスト中に得られたフィードバックに基づき、エンジニアは世界中のユーザーにとってユーザーインターフェースの遅延とページ読み込みパフォーマンスに問題があることを特定しました。現在、このインフラストラクチャは2つの独立したデータセンターで管理されており、高可用性ネットワークとロードバランサーを使用して接続されています。これらのパフォーマンス問題に対処するための最適な方法は、次のうちどれですか？
A. CDNを使用するようにアプリケーションを構成する
B. 大規模言語モデルのキューイングを可能にするRASPの実装
C. 第三データセンター内でのリモートジャーナリング
D. SASE を使用したトラフィック シェーピング
Answer: A
Explanation:
A Content Delivery Network (CDN) caches and distributes static and dynamic web content across multiple geographically distributed edge servers, reducing latency for global users. This directly addresses page- loading delays caused by distance from the primary data centers.
* RASP is for runtime application security, not latency.
* Remote journaling is for data replication, not performance optimization.
* SASE can improve security and WAN routing, but a CDN is purpose-built for content delivery performance.

QUESTION NO: 27
EDRソリューションを用いたセキュリティ評価において、セキュリティエンジニアはシステム内の資産に関する以下のレポートを作成します。
初回報告：
デバイス | タイプ | EDRの状態 | 感染状態
LN002 | Linux SE | 有効(管理対象外) | 不明
OWIN23 | Windows 7 | 有効 | クリーン
OWIN29 | Windows 10 | 有効(バイパス) | クリーン
MAC005 | Mac OS | 有効 | クリーン
5日後：
デバイス | タイプ | EDRの状態 | 感染状態
LN002 | Linux SE | 有効(管理対象外) | 不明
OWIN23 | Windows 7 | 有効 | クリーン
OWIN29 | Windows 10 | 有効(バイパス) | 感染済み
MAC005 | Mac OS | 無効 | クリーン
以下のうち、感染を最も促進した可能性が高いのはどれですか？
A. OWIN23 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 を伝播します。
C. OWIN29 の 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. MAC005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。
Answer: C
Explanation:
The best answer is C. OWIN29 ' s EDR has an unknown vulnerability that was exploited by the attacker . The decisive clue is that OWIN29 had EDR status: Enabled (bypass) in both reports and changed from Clean to Infected after five days. That strongly indicates the endpoint protection on that host was being bypassed, allowing compromise despite the agent being present. In SecurityX terms, this fits the theme of resilience against advanced threats and the possibility that a defensive tool can be circumvented or affected by a zero- day or other unknown weakness. CompTIA's SecurityX certification emphasizes designing and operating secure solutions that remain resilient in the face of modern threats.
Why the other options are less likely:
A is not supported because OWIN23 remained Clean . B is speculative; LN002 stayed Unknown , but there is no evidence it propagated malware to OWIN29. D is also unsupported because MAC005 was Clean even after its EDR became disabled. The only host with a direct clue pointing to failed protection and subsequent infection is OWIN29 , making the EDR bypass or exploitation on that host the most likely cause.
References:
CompTIA SecurityX official certification page.

QUESTION NO: 28
最近のモデムレポートを精査していたセキュリティ担当者は、複数の従業員が採用担当者を装った同一人物から連絡を受けていたことを発見した。このタイプの相関関係を最もよく表しているのは次のうちどれか？
A. スピアフィッシングキャンペーン
B. 脅威モデリング
C.レッドチームの評価
D.攻撃パターン分析
Answer: A
Explanation:
The situation where several employees were contacted by the same individual impersonating a recruiter best describes aspear-phishing campaign. Here's why:
Targeted Approach: Spear-phishing involves targeting specific individuals within an organization with personalized and convincing messages to trick them into divulging sensitive information or performing actions that compromise security.
Impersonation: The use of impersonation, in this case, a recruiter, is a common tactic in spear-phishing to gain the trust of the targeted individuals and increase the likelihood of a successful attack.
Correlated Contacts: The fact that several employees were contacted by the same individual suggests a coordinated effort to breach the organization's security by targeting multiple points of entry through social engineering.
References:

CompTIA Security+ SY0-601 Study Guide by Mike Chapple and David Seidl
NIST Special Publication 800-61: Computer Security Incident Handling Guide OWASP Phishing Cheat Sheet

QUESTION NO: 29
ある企業が、スライドテンプレートの使用を可能にする、広く知られているコラボレーションWebアプリケーション上に知的財産データが存在することを発見しました。システム管理者は、この問題を防止する方法を判断するために、各ツールの設定を精査しています。以下のセキュリティソリューションが導入されています。
* CASB
* 封筒
* WAF
* EDR
* ファイアウォール
* IDS
* SIEM
* DLPエンドポイント
管理者は、この問題に対処するために、次のうちどれを行うべきでしょうか？
A. すべての WAF ポリシーでブロックを有効にします。
B. CASB 内で不正な Web アプリケーションをブロックするポリシーを適用します。
C.
疑わしいウェブサイトへの送信ネットワークトラフィックについて、SIEM内でアラートを作成します。
D.
DLPエンドポイントを設定して、機密データがリムーバブルストレージに保存されないようにします。
Answer: B

QUESTION NO: 30
ある下請け業者が、大手航空機メーカー向けにセーフティクリティカルな航空電子機器ソフトウェアを開発しています。あるインシデント発生後、第三者調査機関は同社に対し、開発ライフサイクルにおいて形式手法の導入を開始するよう勧告しました。以下の調査結果のうち、調査機関の勧告を最も直接的に裏付けるものはどれですか。
A. システムの部品表に商用ライブラリとオープンソース
ライブラリが含まれていませんでした。
B. 会社には、動的かつインタラクティブなアプリケーション セキュリティ
テスト標準が欠けています。
C. コードベースには、機能要件と非機能要件への追跡可能性が欠けています。
D. 実装されたソフトウェアは、コンピューティング リソースとメモリ
リソースを効率的に管理しません。
Answer: C
Explanation:
Formal methods in software engineering use mathematically based specifications to ensure system correctness, safety, and compliance with requirements. SecurityX CAS-005 stresses the importance of traceability between code and both functional and non-functional

requirements for high-assurance systems like avionics. A lack of traceability means it is impossible to verify that the implementation meets all required safety and performance standards-exactly what formal methods address.

QUESTION NO: 31
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。
Answer: B
Explanation:
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

QUESTION NO: 32
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. ブラウザ分離
C.ゾーン転送保護
D. HIDS
Answer: A

QUESTION NO: 33
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
Answer: D
Explanation:
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

QUESTION NO: 34
ある報道機関は、忘れられる権利を遵守するために、ユーザーが虚偽のデータをオンライン出版物から遡及して削除するよう要求できるワークフローを実装したいと考えています。次の規制のうち、この組織が最も対処しようとしているのはどれですか？
A. GDPR
B. カップ
C. CCPA

D. ドラ

Answer: A

Explanation:

The General Data Protection Regulation (GDPR) is the regulation most likely being addressed by the news organization. GDPR includes provisions for the " right to be forgotten, " which allows individuals to request the deletion of personal data that is no longer necessary for the purposes for which it was collected. This regulation aims to protect the privacy and personal data of individuals within the European Union.

References:

CompTIA SecurityX Study Guide: Covers GDPR and its requirements, including the right to be forgotten.

GDPR official documentation: Details the rights of individuals, including data erasure and the right to beforgotten.

" GDPR: A Practical Guide to the General Data Protection Regulation " by IT Governance Privacy Team:

Provides a comprehensive overview of GDPR compliance, including workflows for data deletion requests.

QUESTION NO: 35

医療提供者が保存中の患者データを暗号化することで満たすビジネス要件を最もよく説明しているのは次のうちどれですか?

A. 病院間のデータ転送のセキュリティ確保

B. 否認防止データの提供

C. 個人情報の盗難による責任の軽減

D. 移植性をサポートしながらプライバシーを保護します。

Answer: D

Explanation:

Encrypting patient data at rest is a critical requirement for healthcare providers to ensure compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA). The primary business requirement fulfilled by this practice is the protection of patient privacy while supporting the portability of medical information. By encrypting data at rest, healthcare providers safeguard sensitive patient information from unauthorized access, ensuring that privacy is maintained even if the storage media are compromised.

Additionally, encryption supports the portability of patient records, allowing for secure transfer and access across different systems and locations while ensuring that privacy controls are in place.

References:

CompTIA SecurityX Study Guide: Emphasizes the importance of data encryption for protecting sensitive information and ensuring compliance with regulatory requirements.

HIPAA Security Rule: Requires healthcare providers to implement safeguards, including encryption, to protect patient data.

" Health Informatics: Practical Guide for Healthcare and Information TechnologyProfessionals " by Robert E.

Hoyt: Discusses encryption as a key measure for protecting patient data privacy and supporting data portability.