CompTIA.SY0-701-JPN.v2026-02-24.q453

試験コード：	SY0-701-JPN
試験名称：	CompTIA Security+ Certification Exam (SY0-701日本語版)
認証ベンダー：	CompTIA
無料問題の数：	453
バージョン：	v2026-02-24
ページの閲覧量：	169
問題集の閲覧量：	6955

https://www.jpnshiken.com/shiken/CompTIA.SY0-701-JPN.v2026-02-24.q453.html

質問: **1**
大企業の最高情報セキュリティ責任者 (CISO) は、自社のセキュリティ ポリシーが外部規制当局によって課せられた要件とどのように比較されるかを理解したいと考えています。CISO は次のどれを使用する必要がありますか。
A. 侵入テスト
B. 内部監査
C. 証明
D. 外部検査
正解: (正解を表示します)
An external examination (also known as an external audit or external review) is the best method for the Chief Information Security Officer (CISO) to gain an understanding of how the company's security policies compare to external regulatory requirements. External examinations are conducted by third-party entities that assess an organization's compliance with laws, regulations, and industry standards.
* Penetration tests focus on identifying vulnerabilities, not compliance.
* Internal audits assess internal controls but are not impartial or focused on regulatory requirements.
* Attestation is a formal declaration but does not involve the actual evaluation of compliance.

質問: **2**
アナリストは、ユーザーがフィッシング メール内のリンクをクリックしたインシデントを調査しています。アナリストは、接続が成功したかどうかを判断するために、次のどのログ ソースを利用しますか。
A. ネットワーク
B. システム
C. アプリケーション
D. 認証
正解: (正解を表示します)
To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would

provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.

質問: **3**
セキュリティエンジニアは、攻撃中に増加する様々なトラフィックタイプの影響を最小限に抑えるために、NGFWを設定する必要があります。エンジニアが設定する可能性が最も高いルールの種類は次のうちどれですか？
A. 署名ベース
B. 行動ベース
C. URLベース
D. エージェントベース
正解: **(**正解を表示します**)**
To minimize the impact of the increasing number of various traffic types during attacks, a security engineer is most likely to configure behavioral-based rules on a Next-Generation Firewall (NGFW). Behavioral-based rules analyze the behavior of traffic patterns and can detect and block unusual or malicious activity that deviates from normal behavior.
Behavioral-based: Detects anomalies by comparing current traffic behavior to known good behavior, making it effective against various traffic types during attacks.
Signature-based: Relies on known patterns of known threats, which might not be as effective against new or varied attack types.
URL-based: Controls access to websites based on URL categories but is not specifically aimed at handling diverse traffic types during attacks.
Agent-based: Typically involves software agents on endpoints to monitor and enforce policies, not directly related to NGFW rules.

質問: **4**
セキュリティ管理者が組織内のすべてのハードドライブに暗号化を導入しています。管理者が適用しているセキュリティ概念は次のどれですか？
A. 認証
B. 誠実さ
C. 機密性
D. ゼロトラスト
正解: **C (**コメントを発表する**)**

質問: **5**
組織がインシデント対応プロセスを改善するために使用すべき演習は次のどれですか?
A. テーブルトップ
B. レプリケーション

C. フェイルオーバー
D. 回復
正解: **(**正解を表示します**)**
A tabletop exercise is a simulated scenario that tests the organization's incident response plan and procedures. It involves key stakeholders and decision-makers who discuss their roles and actions in response to a hypothetical incident. It can help identify gaps, weaknesses, and improvement areas in the incident response process. It can also enhance communication, coordination, and collaboration among the participants.

質問: **6**
侵入テストにより、組織全体の複数のサーバーで SMBv1 が有効になっていることが判明しました。
組織はこの脆弱性を可能な限り効率的に修復したいと考えています。そのためには、次のどれを使用すべきでしょうか？
A. GPO
B. SFTP
C. DLP
D. ACL
正解: **A (**コメントを発表する**)**

質問: **7**
複数のエンティティが必要に応じてキーにアクセスできるように、データ セットの暗号化キーを安全に保存する最適な方法はどれですか。
A. 公開鍵インフラストラクチャ
B. 公開台帳を公開する
C. 公開鍵暗号化
D. キーエスクロー
正解: **(**正解を表示します**)**
Key escrow refers to a system where encryption keys are stored in a secure, third-party repository, allowing authorized entities (such as specific individuals or organizations) to access the key when necessary.

質問: **8**
ある組織では、ネットワーク共有データの削除や不適切な権限割り当てといった問題が発生しています。これらの問題を追跡し、解決するために最も効果的な方法は次のうちどれでしょうか？
A. DLP
B. EDR
C. 終了
D. ACL
正解: **C (**コメントを発表する**)**

FIM continuously monitors files and their permissions on network shares, alerting when items are deleted or access rights are changed so administrators can quickly investigate and remediate.

質問: **9**
ユーザーが検証のためにデジタル署名を含むメールを送信します。ユーザーがメールの送信を否定できないようにするためには、次のどのセキュリティコンセプトが役立ちますか？
A. 否認防止
B. 機密保持
C. 誠実さ
D. 認証
正解: **A (**コメントを発表する**)**
A digital signature provides cryptographic proof of origin, preventing the sender from denying they authored and sent the email - this is the essence of non-repudiation.

質問: **10**
侵入テスターがハイパーバイザープラットフォームへの不正アクセスに成功しました。以下の脆弱性のうち、最も悪用された可能性が高いのはどれですか？
A. クロスサイトスクリプティング
B. SQLインジェクション
C. 競合状態
D. VMエスケープ
正解: **D (**コメントを発表する**)**
VM escape occurs when an attacker breaks out of a virtual machine's sandbox to interact directly with the underlying hypervisor, granting unauthorized access to the host platform. This is the vulnerability exploited when compromising a hypervisor.

質問: **11**
アラートを作成し、異常なアクティビティを検出するためにログ データを集約するには、次のどれを使用する必要がありますか?
A. SIEM
B. WAF
C. ネットワークタップ
D. IDS
正解: **A (**コメントを発表する**)**
A Security Information and Event Management (SIEM) solution collects, aggregates, and correlates logs from multiple sources to detect anomalies and generate alerts. SIEMs are essential for security monitoring and incident detection.

質問: **12**

管理者はWebフィルタリング製品を導入していますが、ユーザーが悪意のあるリンクにアクセスしているのが依然として確認されています。セキュリティ管理者が確認する必要がある設定項目は次のどれですか？
A. 侵入防止システム
B. コンテンツの分類
C. 暗号化
D. 暗号化
正解: **(**正解を表示します**)**
Content categorization defines how websites are classified (e.g., gambling, malicious, social media) within the web-filtering product. If users are still accessing malicious links, it likely means the categorization settings need to be reviewed or updated to block those sites effectively.

質問: **13**
毎年の外部侵入テストを完了すると、企業は次のようなガイダンスを受け取ります。
- 現在公開されている未使用のウェブサーバー2台を廃止する
インターネット。
- 既存の運用 Web サーバーで見つかった 18 個の開いている未使用のポートを閉じます。
- 会社のメールアドレスと連絡先情報をパブリックドメインから削除する
登録記録。
これらの推奨事項を最もよく表すセキュリティ プラクティスは次のどれですか。
A. 攻撃対象領域の縮小
B. 脆弱性評価
C. 卓上演習
D. ビジネス影響分析
正解: **(**正解を表示します**)**
Attack surface reduction involves minimizing the number of exploitable points, such as unused servers, open ports, and publicly exposed contact information, that attackers could target.

質問: **14**
ドメインにログインするときにユーザーがよく同意するのは次のどれですか?
A. AUP
B. MAC
C. EULA
D. EAP
正解: **(**正解を表示します**)**
When users log in to a corporate domain, they're typically presented with an acceptable use policy outlining the rules and responsibilities for system use before gaining access. This ensures they agree to organizational guidelines up front.

質問: **15**

セキュリティ アナリストは、リスクベースのアプローチを使用して脆弱性スキャンの結果に優先順位を付けています。アナリストが使用する最も効率的なリソースは次のどれですか。
A. ビジネスインパクト分析
B. 共通脆弱性評価システム
C. リスクレジスタ
D. 露出係数
正解: **(**正解を表示します**)**
CVSS provides a standardized, numerical severity rating for each vulnerability, enabling an analyst to efficiently rank and prioritize scan findings based on objective risk metrics.

質問: **16**
制御と緩和要因を適用した後に存在するリスクを最もよく表しているのは次のうちどれですか?
A. 残差
B. 回避
C. 固有の
D. 運用中
正解: **(**正解を表示します**)**
This is the risk that remains after controls and mitigation efforts have been applied.

質問: **17**
セキュリティ チームは、組織のオンプレミス ソフトウェア アプリケーションをクラウドベースのサービスとしてホストするための新しい環境を設定しています。組織がセキュリティのベストプラクティスに従うために、チームは次のどれを確実に実施する必要がありますか?
A. リソースの可視化と分離
B. ネットワークセグメンテーション
C. データの暗号化
D. 強力な認証ポリシー
正解: **A (**コメントを発表する**)**
When hosting an on-premises software application in a cloud-based service, ensuring visualization and isolation of resources is crucial for maintaining security best practices. This involves using virtualization techniques to create isolated environments (e.g., virtual machines or

containers) for different applications and services, reducing the risk of cross-tenant attacks or resource leakage.
Network segmentation is important but pertains more to securing network traffic rather than isolating computing resources.
Data encryption is also essential but doesn't specifically address resource isolation in a cloud environment.
Strong authentication policies are critical for access control but do not address the need for isolating resources within the cloud environment.

質問: **18**
ある会社は最近、従業員にリモートワークを許可することを決定しました。会社は VPN を使用せずにデータを保護したいと考えています。会社が実装すべきテクノロジーは次のうちどれですか?
A. セキュアウェブゲートウェイ
B. 仮想プライベートクラウドのエンドポイント
C. ディープパケットインスペクション
D. 次世代レーションファイアウォール
正解: **(**正解を表示します**)**
A Secure Web Gateway (SWG) protects users by filtering unwanted software/malware from user-initiated web traffic and enforcing corporate and regulatory policy compliance. This technology allows the company to secure remote users' data and web traffic without relying on a VPN, making it ideal for organizations supporting remote work.

質問: **19**
忘れられる権利に関する個人の要求に応じるために組織が取らなければならない行動は次のどれですか?
A. 個人を特定できる属性をすべて消去します。
B. すべてのデータを暗号化します。
C. 個人のデータをすべて削除します。
D. 個人のデータをすべて難読化します。
正解: **C (**コメントを発表する**)**
The right to be forgotten, as outlined in regulations such as the General Data Protection Regulation (GDPR), requires organizations to permanently delete an individual's personal data upon request, unless there is a legal or contractual obligation to retain it.

質問: **20**
データ処理センターで侵入が発生した後、管理者は管理者パスワードがオンラインで漏洩したという通知を受け取りました。このインシデントの再発を防ぐために、次のうちどれを採用すべきでしょうか?
A. パスワード管理
B. パスワードの複雑さ

C. パスワードポリシー
D. パスワードボールト
正解: **D (**コメントを発表する**)**
A centralized password vault securely stores and manages privileged credentials, encrypting them at rest, controlling access, and enabling strong rotation policies, so administrative passwords are never exposed in plaintext and can't be leaked online.

質問: **21**
転送中のデータを保護する最も適切な方法はどれでしょうか?
A. SHA-256
B. SSL 3.0
C. TLS 1.3
D. AES-256
正解: **(**正解を表示します**)**
Transport Layer Security (TLS) 1.3 is the latest version of the TLS protocol and provides strong encryption for securing data in transit between clients and servers. It offers improved security and performance compared to previous versions like SSL 3.0 and earlier TLS versions.

質問: **22**
次のどの制御タイプが SIEM ツールからのアラートを表していますか?
A. 予防的
B. 修正
C. 補償
D. 探偵
正解: **(**正解を表示します**)**
A SIEM alert is a detective control because it identifies and reports suspicious or malicious activity after it occurs, enabling further investigation and response.

質問: **23**
企業が HIPS を導入して実装しているセキュリティ制御は次のどれですか? (2 つ選択)
A. ディレクティブ
B. 予防的
C. 物理
D. 修正
E. 補償
F. 探偵
正解: **(**正解を表示します**)**
A host-based intrusion prevention system actively monitors and blocks malicious behavior on the endpoint (preventive control) while also alerting or logging suspicious events (detective control).

質問: **24**

組織が複数の種類のログを効率的に管理および分析するために使用すべき戦略は次のどれですか?
A. SIEMソリューションを導入する
B. ログを集計して分析するためのカスタムスクリプトを作成する
C. EDRテクノロジーを実装する
D. 統合脅威管理アプライアンスをインストールする
正解: **(**正解を表示します**)**
Deploying a Security Information and Event Management (SIEM) solution allows for efficient log aggregation, correlation, and analysis across an organization's infrastructure, providing real-time security insights.

質問: **25**
セキュリティチームは、複数の受信トレイに宛てられた、様々な件名のメールが大量に届いているという警告を受けました。各メールには、無効なドメインにリダイレクトするURL短縮リンクが含まれています。セキュリティチームが取るべき最善の対策は次のうちどれですか？
A. すべての件名のブロックリストを作成します。
B. デッドドメインを DNS シンクホールに送信します。
C. 受信したすべてのメールを隔離し、すべての従業員に通知します。
D. Web プロキシで URL 短縮ドメインをブロックします。
正解: **(**正解を表示します**)**
Block the URL shortener domain in the web proxy: By blocking the URL shortener domain, the security team can prevent users from accessing potentially malicious links, even if the domain is currently dead. This proactive measure helps mitigate the risk of future attacks using the same URL shortener.

質問: **26**
セキュリティアナリストは、悪意のあるアクターが環境に潜んでいるのではないかと懸念していますが、不審なアクティビティに関するアラートは受け取っていません。これらのアクターの存在をさらに調査するために、アナリストは次のうちどれを実施すべきでしょうか？
A. 脅威ハンティング
B. デジタルフォレンジック
C. 脆弱性スキャン
D. 電子情報開示
正解: **A (**コメントを発表する**)**
Threat hunting is a proactive activity used to search for hidden or undetected malicious actors when no alerts have been triggered but suspicious activity is suspected.

質問: **27**
機密データに暗号化を適用する際に従うセキュリティ概念は次のどれですか?
A. 機密保持

B. 否認防止
C. 可用性
D. 誠実さ
正解: **A (**コメントを発表する**)**
Encryption ensures confidentiality by protecting sensitive data from unauthorized access, allowing only authorized parties with the correct decryption key to read it.

質問: **28**
セキュリティ担当者が、企業の共有ドライブ上に従業員の個人情報を含むフォルダを発見しました。従業員の個人情報の保管に関する組織のポリシーと基準を特定するために、セキュリティ担当者が使用すべきデータの種類として最も適切なものは次のうちどれですか？
A. 法的
B. 金融
C. プライバシー
D. 知的財産
正解: **C (**コメントを発表する**)**
Privacy data classification includes Personally Identifiable Information (PII), which consists of an employee's personal details such as name, address, Social Security number, or other sensitive information. Organizational policies and standards concerning the storage and protection of such data fall under privacy regulations (e.g., GDPR, CCPA, or HIPAA). Ensuring compliance with these policies helps prevent unauthorized access and data breaches.

質問: **29**
侵入テスト中に、内部PKIの脆弱性が悪用され、特別に細工された証明書を使用してドメイン管理者権限が取得されました。クリーンアップフェーズの一環として、以下のどの修復タスクを完了する必要がありますか？
A. CRLの更新
B. CAへのパッチ適用
C. パスワードの変更
D. SOARの実装
正解: **(**正解を表示します**)**
The first priority is to revoke any compromise certificates. This ensures that those certificates can no longer be used for unauthorized access.

質問: **30**
セキュリティ アナリストがアプリケーション サーバーを調査しているときに、サーバー上のソフトウェアが異常な動作をしていることを発見しました。このソフトウェアは通常、バッチ ジョブをローカルで実行し、トラフィックを生成しませんが、プロセスがランダムな高ポートを介して送信トラフィックを生成しています。このソフトウェアで悪用された可能性のある脆弱性は次のどれですか。

A. メモリインジェクション
B. 競合状態
C. サイドローディング
D. SQLインジェクション
正解: **(**正解を表示します**)**
Memory injection vulnerabilities allow unauthorized code or commands to be executed within a software program, leading to abnormal behavior such as generating outbound traffic over random high ports. This issue often arises from software not properly validating or encoding input, which can be exploited by attackers to inject malicious code.

質問: **31**
インフラストラクチャ環境で低コストの IoT デバイスをインストールして使用する場合、セキュリティ上の懸念事項となる可能性が高いのは次のうちどれですか。
A. 原産国
B. デバイスの応答性
C. 導入の容易さ
D. データの保存
正解: **(**正解を表示します**)**
The sheer volume of data generated by IoT devices can make securing and protecting sensitive information difficult. As more devices are connected to the Internet, there is an increasing risk of data breaches and cyberattacks, which can result in the theft of personal and sensitive data.

質問: **32**
ある組織でセキュリティ侵害が発生し、攻撃者は強化されたPCからリモート接続を介して攻撃者の銀行口座に不正な電信送金を行うことができました。セキュリティアナリストはイベントのタイムラインを作成していたところ、ネットワーク上の別のPCにマルウェアが含まれていることを発見しました。コマンド履歴を確認したところ、以下のことが判明しました。
PS>.\mimikatz.exe "sekurlsa::pth /user:localadmin /domain:corp-ドメイン.com /ntlm:B4B9B02E1F29A3CF193EAB28C8D617D3F327
攻撃者が強化された PC にアクセスした方法を最もよく表しているのは次のうちどれですか?
A. 攻撃者は、銀行プラットフォームによってホストされるファイルレス マルウェアを作成しました。

B. 攻撃者は共有サポート アカウントを使用してパスザハッシュ攻撃を実行しました。
C. 攻撃者は、エンドポイント検出および応答ソフトウェアを回避するために、living-off-the-land バイナリを利用しました。
D. 攻撃者はソーシャルエンジニアリングを利用して会計士に不正な送金を実行させました。
正解: **(**正解を表示します**)**
Mimikatz is an open-source tool that allows users to view and extract credentials stored on a Windows system. It can extract plaintext passwords, hashes, PIN codes, and Kerberos tickets from memory.

質問: **33**
一連のアカウント侵害と認証情報の不正使用が発生した後、企業はセキュリティ プログラムを開発するためにセキュリティ マネージャーを雇います。セキュリティ マネージャーがセキュリティ意識を高めるために最初に実行する必要がある手順はどれですか。
A. 危険な行動を識別し、その結果に関するレポートを配布するツールを評価します。
B. パスワード管理の重要性を説明するニュースレターを四半期ごとに送信します。
C. フィッシング キャンペーンを開発し、成功した場合は管理チームに通知します。
D. ポリシーとハンドブックを更新して、すべての従業員に新しい手順が確実に通知されるようにします。
正解: **(**正解を表示します**)**
The first step in increasing security awareness should be to update policies and handbooks to ensure that all employees are aware of the new procedures and security expectations. Clear, documented policies provide a foundation for employees to understand their roles and responsibilities regarding security. Once the policies are in place, the company can implement additional strategies like training, newsletters, or phishing campaigns to reinforce these practices.

質問: **34**
アナリストは、最新リリースをテストするために、本番環境からUATサーバーにデータを移動したいと考えています。アナリストは、データ保護のために以下のどの戦略を採用すべきでしょうか。
A. データマスキング
B. データのトークン化
C. データの難読化
D. データ暗号化
正解: **A (**コメントを発表する**)**
Data masking protects sensitive production data when moving it into non-production environments by replacing sensitive fields with realistic but fictitious values, allowing safe testing without exposing real data.

質問: **35**

セキュリティアナリストが侵入テストのレポートを検証していたところ、テスターが同じローカルユーザーIDとパスワードを使って重要な社内システムに侵入していたことに気づきました。今後、このような事態を防ぐには、次のうちどれが有効でしょうか。
A. 適切なパスワードポリシーを使用して集中認証を実装する
B. パスワードの複雑さのルールを追加し、パスワード履歴の制限を増やす
C. システムを外部認証サーバーに接続する
D. ユーザーアカウントのパスワード変更権限を制限する
正解: **(**正解を表示します**)**
The penetration tester was able to pivot using the same local user ID and password, indicating that systems were using local authentication rather than a centralized authentication mechanism. Implementing centralized authentication (such as Active Directory, LDAP, or RADIUS) with strong password policies would ensure that credentials are managed centrally, reducing the risk of credential reuse and lateral movement across systems. This approach also enables better monitoring and enforcement of security policies.

質問: **36**
データベースエンジニアはテストのためにサンプル顧客データを必要としています。PII(個人情報)の不正な閲覧や開示を防ぐには、次のうちどれが効果的でしょうか？
A. マスキング
B. RBAC
C. トークン化
D. フィルタリング
正解: **(**正解を表示します**)**
Data masking replaces real PII with realistic but fictional values in non-production environments, ensuring testers can't view or disclose actual sensitive information.

質問: **37**
データセンターのセキュリティを強化するため、セキュリティ管理者はCCTVシステムを導入し、撮影の可能性があることを示す標識をいくつか設置しました。これらの管理策を最もよく表しているのは次のうちどれですか(2つ選択してください)。
A. 予防
B. 抑止力
C. 修正
D. ディレクティブ
E. 補償
F. 探偵
正解: **(**正解を表示します**)**
The CCTV system and signs about the possibility of being filmed serve as both deterrent and detective controls.
Deterrent controls: Aim to discourage potential attackers from attempting unauthorized actions.

Posting signs about CCTV serves as a deterrent by warning individuals that their actions are being monitored.
Detective controls: Identify and record unauthorized or suspicious activity. The CCTV system itself functions as a detective control by capturing and recording footage that can be reviewed later.
Preventive controls: Aim to prevent security incidents but are not directly addressed by the CCTV and signs in this context.
Corrective controls: Aim to correct or mitigate the impact of a security incident.
Directive controls: Provide guidelines or instructions but are not directly addressed by the CCTV and signs.
Compensating controls: Provide alternative measures to compensate for the absence or failure of primary controls.

質問: **38**
次の脅威アクターのうち、利益を動機とする可能性が高いのはどれですか?
A. シャドーIT
B. 組織犯罪
C. ハクティビスト
D. 内部脅威
正解: **(正解を表示します)**

質問: **39**
クライアントの Web ブラウザを制御するために Web ベースのアプリケーションにスクリプトを挿入することを伴う脆弱性のタイプは次のどれですか。
A. SQLインジェクション
B. クロスサイトスクリプティング
C. ゼロデイエクスプロイト
D. オンパス攻撃
正解: **(正解を表示します)**
Cross-site scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into a website, which are then executed in the user's web browser, potentially leading to data theft or session hijacking.

質問: **40**
デバイスとの間の不要な通信や安全でない通信に対して最も効果的な保護を提供するのは次のどれですか?
A. システムの強化
B. ホストベースのファイアウォール
C. 侵入検知システム
D. マルウェア対策ソフトウェア

正解: **B** (コメントを発表する)

質問: **41**
長時間の停電から身を守るための最善の安全策は次のどれですか?
A. オフサイトバックアップ
B. 電池
C. 無停電電源装置
D. ジェネレータ
正解: (正解を表示します)
Generators are the best safeguard against extended power failures, as they can provide power for long durations, unlike batteries or uninterruptible power supplies, which are intended for short-term use.

質問: **42**
限られたコンピューティング リソースでの通信を保護するために、次の暗号化方式のうちどれが適していますか?
A. ハッシュアルゴリズム
B. 公開鍵インフラストラクチャ
C. 楕円曲線暗号
D. 対称暗号化
正解: (正解を表示します)

質問: **43**
さまざまな会社の関係者が集まり、オフショア オフィスに影響を及ぼすセキュリティ侵害が発生した場合の役割と責任について話し合います。これは次のどれに該当しますか。
A. テーブルトップ演習
B. 侵入テスト
C. 地理的分散
D. インシデント対応
正解: (正解を表示します)
A tabletop exercise is a discussion-based activity where stakeholders simulate a security breach scenario to identify gaps in response plans and clarify roles and responsibilities.

質問: **44**
退職前に顧客リストを個人アカウントに電子メールで送信している従業員を検出するには、次のうちどれを使用しますか?
A. DLP
B. 終了
C. IDS
D. EDR

正解: (正解を表示します)
Data Loss Prevention (DLP) monitors and controls the movement of sensitive data, enabling detection of attempts to send protected information, such as a customer list, to unauthorized destinations.

質問: **45**
システム管理者がVPNログを確認したところ、勤務時間外にユーザーが会社のファイルサーバーにアクセスし、情報が不審なIPアドレスに転送されていることに気付きました。以下の脅威のうち、最も発生している可能性が高いのはどれですか？
A. データの流出
B. タイプミススクワッティング
C. ルートまたは信頼
D. 脅迫
正解: **A** (コメントを発表する)

質問: **46**
ビジネス継続性の机上演習を実施しているとき、セキュリティ チームは、長期間の停電中に発電機に障害が発生した場合の潜在的な影響について懸念を抱きます。
インフラストラクチャ保守活動を実施および計画する際に、チームが最も考慮する可能性が高いのは次のどれですか。
A. RPO
B. ARO
C. MTBF
D. 平均所要時間
正解: (正解を表示します)
They're worried about how long the generator can run before it's likely to fail during a prolonged outage. MTBF quantifies the expected operational time between failures, guiding preventive maintenance schedules and part replacement intervals to reduce the chance of a fault when the generator is most needed.

質問: **47**

従業員は、会社の最高経営責任者を名乗る未知の番号から、ギフトカードをいくつか購入するように求めるテキスト メッセージを受け取ります。これは、次のどの種類の攻撃を表していますか。
A. ヴィッシング
B. スミッシング
C. プリテキスティング
D. フィッシング
正解**: B (**コメントを発表する**)**
Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack.

質問**: 48**
長期にわたる停電が企業の環境に与える影響を最も軽減できるのはどれでしょうか?
A. ホットサイト
B. UPS
C. スナップショット
D. 飛翔
正解**: B (**コメントを発表する**)**
A UPS (Uninterruptible Power Supply) would most likely mitigate the impact of an extended power outage on a company's environment. A UPS provides backup power and ensures that systems continue to run during short-term power outages, giving enough time to perform an orderly shutdown or switch to a longer-term power solution like a generator.
Hot site: A fully operational offsite data center that can be used if the primary site becomes unavailable. It's more suitable for disaster recovery rather than mitigating short-term power outages.
UPS: Provides immediate backup power, protecting against data loss and hardware damage during power interruptions.
Snapshots: Used for data backup and recovery, not for power outage mitigation.
SOAR (Security Orchestration, Automation, and Response): A platform for automating security operations, not related to power outage mitigation.

質問**: 49**
インフラストラクチャ環境で低コストの IoT デバイスをインストールして使用する場合、セキュリティ上の懸念事項となる可能性が高いのは次のうちどれですか。
A. 偽造品
B. デバイスの応答性

C. 導入の容易さ
D. データ残留
正解: **A (**コメントを発表する**)**
Low-cost IoT devices often come from unvetted or knock-off manufacturers, introducing counterfeit or tampered hardware and firmware that can embed backdoors or malicious components, posing a major supply-chain security risk.

質問: **50**
システム管理者は、デバイスがネットワーク認証を実行するように再設計しています。次の要件を満たす必要があります。
* 既存の内部証明書を使用する必要があります。
* 有線および無線ネットワークをサポートする必要があります
* 承認されていないデバイスは隔離サブネットに隔離する必要があります
* 承認されたデバイスはリソースにアクセスする前に更新する必要があります
次のどれが要件を最もよく満たすでしょうか?
A. 802.IX
B. EAP
C. RADIUS
D. WPA2
正解: **(**正解を表示します**)**
802.1X is a network access control protocol that provides an authentication mechanism to devices trying to connect to a LAN or WLAN. It supports the use of certificates for authentication, can quarantine unapproved devices, and ensures that only approved and updated devices can access network resources. This protocol best meets the requirements of securing both wired and wireless networks with internal certificates.

質問: **51**
ネットワーク管理者は、会社のクラウド環境にロードバランサーを導入するプロジェクトに取り組んでいます。このプロジェクトは、以下の基本的なセキュリティ要件のうちどれを満たしていますか？
A. プライバシー
B. 誠実さ
C. 機密性
D. 可用性
正解: **(**正解を表示します**)**
Deploying a load balancer in the company's cloud environment primarily fulfills the fundamental security requirement of availability. A load balancer distributes incoming network traffic across multiple servers, ensuring that no single server becomes overwhelmed and that the service remains available even if some servers fail.

Availability: Ensures that services and resources are accessible when needed, which is directly supported by load balancing.
Privacy: Protects personal and sensitive information from unauthorized access but is not directly related to load balancing.
Integrity: Ensures that data is accurate and has not been tampered with, but load balancing is not primarily focused on data integrity.
Confidentiality: Ensures that information is accessible only to authorized individuals, which is not the primary concern of load balancing.

質問: **52**
ある組織は、地理的に分散した組織環境内の複数のサーバーへのアクセスを構成することで、アプリケーションの耐障害性を高めたいと考えています。このアーキテクチャを最もよく表すのは次のどれですか。
A. コンテナ化された
B. マルチテナント
C. 負荷分散
D. 仮想化
正解: **(**正解を表示します**)**
A load-balanced architecture distributes incoming application traffic across multiple servers, potentially in different geographic locations, to optimize resource use, improve response times, and provide redundancy if any single server fails.

質問: **53**
歩行者の通行を許可しながら、不正な車両がデータセンターに侵入するのを防ぐための、最も効果的な物理的セキュリティ対策は次のどれですか?
A. アクセス制御玄関
B. フェンシング
C. ビデオ監視
D. 格納式ボラード
正解: **(**正解を表示します**)**
Retractable bollards provide a strong physical barrier to stop unauthorized vehicles while remaining low enough (or lowered) to let pedestrians pass freely, making them ideal for controlling vehicle access without impeding foot traffic.

質問: **54**
クラウド環境で意図しない企業認証情報の漏洩が発生する一般的な原因は次のどれですか?
A. コードリポジトリ
B. ダークウェブ
C. 脅威フィード
D. 国家主体

E. 脆弱性データベース
正解: **(**正解を表示します**)**
Code repositories: Developers sometimes inadvertently include sensitive information, such as API keys, passwords, and other credentials, in their code. When this code is pushed to public repositories (e.g., GitHub, GitLab), those credentials can be exposed to the world, leading to potential credential leakage.

質問: **55**
次の脅威アクターのうち、巨額の資金を使って他国にある重要なシステムを攻撃する可能性が高いのはどれですか?
A. インサイダー
B. 未熟な攻撃者
C. 国民国家
D. ハクティビスト
正解: **(**正解を表示します**)**
A nation-state is a threat actor that is sponsored by a government or a political entity to conduct cyberattacks against other countries or organizations. Nation-states have large financial resources, advanced technical skills, and strategic objectives that may target critical systems such as military, energy, or infrastructure. Nation-states are often motivated by espionage, sabotage, or warfare.

質問: **56**
セキュリティ オペレーション センターは、サーバー上で検出された悪意のあるアクティビティが正常であると判断します。
次のアクティビティのうち、検出されたアクティビティを将来無視する行為を説明しているものはどれですか?
A. チューニング
B. 集約
C. 隔離中
D. アーカイブ
正解: **(**正解を表示します**)**
Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the

network to prevent further damage or spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options.

質問: **57**
セキュリティ アナリストが脆弱性の修復を優先順位付けするために使用すべきものは次のどれですか。
A. OSINT
B. CVE
C. IoC
D. CVSS
正解: **(**正解を表示します**)**
The Common Vulnerability Scoring System (CVSS) provides a standardized severity score for vulnerabilities, enabling analysts to prioritize remediation efforts based on risk impact.

質問: **58**
暗号化されていない PLC 管理トラフィックが最も多く見つかるのは次のうちどれですか?
A. SDN
B. IoT
C. VPN
D. SCADA
正解: **D (**コメントを発表する**)**
SCADA systems orchestrate and manage PLCs in industrial environments, and their native management protocols (e.g., Modbus, DNP3) are often sent unencrypted.

質問: **59**
サードパーティの侵入テスターによるテストの条件についての詳細を示すものはどれですか?
A. 交戦規則
B. サプライチェーン分析
C. 監査権条項
D. デューデリジェンス
正解: **(**正解を表示します**)**
Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable.

質問: **60**
内部ソースによって生成される証明書の例は次のどれですか?
A. デジタル署名
B. 非対称鍵
C. 自己署名
D. 対称鍵
正解: **C (**コメントを発表する**)**
A self-signed certificate is created and signed by the issuing organization itself rather than by an external Certificate Authority, making it an internally generated certificate.

質問: **61**
新しい Web サーバーが稼働する前に、セキュリティ チームが最初に実行する必要があるのは次のうちどれですか。
A. ネットワーク侵入検出を有効にします。
B. WAF ルールを作成します。
C. 仮想ホストを強化します。
D. パッチ管理を適用する
正解: **(**正解を表示します**)**

質問: **62**
セキュリティ管理者は、インシデントを調査しているときに、Web サーバー ログで次のことを観察しました。
「GET ../../../../etc/passwd」
セキュリティ管理者が最も遭遇する可能性が高い攻撃は次のどれですか?
A. ディレクトリトラバーサル
B. 権限昇格
C. ブルートフォース
D. 資格情報の再生
正解: **(**正解を表示します**)**

質問: **63**

セキュリティ アナリストは、組織の SIEM からのログを監視しており、営業担当者の 1 人に関連するログを特定しました。

Time	IP address	Location	EmpID	App	Status
14:02	72.45.38.27	Atlanta	25687	VPN	Success
14:04	72.45.38.27	Atlanta	25687	Email	Failure
14:07	58.67.47.48	Beijing	25687	VPN	Success
14:15	72.45.38.27	Atlanta	25687	Teams	Success

ログには次のうちどれが表示されますか?

A. 不可能な移動

B. SMTPリプレイ

C. ディレクトリトラバーサル

D. クロスサイトリクエストフォージェリ

正解: **(**正解を表示します**)**

The logs show the same employee account accessing services from geographically distant locations (Atlanta and Beijing) within a short time frame, which is not physically possible, this is known as impossible travel.

質問: **64**

セキュリティアナリストは、会社のグループポリシーの導入後、ワークステーションの脆弱性が増加していることに気づきました。アナリストがワークステーション上で発見する可能性が高い脆弱性の種類は次のうちどれですか。

A. 設定ミス

B. ゼロデイ

C. 悪意のあるアップデート

D. サプライチェーン

正解: **(**正解を表示します**)**

A misconfiguration vulnerability occurs when system settings - such as those deployed via group policy - are set insecurely, unintentionally weakening security and increasing exposure to threats.

質問: **65**

次のアクティビティのうち、脆弱性管理に関連するものはどれですか? (2 つ選択してください。)

A. レポート

B. 優先順位付け

C. 悪用

D. 相関関係

E. 封じ込め

F. 卓上演習

正解: **(**正解を表示します**)**

Reporting involves documenting and communicating the findings of vulnerability scans and assessments. This allows stakeholders to be informed about existing vulnerabilities and track remediation efforts.
Prioritization is the process of ranking vulnerabilities based on their severity, impact, and exploitability, helping the organization address the most critical vulnerabilities first.

質問: **66**
セキュリティ レポートによると、2 週間のテスト期間中に、従業員の 80% が外部 Web サイトにアクセスする際に無意識のうちに SSO 認証情報を公開していました。組織は、コストのかからないパスワード複雑性テストをシミュレートするために Web サイトを意図的に作成しました。今後、同様の Web サイトへのアクセス回数を減らすのに最も役立つのは次のうちどれですか。
A. フィッシング攻撃を認識するためのキャンペーンを導入します。
B. ウェブサイトの拒否リストを実装します。
C. イントラネットからのすべての送信トラフィックをブロックします。
D. 資格情報を開示した従業員のインターネット アクセスを制限します。
正解: **A (**コメントを発表する**)**

質問: **67**
従来のインフラストラクチャ モデルよりも、Infrastructure as Code (IaC) がセキュリティ アーキテクチャとして推奨される理由は次のとおりです。
A. 一般的な攻撃は効果が低くなります。
B. 構成をより適切に管理および複製できます。
C. ネットワーク防御の専門知識を持つ第三者へのアウトソーシングも可能です。
D. 最適化は、複数のコンピューティング インスタンスにわたって実行できます。
正解: **(**正解を表示します**)**
Infrastructure as Code (IaC) enables automated provisioning and configuration of infrastructure, making environments repeatable, consistent, and scalable. The ability to better manage and replicate configurations ensures that security settings are not missed and reduces misconfigurations.

質問: **68**
システム管理者は、多数のエンド ユーザーのアカウント作成時に時間を節約し、人為的エラーを防ぐスクリプトを作成しています。このタスクに適した使用例はどれですか。
A. 市販ソフトウェア
B. オーケストレーション
C. ベースライン
D. ポリシーの適用
正解: **(**正解を表示します**)**
Orchestration is the process of automating multiple tasks across different systems and applications. It can help save time and reduce human error by executing predefined workflows

and scripts. In this case, the systems administrator can use orchestration to create accounts for a large number of end users without having to manually enter their information and assign permissions.

質問: **69**
セキュリティ管理者は、会社が所有する多数のドメインとサブドメインに証明書を実装するための費用対効果の高いソリューションを模索しています。管理者は、以下のどの種類の証明書を実装すべきでしょうか。
A. ワイルドカード
B. クライアント証明書
C. 自己署名
D. コード署名
正解: (正解を表示します)
Wildcard certificates allow you to secure a domain and all of its subdomains with a single certificate. This can be a cost-effective solution for managing certificates for a large number of domains and subdomains.

質問: **70**
法医学的画像が取得される捜査の段階は次のどれですか?
A. 取得
B. 保存
C. レポート
D. 電子証拠開示
正解: (正解を表示します)
The acquisition phase involves creating forensic images (exact replicas) of storage devices or memory to ensure data integrity for further analysis.

質問: **71**
米国を拠点とするクラウド ホスティング プロバイダーは、データ センターを新しい海外の拠点に拡張したいと考えています。ホスティング プロバイダーが最初に検討すべき事項は次のうちどれですか。
A. 地域のデータ保護規制
B. 他国に居住するハッカーによるリスク
C. 既存の契約上の義務への影響
D. ログ相関におけるタイムゾーンの違い
正解: (正解を表示します)
Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders. Different countries or regions may have different data protection

regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States. A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage. Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there.

質問: **72**
セキュリティエンジニアが社外弁護士からの依頼に対応するために割り当てられました。セキュリティエンジニアは、指定された日付までにすべてのメールのやり取りを提出する必要があります。この依頼に対応するために、以下のどのアクションを最初に実行すべきでしょうか？
A. 影響を受けるデータを識別する訴訟保留通知を送信します。
B. 根本原因分析を決定するためのチームを結成します。
C. 保管チェーンを確立します。
D. 証拠に必要な保存の種類を決定します。
正解: **(**正解を表示します**)**
Sending litigation hold notifications is the first step to ensure that all relevant email correspondence within the specified date range is preserved and not altered or deleted, maintaining compliance with legal requirements.

質問: **73**
内部脅威のシナリオにおいて、悪意のある攻撃者の注意を引く可能性のある手法は次のどれですか?
A. /docs/salaries に偽のテキストファイルを作成する
B. /etc/shadow に弱いパスワードを設定する
C. /etc/crontab で脆弱なジョブをスケジュールする
D. /etc/passwdに偽のアカウントを追加する
正解: **A (**コメントを発表する**)**
A file with a name like "salaries" suggests sensitive information, which would likely draw the attention of an insider threat looking for valuable or confidential data. This technique is often used as part of a honeypot strategy to monitor and detect suspicious activity by insiders attempting unauthorized access.

質問: **74**
システム管理者は、ファイル整合性監視ツールから次のアラートを受信します。
cmd.exe ファイルのハッシュが変更されました。
システム管理者は OS ログをチェックし、過去 2 か月間にパッチが適用されていないことに気付きました。次のどれが最も可能性が高いでしょうか。
A. エンドユーザーがファイルの権限を変更しました。

B. 暗号衝突が検出されました。
C. ファイル システムのスナップショットが取得されました。
D. ルートキットが展開されました。
正解**: D (**コメントを発表する**)**
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS.

質問**: 75**
空港で飛行機を待っているユーザーが、公衆Wi-Fiを使って航空会社のウェブサイトにログインし、セキュリティ警告を無視して座席のアップグレードを購入しました。飛行機が着陸すると、クレジットカードに不正な請求が行われていることに気付きました。以下の攻撃のうち、最も発生確率が高いのはどれですか？
A. リプレイ攻撃
B. メモリリーク
C. バッファオーバーフロー攻撃
D. オンパス攻撃
正解**: D (**コメントを発表する**)**
An on-path attack, also known as a man-in-the-middle (MITM) attack, occurs when an attacker intercepts the communication between two parties (in this case, the user and the airline's website). Since the user was on a public Wi-Fi network and ignored security warnings, it's possible that the attacker was able to intercept the credit card information during the transaction, leading to unauthorized charges.

質問**: 76**
システム管理者は多層防御戦略に取り組んでおり、勤務時間外の従業員の活動を制限する必要があります。システム管理者は次のうちどれを実施すべきでしょうか？
A. ロールベースの制限
B. 属性ベースの制限
C. 必須の制限
D. 時間帯制限
正解**: D (**コメントを発表する**)**
To restrict activity from employees after hours, the systems administrator should implement time-of-day restrictions. This method allows access to network resources to be limited to specific times, ensuring that employees can only access systems during approved working hours. This is

an effective part of a defense-in-depth strategy to mitigate risks associated with unauthorized access during off- hours, which could be a time when security monitoring might be less stringent.
Time-of-day restrictions: These control access based on the time of day, preventing users from logging in or accessing certain systems outside of designated hours.
Role-based restrictions: Control access based on a user's role within the organization.
Attribute-based restrictions: Use various attributes (such as location, department, or project) to determine access rights.
Mandatory restrictions: Typically refer to non-discretionary access controls, such as those based on government or organizational policy.

質問: **77**
承認されていないソフトウェアの導入によって企業ネットワークに脆弱性が生じる可能性が最も高いのは次のどれですか?
A. ハクティビスト
B. スクリプトキディ
C. 競合他社
D. シャドーIT
正解: **(**正解を表示します**)**
Shadow IT refers to information technology systems used within organizations without explicit organizational approval.

質問: **78**
ある組織は、データの損失や悪意のあるコードのインストールを防ぐため、エンドユーザーが会社のデバイスからアクセスすることを許可されていないドメインのリストを公開しました。セキュリティアナリストは、エンドユーザーのワークステーションから新たな疑わしいドメインへのアクセスが複数回成功したことを確認しました。許可されていないドメインへの将来のアクセスを最も効果的に防止できる選択肢はどれですか？
A. ユーザー意識向上トレーニングを割り当てます。
B. 不正コンテンツポリシーを変更します。
C. 許可リストを展開します。
D. プロキシ フィルターを更新します。
正解: **(**正解を表示します**)**

Updating the proxy filters will block access to the new suspicious domain at the network level, effectively preventing users from reaching unauthorized or malicious websites in the future.

質問: **79**
次の契約タイプのうち、ベンダーが応答する必要がある時間枠を定義するのはどれですか?
A. 種をまく
B. サービスレベル保証
C. モア
D. 覚書
正解: **B (**コメントを発表する**)**
A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.

質問: **80**
ある企業が業務をクラウドに移行することを決定しました。ユーザーが会社のアプリケーションを私的にダウンロードすることを防ぎ、アップロードされるデータを制限し、社内でどのアプリケーションが使用されているかを可視化できるテクノロジーを活用したいと考えています。これらの要件を満たす最適なソリューションはどれでしょうか？
A. NGFW
B. CASB
C. アプリケーションのホワイトリスト
D. NG-SWG
正解: **(**正解を表示します**)**
A Cloud Access Security Broker (CASB) would best meet the requirements stated in the scenario. CASBs can provide visibility into which cloud applications are being used across a company, restrict data that is uploaded to the cloud, and prevent unauthorized downloading of company applications for personal use. They act as a gatekeeper, allowing the organization to extend its security policies beyond its own infrastructure. CASBs provide features like visibility, data security, threat protection, and compliance, ensuring secure and only authorized use of cloud services by employees.

質問: **81**
セキュリティチームは組織のネットワークにIPSをインストールし、特定のネットワーク攻撃を検知 防御するためにシステムを設定する必要があります。IPS内で最初に設定すべき設定は次のうちどれですか？
A. 許可リストポリシー

B. パケット検査
C. ログとレポート
D. ファイアウォールルール
正解: **B (**コメントを発表する**)**
Packet inspection is the core functionality of an IPS, as it enables the system to analyze network traffic against signatures and anomalies to detect and prevent specific attacks.

質問: **82**
社内開発されたアプリケーション内でロジック爆弾を使用して組織を標的にする可能性が高い脅威アクターは次のうちどれですか?
A. 国民国家
B. 信頼できるインサイダー
C. 組織犯罪グループ
D. ハクティビスト
正解: **(**正解を表示します**)**
A trusted insider, such as a disgruntled employee or contractor with authorized access to internal systems, is most likely to plant a logic bomb in an internally-developed application since they have both the access and knowledge needed to insert the malicious code.

質問: **83**
ある組織が本社と支社の間で VPN を活用しています。VPN が保護しているのは次のどれですか?
A. 使用中のデータ
B. 転送中のデータ
C. 地理的制限
D. データ主権
正解: **(**正解を表示します**)**
Data in transit is data that is moving from one location to another, such as over a network or through the air. Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it.

質問: **84**
セキュリティ マネージャーは MFA とパッチ管理を実装しています。制御の種類とカテゴリを最もよく表すのは次のどれですか (2 つ選択)。
A. 物理
B. 管理職
C. 探偵
D. 管理者
E. 予防的
F. テクニカル

正解: (正解を表示します)
Multi-Factor Authentication (MFA) and patch management are both examples of preventative and technical controls. MFA prevents unauthorized access by requiring multiple forms of verification, and patch management ensures that systems are protected against vulnerabilities by applying updates. Both of these controls are implemented using technical methods, and they work to prevent security incidents before they occur.

質問: **85**
セキュリティ管理者は、機密性の高い顧客データの流出を防ぐために DLP ソリューションを導入しています。管理者が最初に行うべきことは何ですか?
A. クラウド ストレージ Web サイトへのアクセスをブロックします。
B. 送信メールの添付ファイルをブロックするルールを作成します。
C. データに分類を適用します。
D. ファイル サーバー上の共有からすべてのユーザー権限を削除します。
正解: (正解を表示します)
Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk. Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data.

質問: **86**
セキュリティ コンサルタントは、安全なシステムを物理的に分離したいと考えているクライアントと協力しています。このアーキテクチャを最もよく表すのは次のどれですか。
A. 高可用性
B. コンテナ化された
C. エアギャップ
D. SDN
正解: (正解を表示します)

質問: **87**
管理者は期限切れの SSL 証明書を置き換える必要があります。管理者が新しい SSL 証明書を作成するために必要なのは次のどれですか。
A. CSR
B. OCSP
C. Key
D. CRL
正解: (正解を表示します)

A Certificate Signing Request (CSR) is a request sent to a certificate authority (CA) to issue an SSL certificate. The CSR contains information like the public key, which will be part of the certificate.

質問: **88**
ウイルス、マルウェア、トロイの木馬がインストールされ、ネットワーク全体に広がるのを防ぐためにコンピュータを保護するために使用されるのは次のどれですか?
A. IDS
B. ACL
C. EDR
D. NAC
正解: **(**正解を表示します**)**
Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status.

質問: **89**
侵入テストの報告書では、組織はデータベースの入力検証に関する対策を実装する必要があると指摘されています。テスト中に発見された可能性のある脆弱性の種類を最もよく表しているのは次のうちどれですか。
A. XSS
B. コマンドインジェクション
C. バッファオーバーフロー
D. SQLi
正解: **D (**コメントを発表する**)**
SQL injection (SQLi) exploits improper or missing input validation in database queries, allowing attackers to manipulate SQL commands and access or modify database content.

質問: **90**
ある企業は、従業員が就業時間中に仮想デスクトップからファイルをコピーすることを許可し、就業時間外にはコピーを制限したいと考えています。企業は次のどのセキュリティ対策を実施すべきでしょうか。
A. 時間ベースのアクセス制御
B. デジタル著作権管理

C. ロールベースのアクセス制御
D. ネットワークアクセス制御
正解: (正解を表示します)

質問: **91**
レガシー IoT デバイスの OS に新たにネットワーク アクセスの脆弱性が見つかりました。
この脆弱性を迅速に軽減するには、次のうちどれが最適ですか?
A. 保険
B. パッチ適用
C. セグメンテーション
D. 置換
正解: (正解を表示します)
Segmentation is a technique that divides a network into smaller subnetworks or segments, each with its own security policies and controls. Segmentation can help mitigate network access vulnerabilities in legacy IoT devices by isolating them from other devices and systems, reducing their attack surface and limiting the potential impact of a breach. Segmentation can also improve network performance and efficiency by reducing congestion and traffic. Patching, insurance, and replacement are other possible strategies to deal with network access vulnerabilities, but they may not be feasible or effective in the short term. Patching may not be available or compatible for legacy IoT devices, insurance may not cover the costs or damages of a cyberattack, and replacement may be expensive and time-consuming.

質問: **92**
証明書ベンダーから、最近無効になった証明書を更新する必要がある可能性があるという通知が企業に届きました。セキュリティ管理者は、企業のマシンにインストールされている証明書を更新する必要があるかどうかを判断するために、以下のどのメカニズムを使用すべきでしょうか。
A. SCEP
B. OCSP
C. CSR
D. CRL
正解: (正解を表示します)

From a practical standpoint, an administrator would use automation to compare all existing certificates with the revocation list, but potentially they could also script to OCSP per each certificate in the environment. Either option seem valid, but CRL seems the better option from enterprise scan perspective.

質問: **93**
リモートワーク中の従業員が会社所有のパソコンでショッピングサイトにアクセスし、悪意のあるファイルを含むリンクをクリックします。このファイルのダウンロードを防ぐには、次のうちどれが有効でしょうか？
A. DLP
B. FIM
C. NAC
D. EDR
正解: **(**正解を表示します**)**
An EDR solution actively monitors and blocks malicious behaviors at the endpoint, including intercepting and preventing unauthorized or malicious file downloads, before they can reach the system.

質問: **94**
感染の可能性があるシステムを隔離するために、システム管理者が実行する必要があるアクティビティは次のどれですか?
A. デバイスをエアギャップ環境に移動します。
B. グループ ポリシーを通じてリモート ログインを無効にします。
C. デバイスをサンドボックスに変換します。
D. MDM プラットフォームを使用してデバイスをリモートワイプします。
正解: **(**正解を表示します**)**
Quarantining a potentially infected system by placing it into an air-gapped environment physically disconnects it from the network. This prevents the spread of malware while maintaining the integrity of forensic evidence.

質問: **95**
インシデント対応の一環として根本原因分析を実施する必要がある理由を説明しているのはどれですか?
A. 調査のための証拠を集める
B. 影響を受けたシステムを見つける
C. ネットワーク上のマルウェアの痕跡を根絶する
D. 同様の事件が今後起こらないようにするため
正解: **(**正解を表示します**)**
Root cause analysis is a process of identifying and resolving the underlying factors that led to an incident. By conducting root cause analysis as part of incident response, security professionals

can learn from the incident and implement corrective actions to prevent future incidents of the same nature. For example, if the root cause of a data breach was a weak password policy, the security team can enforce a stronger password policy and educate users on the importance of password security. Root cause analysis can also help to improve security processes, policies, and procedures, and to enhance security awareness and culture within the organization. Root cause analysis is not meant to gather IoCs (indicators of compromise) for the investigation, as this is a task performed during the identification and analysis phases of incident response. Root cause analysis is also not meant to discover which systems have been affected or to eradicate any trace of malware on the network, as these are tasks performed during the containment and eradication phases of incident response.

質問: **96**
ハクティビストの動機として最も可能性が高いのは次のどれでしょうか?
A. 金銭的利益
B. スパイ活動
C. 哲学的信念
D. 復讐
正解: **(**正解を表示します**)**
Hacktivists are typically driven by ideological or political motivations, using hacking to promote or protest specific philosophical beliefs or causes.

質問: **97**
コンテナ イメージを本番環境に展開する前に、次の強化手法のどれを適用する必要がありますか? (2 つ選択してください。)
A. デフォルトのアプリケーションを削除します。
B. NIPS をインストールします。
C. Telnet を無効にします。
D. DNSを再設定します。
E. SFTP サーバーを追加します。
F. 公開証明書を削除します。
正解: **A,C (**コメントを発表する**)**
Removing default applications reduces the attack surface by eliminating unnecessary software that could be exploited. Disabling Telnet is essential because it is an insecure protocol, and leaving it enabled can create vulnerabilities within the container.

質問: **98**
セキュリティ保護された施設への訪問者は、写真付き身分証明書でチェックインし、アクセス制御玄関から施設に入る必要があります。次のうち、この形式のセキュリティ制御を説明しているものはどれですか?
A. 物理

B. 管理職
C. テクニカル
D. 運用中
正解: **(**正解を表示します**)**
A physical security control is a device or mechanism that prevents unauthorized access to a physical location or asset. An access control vestibule, also known as a mantrap, is a physical security control that consists of a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. This prevents unauthorized individuals from following authorized individuals into the facility, a practice known as piggybacking or tailgating. A photo ID check is another form of physical security control that verifies the identity of visitors. Managerial, technical, and operational security controls are not directly related to physical access, but rather to policies, procedures, systems, and processes that support security objectives.

質問: **99**
最高情報責任者(CIO)は、ネットワークデバイスがパブリックインターネットやローカルネットワークに接続してファームウェアを直接アップデートできないようにしたいと考えています。ITチームは、ポータブルデバイスを使用してアップデートプロセスを手動で実行する必要があります。この説明に最も適したアーキテクチャタイプは次のどれですか？
A. マイクロサービス
B. エアギャップ
C. ソフトウェア定義ネットワーク
D. サーバーレス
正解: **(**正解を表示します**)**
An air-gapped architecture physically or logically isolates systems from external and internal networks, preventing direct connectivity and requiring manual methods, such as portable devices, to perform updates.

質問: **100**
セキュリティアナリストは、会社が購入しようとしている SaaS アプリケーションのセキュリティをレビューしています。
セキュリティ アナリストが SaaS アプリケーション ベンダーに要求する必要があるドキュメントは次のうちどれですか。
A. サービスレベル契約
B. 第三者監査
C. 作業明細書
D. データプライバシー契約
正解: **(**正解を表示します**)**
A third-party audit report (such as a SOC 2 or ISO 27001 certification) provides independent validation of the vendor's security controls and assurance of its security posture.

質問: **101**
組織には、財務システムに対する是正管理を実装するという新しい規制要件があります。
新しい要件の理由として最も可能性が高いのは次のどれですか?
A. 銀行の詳細を改ざんする内部者の脅威から身を守るため
B. エラーが他のシステムに渡されないようにするため
C. ビジネス保険を購入できるようにする
D. 財務データへの不正な変更を防ぐため
正解: **(**正解を表示します**)**
Corrective controls, such as auditing and versioning, help prevent unauthorized changes to financial data, ensuring data integrity and compliance with regulations.

質問: **102**
セキュリティ アナリストが会社のパブリック ネットワークをスキャンし、実稼働ネットワークへのアクセスに使用できるリモート デスクトップがホストで実行されていることを発見しました。
セキュリティ アナリストは次のどの変更を推奨すべきでしょうか。
A. リモートデスクトップポートを非標準の番号に変更する
B. VPNを設定し、ジャンプサーバーをファイアウォール内に配置する
C. リモート デスクトップ サーバーからの Web 接続にプロキシを使用する
D. リモートサーバーをドメインに接続し、パスワードの長さを増やす
正解: **B (**コメントを発表する**)**
A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server.

質問: **103**
ある企業は、セキュリティ運用を主導するために、社外からセキュリティ マネージャーを雇いました。
セキュリティ マネージャーがこの新しい役割で最初に実行する必要があるアクションは次のどれですか。
A. セキュリティ ベースラインを確立します。

B. セキュリティ ポリシーを確認します。
C. セキュリティベンチマークを採用します。
D. ユーザー ID の再検証を実行します。
正解**: (**正解を表示します**)**
When a security manager is hired from outside the organization to lead security operations, the first action should be to review the existing security policies. Understanding the current security policies provides a foundation for identifying strengths, weaknesses, and areas that require improvement, ensuring that the security program aligns with the organization's goals and regulatory requirements.
Review security policies: Provides a comprehensive understanding of the existing security framework, helping the new manager to identify gaps and areas for enhancement.
Establish a security baseline: Important but should be based on a thorough understanding of existing policies and practices.
Adopt security benchmarks: Useful for setting standards, but reviewing current policies is a necessary precursor.
Perform a user ID revalidation: Important for ensuring user access is appropriate but not the first step in understanding overall security operations.

質問**: 104**
ユーザーがオンラインフォーラムからソフトウェアをダウンロードしました。ユーザーがソフトウェアをインストールした後、セキュリティチームは、通常とは異なるポートを経由してユーザーのコンピュータに接続する外部ネットワークトラフィックを確認しました。この不正な接続の原因として最も可能性が高いのは次のうちどれですか？
A. ソフトウェアには隠されたキーロガーが含まれていました。
B. ソフトウェアはランサムウェアでした。
C. ユーザーのコンピュータにファイルレス ウイルスが感染していました。
D. ソフトウェアにはバックドアが含まれていました。
正解**: (**正解を表示します**)**
The software contained a backdoor bypassing normal authentication method.

質問**: 105**
システム管理者は、業務を中断することなくシステムを更新する必要があります。システム管理者と会社の経営陣が合意すべき事項は次のうちどれですか？
A. メンテナンスウィンドウ
B. バックアウト計画
C. 標準操作手順
D. 影響分析
正解**: A (**コメントを発表する**)**
A maintenance window is a scheduled period agreed upon in advance during which updates or changes can be made without disrupting normal business operations.

質問: **106**
マーケティング部門は、関係部門に通知せずに独自のプロジェクト管理ソフトウェアを導入しました。このシナリオを説明するのは次のどれですか。
A. シャドーIT
B. 内部脅威
C. データの引き出し
D. サービス中断
正解: **(正解を表示します)**
Explanation:Shadow IT is the term used to describe the use of unauthorized or unapproved IT resources within an organization. The marketing department set up its own project management software without telling the appropriate departments, such as IT, security, or compliance. This could pose a risk to the organization's security posture, data integrity, and regulatory compliance.

質問: **107**
訪問者はロビーのネットワーク ジャックにラップトップを接続し、会社のネットワークに接続できます。
このアクティビティを最も効果的に防止するには、既存のネットワーク インフラストラクチャで次のどれを構成する必要がありますか?
A. ポートセキュリティ
B. トランスポート層セキュリティ
C. 仮想プライベートネットワーク
D. Web アプリケーション ファイアウォール
正解: **(正解を表示します)**

質問: **108**
バグ報奨金プログラムを開始することによる利点は次のどれですか? (2 つ選択してください。)
A. 組織の評判の向上
B. ゼロデイ脆弱性の数の削減
C. 従業員のセキュリティ意識の向上
D. プログラム管理コストの削減
E. 脆弱性のより迅速な発見

F. パッチ管理プロセスの改善
正解: (正解を表示します)
A bug bounty program can improve an organization's reputation by demonstrating a proactive approach to security.
It enables quicker discovery of vulnerabilities by leveraging external researchers to identify issues faster than internal teams alone.

質問: **109**
サポート終了したアプリケーションをネットワーク上で使用している企業にとって、リスクとなるのは次のどれですか?
A. サービスポートを開く
B. デフォルトの資格情報
C. 安全でないネットワーク
D. 脆弱なソフトウェア
正解: (正解を表示します)

質問: **110**
車両による損傷を防ぐための最も効果的な物理的セキュリティ制御は次のどれですか?
A. 警備員
B. フェンシング
C. 照明
D. ボラード
正解: (正解を表示します)
Bollards serve as a robust physical barrier designed to withstand and absorb the kinetic impact of a vehicle, thereby preventing unauthorized vehicular access or accidental collisions that could cause structural damage or endanger personnel.

質問: **111**
DNS シンクホールの使用例を最もよく表しているのは次のうちどれですか?
A. 攻撃者は、DNS シンクホールを、企業のドメイン構造を識別するための非常に貴重なリソースと見なすことができます。
B. DNS シンクホールは、従業員を既知の安全な Web サイトから攻撃者が所有する悪意のある Web サイトへと誘導するために使用される可能性があります。
C. DNS シンクホールは、攻撃者が使用する既知の悪意のあるドメインへのトラフィックをキャプチャするために使用できます。
D. DNS シンクホールを設定すると、潜在的な攻撃者を企業のネットワーク リソースから遠ざけることができます。
正解: (正解を表示します)
DNS sinkhole intercepts attempts to visit harmful websites and redirects them so you don't end up reaching a malicious website and keeps your computer safe.

質問: **112**
ユーザーが顧客に請求書を送信しようとしました。請求書が届いたかどうかを確認するために顧客に連絡したところ、顧客からスパムフォルダに入っていたとの連絡がありました。経営陣はシステム管理者に対し、サーバー認証を導入することでこのような事態の再発を防ぐ対策を実施するよう指示しました。システム管理者が実施すべき対策は次のうちどれですか？
A. SPF
B. DMARC
C. XDR
D. DNSSEC
正解: **(正解を表示します)**
SPF (Sender Policy Framework) lets the domain owner specify which mail servers are authorized to send email on its behalf. Publishing an SPF record in DNS helps recipient mail systems verify the sending server's legitimacy, reducing the chance that legitimate messages are marked as spam.

質問: **113**
ある企業の最高情報セキュリティ責任者(CISO)は、インシデント対応チームの能力強化を希望しています。CISOは、インシデント対応チームに対し、侵害の可能性があるシステムのホストおよびネットワークデータを迅速に分析し、さらなる相関分析とレポート作成のためにデータを転送するツールを導入するよう指示しました。インシデント対応チームは、以下のツールのうちどれを導入すべきでしょうか？
A. NAC
B. IPS
C. SIEM
D. EDR
正解: **D (コメントを発表する)**
EDR agents sit on hosts, continuously collect rich telemetry (processes, connections, file changes), and can capture network indicators from those endpoints. They rapidly analyze this data locally and ship it to a backend where it's correlated and reported - that's what the CISO wants to speed detection and investigation of compromised systems.

質問: **114**
金融業界で機密データを隠すために最もよく使用されるソリューションは次のどれですか?
A. トークン化
B. ハッシュ
C. 塩漬け
D. ステガノグラフィー
正解: **A (コメントを発表する)**

Tokenization replaces sensitive data, such as credit card numbers, with non-sensitive equivalents (tokens) that have no exploitable value outside the system. It is widely used in the financial industry to protect data while maintaining functionality for processing and analysis.

質問: **115**
ネットワーク エンジニアは、ネットワーク デバイスの全体的なセキュリティを強化しており、デバイスを強化する必要があります。
このタスクを最も効果的に達成できるのは次のどれでしょうか?
A. HTTP管理を有効にする
B. Telnet を SSH に置き換える
C. 集中ログの構成
D. ローカル管理者アカウントの生成
正解: **(**正解を表示します**)**

質問: **116**
ある企業のセキュリティチームは事業継続計画を見直しており、災害発生後の業務再開に必要な時間を決定する必要があります。セキュリティチームが決定しようとしている時間枠について、以下のどれが当てはまりますか？
A. 回復時間目標
B. リカバリポイント目標
C. 平均故障間隔
D. 平均修復時間
正解: **A (**コメントを発表する**)**
RTO is the maximum acceptable downtime: the target window within which systems and operations must be restored after a disruption. When the team asks "how long until we're back up?", they're defining the RTO.

質問: **117**
次のうち、VoIP に関連する一般的な脆弱性はどれですか (2 つ選択してください)。
A. スピム
B. フィッシング
C. VLANホッピング
D. フィッシング
E. DHCPスヌーピング
F. テールゲーティング
正解: **A,B (**コメントを発表する**)**
SPIM (Spam over Internet Messaging) poses a threat to VoIP systems by consuming bandwidth, diverting resources, and potentially causing denial of service attacks. The influx of SPIM messages can degrade the quality of VoIP calls, overload servers, and serve as a platform for social engineering attacks, jeopardizing the security of VoIP users. To mitigate these risks,

organizations should implement spam filters, intrusion detection systems, and regular software updates while also educating users to recognize and avoid potential threats associated with SPIM.

質問: **118**
ビジネス影響分析を実施する際の RTO の利点は次のどれですか?
A. インシデントの発生可能性とそのコストを決定します。
B. インシデント対応者の役割と責任を決定します。
C. インシデント発生後にシステムを復元する状態を決定します。
D. インシデント発生後に組織がダウンタイムを許容できる時間を決定します。
正解: **D (**コメントを発表する**)**
The Recovery Time Objective (RTO) specifies the maximum acceptable duration that a system or service can be unavailable following a disruption, directly defining tolerated downtime limits.

質問: **119**
従業員がベンダーから添付ファイル付きのマーケティングコミュニケーションメールを受け取りました。従業員が添付ファイルを開くと、画面に奇妙なテキストが表示され、データの復旧と引き換えに料金の支払いを要求しました。数秒後、全社宛てのメールが従業員に送信され、コンピュータをインターネットから切断し、シャットダウンするよう要求されました。このタイプのマルウェアを説明するものは次のうちどれですか？
A. トロイの木馬
B. ワーム
C. ランサムウェア
D. ウイルス
正解: **C (**コメントを発表する**)**
Ransomware encrypts a user's files (displaying garbled text) and demands payment to restore access, matching the behavior described.

質問: **120**
EDR ソリューションは、特定のワークステーションに悪意のある IP への送信トラフィックがあることを認識します。
脅威を封じ込めるために取るべき最善の行動は次のどれでしょうか?
A. そのワークステーションにアクセスするすべてのユーザーのパスワードを変更します。
B. 即時対応の一環としてワークステーションを隔離します。
C. ワークステーションは脆弱である可能性が高いため、パッチを適用してください。
D. そのワークステーションに影響する強化とポリシーを確認します。
正解: **(**正解を表示します**)**
Isolating the workstation immediately stops communication with the malicious IP and prevents further spread or data exfiltration, making it the most effective containment action.

質問: **121**
EDR ソリューションは次のどのセキュリティ カテゴリに属しますか?
A. テクニカル
B. 物理
C. 管理職
D. 運用中
正解: (正解を表示します)

質問: **122**
次のどれがメモリインジェクションの例ですか?
A. 実行可能ファイルがディスク上で上書きされ、次回実行時に悪意のあるコードが実行されます。
B. 悪意のあるコードが、すでに実行中のプロセスの割り当てられた領域にコピーされます。
C. 2 つのプロセスが同じ変数にアクセスし、一方のプロセスが権限昇格を引き起こす可能性があります。
D. プロセスが予期しない量のデータを受信し、悪意のあるコードが実行されます。
正解: (正解を表示します)

質問: **123**
組織は、内部からの脅威を防ぐために、ユーザーの活動を監視する必要があります。次のソリューションのうち、組織がこの目標を達成するのに役立つものはどれですか。
A. 行動分析
B. アクセス制御リスト
C. アイデンティティとアクセス管理
D. ネットワーク侵入検知システム
正解: (正解を表示します)
Behavioral analytics tools monitor user actions and detect anomalies that may indicate insider threats, such as unauthorized access or unusual data exfiltration activities. These tools establish baselines for normal behavior and flag deviations.

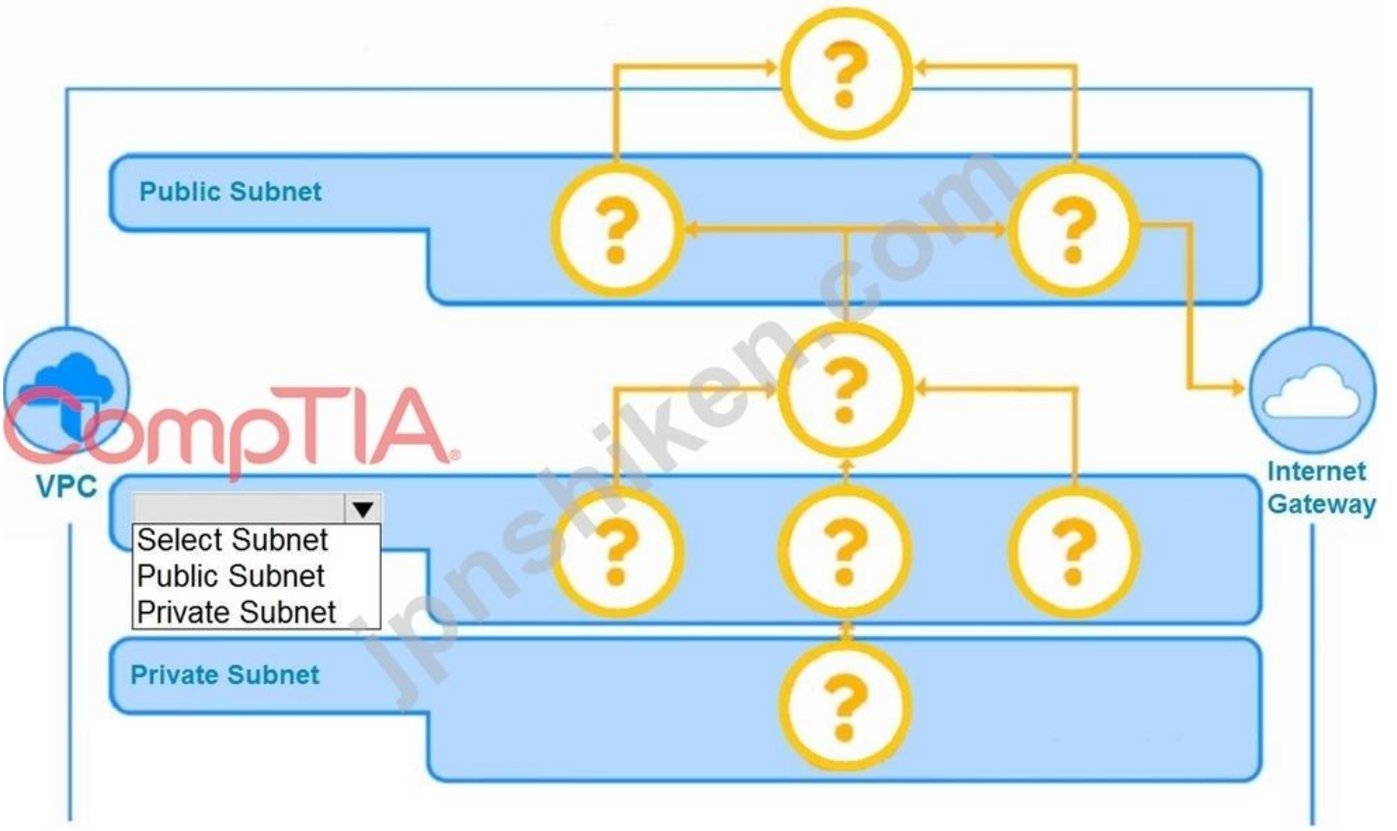
質問: **124**
シミュレーション2

セキュリティ アナリストは、サードパーティのクラウド サービス プロバイダーによってホストされる同社の新しい顧客向け支払いアプリケーションのネットワーク ダイアグラムの初版を作成しています。

説明書

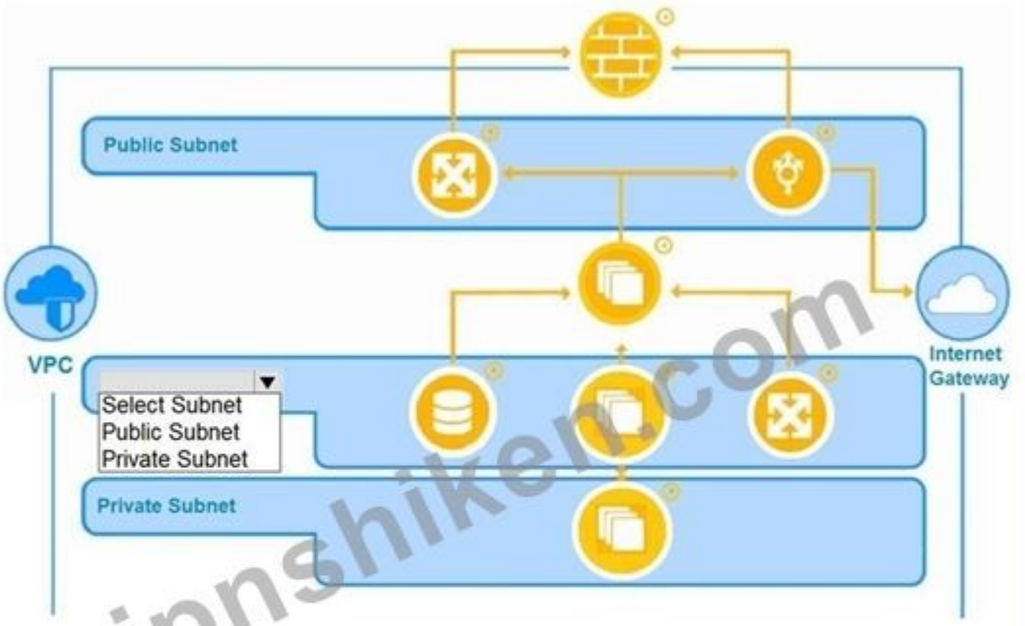
？をクリックして適切なアイコンを選択し、安全で冗長性のあるWebアプリケーションを作成してください。ドロップダウンメニューを使用して適切なサブネットタイプを選択してください。図内のすべてのスペースを埋めてください。

いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。



正解:

The diagram should be filled in the way shown below.



WAF (Web Application Firewall) at the top to handle incoming traffic from the Internet Gateway.
Load Balancer for distributing traffic between instances.
Instances for handling the application workloads, ensuring multiple instances for redundancy.
Autoscaling Instance to adjust the number of instances based on demand dynamically.

In the middle of the diagram, you should select **Private Subnet** in the dropdown menu.

This choice is appropriate because the elements in the lower section, especially the **Database** instances, are part of the private subnet. Placing databases in a private subnet adds an additional layer of security, as it prevents direct internet access to sensitive data. The private subnet is also typically used for backend resources that don't need to be exposed publicly.

質問: **125**
弁護士は、複数のワークステーションと受付デスクの近くにあるオフィススペースで、機密文書をコピー機で印刷しようとしていました。弁護士が文書を取りにコピー機へ向かうと、文書がなくなっていました。
この再発を防ぐには、次のうちどれが最適ですか?
A. コピー機を法務部門に設置します。
B. 弁護士のワークステーションで DLP を構成します。
C. プリンタで LDAP 認証を設定します。
D. 物理的な侵入テストを実施します。
正解: **(**正解を表示します**)**
LDAP authentication on the printer would require users to authenticate before printing, enabling secure print release. This ensures that documents are not printed until the authorized user is physically present, which directly addresses the issue of missing confidential documents.

質問: **126**

運用サーバーに影響を与えずに潜在的な攻撃者の活動を特定するために使用できるのは次のうちどれですか?
A. ハニーポット
B. ビデオ監視
C. ゼロトラスト
D. ジオフェンシング
正解**: A (**コメントを発表する**)**
A honey pot is a system or a network that is designed to mimic a real production server and attract potential attackers. A honey pot can be used to identify the attacker's methods, techniques, and objectives without affecting the actual production servers. A honey pot can also divert the attacker's attention from the real targets and waste their time and resources. The other options are not effective ways to identify potential attacker activities without affecting production servers:
Video surveillance: This is a physical security technique that uses cameras and monitors to record and observe the activities in a certain area. Video surveillance can help to deter, detect, and investigate physical intrusions, but it does not directly identify the attacker's activities on the network or the servers.
Zero Trust: This is a security strategy that assumes that no user, device, or network is trustworthy by default and requires strict verification and validation for every request and transaction. Zero Trust can help to improve the security posture and reduce the attack surface of an organization, but it does not directly identify the attacker's activities on the network or the servers. Geofencing: This is a security technique that uses geographic location as a criterion to restrict or allow access to data or resources. Geofencing can help to protect the data sovereignty and compliance of an organization, but it does not directly identify the attacker's activities on the network or the servers.

質問**: 127**
ある企業は、開発したソフトウェアが最終版完成後に改ざんされないことを保証したいと考えています。この企業にとって最も適切な対策は次のどれでしょうか。
A. ハッシュ
B. 暗号化
C. ベースライン
D. トークン化
正解**: (**正解を表示します**)**
Hashing ensures integrity of software by detecting any unauthorized changes or tampering after its final version.

質問**: 128**
ハード ドライブを再利用できるようにしながら、ハード ドライブに含まれるデータをサニタイズするために使用できる技術は次のどれですか。
A. ドライブシュレッダー

B. ワイプツール
C. 消磁
D. 保持プラットフォーム
正解: **(**正解を表示します**)**

質問: **129**
セキュリティ インシデントが発生した後、システム管理者は会社に NAC プラットフォームの購入を依頼します。システム管理者が保護しようとしている攻撃対象領域は次のどれですか。
A. ブルートゥース
B. 有線
C. NFC
D. SCADA
正解: **(**正解を表示します**)**
A NAC (network access control) platform is a technology that enforces security policies on devices that attempt to access a network. A NAC platform can verify the identity, role, and compliance of the devices, and grant or deny access based on predefined rules. A NAC platform can protect both wired and wireless networks, but in this scenario, the systems administrator is trying to protect the wired attack surface, which is the set of vulnerabilities that can be exploited through a physical connection to the network.

質問: **130**
プログラム マネージャーは、契約社員が会社のコンピュータを月曜日から金曜日の午前 9 時から午後 5 時までしか使用できないようにしたいと考えています。このアクセス制御を最も効果的に実施するには、次のうちどれが適切でしょうか。
A. すべての契約社員のGPOを作成し、時間帯によるログイン制限を設定する
B. 契約社員に対する裁量アクセスポリシーの作成とルールベースのアクセス設定
C. OAuth サーバーを実装し、契約社員に最小限の権限を設定する
D. 契約社員の認証サーバーへのフェデレーションによるSAMLの実装
正解: **(**正解を表示します**)**
The most appropriate method is to use a Group Policy Object (GPO) with time-of-day restrictions. This is a native capability in Windows environments that allows administrators to control when users are allowed to log in to domain-joined systems.

質問: **131**
システム管理者はクラウド環境へのVPNアクセスを正常に構成しました。リモート管理を最も効率的に行うために、管理者は次のどの機能を使用すべきでしょうか？
A. 共有サービスセキュリティゾーン内のジャンプホスト
B. 企業LAN内のSSHサーバー
C. ファイアウォール上のリバースプロキシ
D. 条件付きアクセスを備えたMDMソリューション

正解: (正解を表示します)
A jump host in a shared services security zone is specifically designed to provide secure access to remote environments, such as a cloud environment, while ensuring that access is monitored and controlled. This setup facilitates remote administration by providing a dedicated entry point, allowing administrators to access sensitive network areas through a secure, segmented pathway. This setup minimizes direct exposure to the cloud environment and enhances security.

質問: **132**
ある組織は、ランサムウェア対策のための新しいソリューションのライセンス費用を評価しています。この決定を下す上で、最も役立つのは次のうちどれですか？
A. エール
B. SLE
C. RTO
D. ARO
正解: (正解を表示します)
Annual Loss Expectancy (ALE) estimates the yearly financial impact of a risk, helping the organization compare the potential cost of ransomware incidents against the cost of licensing the prevention solution.

質問: **133**
ある組織は 忘れられる権利」に関する規制を考慮に入れませんでした。この行動は、会社にどのような影響を与える可能性がありますか？
A. 罰金
B. データ侵害損失
C. 収益損失
D. 脅迫
正解: (正解を表示します)
Failing to comply with right-to-be-forgotten regulations, such as GDPR requirements, can lead to legal penalties and fines from regulatory authorities.

質問: **134**
効果的な変更管理手順を説明しているのは次のどれですか?
A. デプロイメントが成功した後に変更を承認する
B. パッチが失敗した場合のバックアウト計画がある
C. 変更を追跡するためのスプレッドシートの使用
D. セキュリティ更新の自動変更管理バイパスを使用する
正解: (正解を表示します)
Effective change management includes having a backout plan, so that if a patch or change fails, systems can be restored to their previous, stable state.

質問: **135**
最高情報責任者 (CIO) は、ベンダーのサービスが満たすコンプライアンス フレームワーク内の特定の目標を詳述したドキュメントをベンダーに提供するよう依頼しました。ベンダーは、サービスが 21 の目標のうち 17 を満たしていることを示すレポートと署名入りの手紙を提供しました。ベンダーが CIO に提供したのは次のどれですか。
A. 第三者監査レポート
B. 自己評価結果
C. 侵入テストの結果
D. コンプライアンスの証明
正解: **(**正解を表示します**)**

質問: **136**
ある企業は、企業内で広く使用されているネットワーク デバイス ベンダーが政府によって禁止されたという警告を受け取ります。
これらのデバイスのハードウェア更新時に、会社の法務顧問が最も懸念すると思われるのは次のどれですか?
A. 制裁
B. データ主権
C. 交換費用
D. ライセンスの喪失
正解: **(**正解を表示します**)**
The ban represents a government-imposed sanction; the general counsel must ensure the hardware refresh avoids any continued use or procurement of the sanctioned vendor's devices to remain legally compliant.

質問: **137**
中小企業の管理者は、なりすましの Web サイトにアクセスしようとした後にページがブロックされたというメッセージを受け取る従業員からのサポート コールが増加していることに気付きました。管理者は次のうちどれを行う必要がありますか。
A. 多要素認証を導入します。
B. ウェブフィルタ設定のレベルを下げる
C. セキュリティ意識向上トレーニングを実施します。

D. 利用規定を更新する
正解: **(**正解を表示します**)**
In this scenario, employees are attempting to navigate to spoofed websites, which is being blocked by the web filter. To address this issue, the administrator should implement security awareness training. Training helps employees recognize phishing and other social engineering attacks, reducing the likelihood that they will attempt to access malicious websites in the future.
* Deploying multifactor authentication (MFA) would strengthen authentication but does not directly address user behavior related to phishing websites.
* Decreasing the level of the web filter would expose the organization to more threats.
* Updating the acceptable use policy may clarify guidelines but is not as effective as hands-on training for improving user behavior.

質問: **138**
セキュリティアナリストがデバイス上のブロートウェアを回避するために使用する可能性が最も高い緩和手法は次のどれですか?
A. 無効なポート/プロトコル
B. アプリケーション許可リスト
C. デフォルトのパスワードの変更
D. アクセス制御権限
正解: **(**正解を表示します**)**
An application allow list ensures that only approved applications can be installed or run on a device, effectively preventing the installation of unwanted bloatware.

質問: **139**
割り当てられた職務を効果的に遂行するために必要な権限をユーザーが持っていることを確認するには、次のうちどれを使用する必要がありますか?
A. デフォルトのパスワードの変更
B. 最小権限の実装
C. ベースライン構成の適用
D. ネットワークセグメンテーションの適用
正解: **(**正解を表示します**)**
The principle of least privilege ensures users are granted only the permissions necessary to perform their specific job functions, minimizing the risk of unauthorized access or actions.

質問: **140**
オンボーディング プロセス中に、従業員はイントラネット アカウントのパスワードを作成する必要があります。
パスワードには、10 個の文字、数字、文字、および 2 つの特殊文字を含める必要があります。
パスワードが作成されると、会社はイントラネット プロファイルに基づいて、従業員に会社所有の他の Web サイトへのアクセスを許可します。イントラネット アカウントを保護し、ユーザーの

イントラネット アカウントに基づいて複数のサイトへのアクセスを許可するために、会社が使用するアクセス管理の概念は次のどれですか (2 つ選択)。
A. 連邦
B. 本人確認
C. パスワードの複雑さ
D. デフォルトのパスワードの変更
E. パスワードマネージャー
F. オープン認証
正解: **(**正解を表示します**)**
Federation is an access management concept that allows users to authenticate once and access multiple resources or services across different domains or organizations. Federation relies on a trusted third party that stores the user's credentials and provides them to the requested resources or services without exposing them. Password complexity is a security measure that requires users to create passwords that meet certain criteria, such as length, character types, and uniqueness. Password complexity can help prevent brute-force attacks, password guessing, and credential stuffing by making passwords harder to crack or guess.

質問: **141**
管理者は、すべてのユーザー ワークステーションとサーバーに、拡張子 .ryk を含むファイルに関連付けられたメッセージが表示されていることに気付きました。システムに存在する感染の種類は次のどれですか。
A. ウイルス
B. トロイの木馬
C. スパイウェア
D. ランサムウェア
正解: **(**正解を表示します**)**
Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms.

質問: **142**
従業員を異なる役割に割り当てることで不正行為を検出するために最も効果的なのは次のうちどれですか?
A. 最小権限
B. 強制休暇
C. 職務の分離
D. ジョブローテーション
正解: **(**正解を表示します**)**

Job rotation is a strategy used in organizations to detect and prevent fraud by periodically assigning employees to different roles within the organization. This approach helps ensure that no single employee has exclusive control over a specific process or set of tasks for an extended period, thereby reducing the opportunity for fraudulent activities to go unnoticed. By rotating roles, organizations can uncover irregularities and discrepancies that might have been concealed by an employee who had prolonged access to sensitive functions. Job rotation also promotes cross-training, which can enhance the organization's overall resilience and flexibility.

質問: **143**
経理担当者は、新しい口座を使用するよう不正な指示を受け、攻撃者の銀行口座に送金しました。今後、このような行為を阻止できる可能性が最も高いのは次のうちどれですか。
A. セキュリティインシデント報告の標準化
B. 定期的なフィッシングキャンペーンの実行
C. 内部脅威検出対策の実施
D. 電信送金の送信プロセスの更新
正解: **(**正解を表示します**)**
To prevent an accounting clerk from sending money to an attacker's bank account due to fraudulent instructions, the most effective measure would be updating the processes for sending wire transfers. This can include implementing verification steps, such as requiring multiple approvals for changes in payment instructions and directly confirming new account details with trusted sources.
Updating processes for sending wire transfers: Involves adding verification and approval steps to prevent fraudulent transfers.
Standardizing security incident reporting: Important for handling incidents but not specifically focused on preventing fraudulent wire transfers.
Executing regular phishing campaigns: Helps raise awareness but may not directly address the process vulnerability.
Implementing insider threat detection measures: Useful for detecting malicious activities but does not directly prevent fraudulent transfer instructions.

質問: **144**
セキュリティ管理者は、組織を悪意のあるインバウンドトラフィックから保護するために、即座に行動を起こす自動化ソリューションを必要としています。次のうち、最適なソリューションはどれですか？
A. UEM
B. IPS
C. WAF
D. VPN
正解: **(**正解を表示します**)**
An Intrusion Prevention System (IPS) automatically detects and blocks malicious network traffic in real time, providing immediate protection against inbound threats.

質問: **145**
公式アプリケーション ストア以外の手段でデバイスにアプリケーションが不正にインストールされることを指す脆弱性のタイプは次のどれですか。
A. クロスサイトスクリプティング
B. バッファオーバーフロー
C. 脱獄
D. サイドローディング
正解: **D (**コメントを発表する**)**
Side loading refers to the process of installing applications on a device from outside the official app store, which can introduce security vulnerabilities by bypassing standard app validation processes.

質問: **146**
IT マネージャーは、データ分類イニシアチブによって機密データが環境から流出する可能性があることが判明した後、組織のセキュリティ機能を強化しています。次のソリューションのどれがリスクを軽減しますか?
A. XDR
B. SPF
C. DLP
D. DMARC
正解: **(**正解を表示します**)**
To mitigate the risk of sensitive data being exfiltrated from the environment, the IT manager should implement a Data Loss Prevention (DLP) solution. DLP monitors and controls the movement of sensitive data, ensuring that unauthorized transfers are blocked and potential data breaches are prevented.
XDR (Extended Detection and Response) is useful for threat detection across multiple environments but doesn't specifically address data exfiltration.
SPF (Sender Policy Framework) helps prevent email spoofing, not data exfiltration.
DMARC (Domain-based Message Authentication, Reporting & Conformance) also addresses email security and spoofing, not data exfiltration.

質問: **147**
高可用性 Web サイトを持つ企業は、どんな犠牲を払ってでも管理を強化したいと考えています。企業は、起こりうる問題をすべて見つけて、サイトのセキュリティを確保したいと考えています。この目標を達成できる可能性が最も高いのは次のうちどれでしょうか。
A. 権限制限
B. バグ報奨金プログラム
C. 脆弱性スキャン
D. 偵察

正解: (正解を表示します)
A bug bounty program leverages a large, diverse community of security researchers who use a wide range of testing methods to uncover vulnerabilities. This crowd-sourced approach maximizes the chances of finding any possible issue, far beyond what a single scan or internal team could achieve.

質問: **148**
ある会社のウェブサーバーが、非標準のパス上にある、信頼性の低いパブリックIPアドレスへのアウトバウンドトラフィックを送信しています。このウェブサーバーは、会社に画像をアップロードするクライアントに、認証されていないページを表示するために使用されています。アナリストは、会社の開発チームが作成したものではない、サーバー上で不審なプロセスが動作していることに気付きました。このセキュリティインシデントの原因として最も可能性が高いのは次のうちどれですか？
A. ページを通じて Web シェルがサーバーに展開されました。
B. 脆弱性が悪用され、サーバーにワームが展開されました。
C. 悪意のある内部者がサーバーを使用して暗号通貨をマイニングしています。
D. 攻撃者は、公開された RDP ポート経由でサーバーにルートキットトロイの木馬を展開しました。
正解: (正解を表示します)
The shell would allow the attacker to gain unauthorized access and control over the server.

質問: **149**
ある組織がCOPEモバイルデバイス管理ポリシーを導入しようとしています。COPEポリシーに含めるべき項目は次のうちどれですか？(2つ選択してください。)
A. 8文字のパスワードを要求する
B. 従業員データの所有権
C. デバイスのリモートワイプ
D. データ暗号化
E. 個人アプリケーションストアへのアクセス
F. データ使用量の上限
正解: (正解を表示します)

質問: **150**
主要なアプリケーションとソフトウェアを安全に構築するために、開発者と防御的テスト手法と攻撃的テスト手法の両方を使用するテスト手法は次のどれですか。
A. 青
B. 黄色
C. 赤
D. 緑
正解: **B** (コメントを発表する)

The Yellow Team is a relatively newer concept in cybersecurity testing that combines both defensive (Blue Team) and offensive (Red Team) methodologies. This team works with developers to securely build key applications and software by integrating security practices throughout the development lifecycle, also known as Secure Development Lifecycle (SDLC). Their focus is on proactively addressing vulnerabilities while also testing the application for security flaws from an attacker's perspective.

質問: **151**
ある会社では、すべてのラップトップに資産目録ステッカーを貼り、従業員 ID と関連付けるようになりました。これらのアクションによって得られるセキュリティ上の利点は次のうちどれですか? (2 つ選択してください。)
A. 侵入テストを実施する際、セキュリティ チームは目的のラップトップをターゲットにすることができます。
B. ユーザーベースのファイアウォール ポリシーを適切なラップトップに正しく適用できます。
C. セキュリティ チームは、適切なデバイスにユーザー意識向上トレーニングを送信できるようになります。
D. 従業員が組織を退職した場合でも、会社のデータを把握できます。
E. ソフトウェア MFA トークンを構成するときに、ユーザーをデバイスにマッピングできます。
F. デバイス上でセキュリティ インシデントが発生した場合、適切な従業員に通知できます。
正解: **(**正解を表示します**)**

質問: **152**
最近、ある従業員が会社を退職しました。この従業員は、過去 5 年間、毎週のバッチ ジョブの管理とサポートを担当していました。従業員が退職してから数週間後、バッチ ジョブの 1 つが通信し、大きな混乱を引き起こしました。このタイプのインシデントの再発を防ぐには、次のうちどれが最も効果的でしょうか。
A. ジョブローテーション
B. 保持
C. アウトソーシング
D. 職務の分離
正解: **A (**コメントを発表する**)**

Job rotation is a security control that involves regularly moving employees to different roles within an organization. This practice helps prevent incidents where a single employee has too much control or knowledge about a specific job function, reducing the risk of disruption when an employee leaves. It also helps in identifying any hidden issues or undocumented processes that could cause problems after an employee's departure.

質問: **153**
原産国の法律と要件に従いながら、原産国外で情報が保存されるという概念を最もよく表しているのは、次のうちどれですか。
A. データ主権
B. 地理位置情報
C. 知的財産
D. 地理的制限
正解: **(**正解を表示します**)**
Data sovereignty refers to the principle that data stored in another country remains subject to the originating country's laws. This is a common concern in cloud computing.

質問: **154**
最高情報セキュリティ責任者は、PLI を保護するためのセキュリティ対策を講じたいと考えています。この目標を達成するには、組織は既存のラベル付けおよび分類システムを使用する必要があります。要件を満たすように構成する可能性が高いのは次のうちどれですか。
A. トークン化
B. S/MIME
C. DLP
D. MFA
正解: **C (**コメントを発表する**)**
Data Loss Prevention (DLP) systems are typically configured to protect sensitive data such as Personally Identifiable Information (PII) within an organization. DLP tools enforce policies that monitor, detect, and block the unauthorized transmission of sensitive data. By leveraging the organization's existing labeling and classification system, DLP solutions can identify and protect data based on its classification, ensuring that PII is appropriately secured according to organizational policies.

質問: **155**
セキュリティ チームには、レガシー デバイスへのアクセスを提供する新しい分離されたネットワーク セグメント (10.9.8.14) に対して、ホスト A (10.2.2.7) とホスト B (10.3.9.9) のみを有効にするように依頼されています。
他のすべてのホストからのアクセスはブロックする必要があります。ファイアウォールに追加する必要があるエントリは次のうちどれですか？

A.
```
Permit 10.2.2.0/24 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27
```

B.
```
Deny 0.0.0.0/0 to 10.9.8.14/27
Permit 10.2.2.0/24 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27
```

C.
```
Permit 10.2.2.7/32 to 10.9.8.14/27
Permit 10.3.9.9/32 to 10.9.8.14/27
Deny 0.0.0.0/0 to 10.9.8.14/27
```

D.
```
Permit 10.2.2.7/32 to 10.9.8.14/27
Permit 10.3.9.0/24 to 10.9.8.14/27
Deny 10.9.8.14/27 to 0.0.0.0/0
```

正解: **C** (コメントを発表する)

Permit 10.2.2.7/32 to 10.9.8.14/27: This rule allows host A (10.2.2.7) specific access to the isolated network (10.9.8.14/27).
Permit 10.3.9.9/32 to 10.9.8.14/27: This rule allows host B (10.3.9.9) specific access to the isolated network (10.9.8.14/27).
Deny 0.0.0.0/0 to 10.9.8.14/27: This rule blocks access from all other IPs to the isolated network (10.9.8.14/27).

質問: **156**

次の攻撃のうち、安全でないネットワークを主に標的とするものは何ですか?

A. 邪悪な双子
B. なりすまし
C. 水飲み場
D. プリテキスティング

正解: (正解を表示します)

An evil twin attack sets up a rogue wireless access point that mimics a legitimate one, targeting insecure or poorly secured networks to capture user data.

質問: **157**

ある組織で、ハッカーがダークウェブで見つけた2年前の標準ユーザーのパスワードを悪用したために、情報漏洩が発生しました。この攻撃を防ぐことができたのは次のうちどれですか?

A. 特権アクセス管理
B. アカウントロックアウト
C. 再利用ポリシー
D. 複雑さの要件

正解: **C** (コメントを発表する)

A reuse policy prevents users from using old passwords, which helps protect accounts even if previous passwords are compromised and available on the dark web.

質問: **158**
インフラストラクチャの展開を自動化しようとする組織では、次のテクノロジのどれを使用する必要がありますか?
A. IaC
B. IaaS
C. IoC
D. IoT
正解: **A (**コメントを発表する**)**
Infrastructure as Code (IaC) expresses infrastructure configurations in executable code, enabling automated, repeatable deployment and management of servers, networks, and other resources.

質問: **159**
システム管理者は、ユーザーの責任に基づいて、ユーザーがデータにアクセスできないようにしたいと考えています。また、管理者は、必要なアクセス構造を簡略化された形式で適用したいと考えています。管理者は、次のどれをサイト回復リソース グループに適用する必要がありますか?
A. RBAC
B. ACL
C. SAML
D. GPO
正解: **(**正解を表示します**)**
RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format.

質問: **160**
許可された担当者だけが安全な施設にアクセスできるようにするには、次のどれが最適な方法でしょうか (2 つ選択)。
A. フェンシング
B. ビデオ監視
C. バッジアクセス
D. アクセス制御玄関
E. サインインシート
F. センサー
正解: **C,D (**コメントを発表する**)**

Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened. This prevents tailgating or piggybacking by unauthorized individuals.

質問: **161**
システム管理者は、会社の最高経営責任者を名乗る未知の番号からテキスト メッセージを受け取ります。メッセージには、緊急事態のためパスワードをリセットする必要があると書かれています。次のどの脅威ベクトルが使用されていますか?
A. タイプミススクワッティング
B. スミッシング
C. プリテキスティング
D. なりすまし
正解: **(**正解を表示します**)**
Smishing is a type of phishing attack that uses SMS text messages to deceive recipients into taking actions such as revealing sensitive information. The urgency in the text indicates this vector.

質問: **162**
会社のウェブサイトはwww.company.comです。攻撃者はこのドメインを購入しました。www.company.com。この例に当てはまる攻撃の種類は次のどれですか？
A. タイプミススクワッティング
B. ブランドのなりすまし
C. パス上
D. 水飲み場
正解: **(**正解を表示します**)**
Typosquatting, also known as URL hijacking, is a form of cybersquatting where attackers register domain names that are intentionally similar to legitimate ones, often differing by a single character or a common typographical error. For example, an attacker might register 'wwww.company.com' to mimic 'www.company.com,' tricking users who mistype the URL into visiting a malicious site. This attack exploits human error and can be used to steal credentials, distribute malware, or impersonate the legitimate entity.

質問: **163**
従業員がフィッシング詐欺に引っかかり、攻撃者が会社の PC にアクセスできるようになりました。攻撃者は PC のメモリをスクレイピングして他の認証情報を探しました。攻撃者はこれらの認

証情報を解読することなく、それを使用して企業ネットワークを横方向に移動しました。このタイプの攻撃を説明するのは次のうちどれですか。
A. 権限昇格
B. バッファオーバーフロー
C. SQLインジェクション
D. ハッシュのパス
正解: **(**正解を表示します**)**
Unlike other credential theft attacks, a pass the hash attack does not require the attacker to know or crack the password to gain access to the system. Rather, it uses a stored version of the password to initiate a new session.

質問: **164**
ユーザーのワークステーションが応答しなくなり、ファイルの復号と引き換えに身代金を要求するメッセージが表示されました。攻撃前に、ユーザーはメッセージで受信した履歴書を開き、会社のウェブサイトを閲覧し、OSのアップデートをインストールしていました。この攻撃の経路として最も可能性が高いのは次のうちどれですか？
A. 水飲み場
B. スピアフィッシング添付ファイル
C. 感染したウェブサイト
D. タイプミススクワッティング
正解: **(**正解を表示します**)**

質問: **165**
システム管理者は、ユーザーのログイン時に OS のバージョン、パッチ レベル、およびインストールされているアプリケーションを検証するスクリプトを作成します。次の例のうち、このスクリプトの目的を最もよく表すものはどれですか。
A. リソースのスケーリング
B. ポリシーの列挙
C. ベースラインの強制
D. ガードレールの実装
正解: **(**正解を表示します**)**
Baseline enforcement ensures that all systems adhere to predefined security configurations, such as approved OS versions and patch levels, improving compliance and reducing vulnerabilities.

質問: **166**
セキュリティ チームは、サード パーティが侵入テストを実行した後に配信されたレポートの調査結果を確認しています。調査結果の 1 つでは、Web アプリケーション フォーム フィールドがクロスサイト スクリプティングに対して脆弱であることが示されています。セキュリティ アナリストは、この脆弱性を防ぐために開発者に次のどのアプリケーション セキュリティ手法を実装するよう推奨する必要がありますか。

A. セキュアクッキー
B. バージョン管理
C. 入力検証
D. コード署名
正解: **(**正解を表示します**)**
Input validation is a technique that checks the user input for any malicious or unexpected data before processing it by the web application. Input validation can prevent cross-site scripting (XSS) attacks, which exploit the vulnerability of a web application to execute malicious scripts in the browser of a victim. XSS attacks can compromise the confidentiality, integrity, and availability of the web application and its users. Input validation can be implemented on both the client-side and the server-side, but server-side validation is more reliable and secure. Input validation can use various methods, such as whitelisting, blacklisting, filtering, escaping, encoding, and sanitizing the input data.

質問: **167**
組織は、機密情報を含むサーバーをワークステーションと同じネットワーク内に保持します。攻撃者がワークステーションに侵入し、サーバーに侵入しました。攻撃者がサーバーにアクセスするのを阻止できた可能性のある手段は次のどれですか？
A. ロードバランサー
B. セキュリティゾーン
C. 仮想プライベートネットワーク
D. プロキシサーバー
正解: **(**正解を表示します**)**
By placing servers and workstations into separate security zones (network segments) with controlled access between them, the organization would prevent a compromised workstation from directly reaching the confidential servers. This isolation stops lateral movement without needing VPNs, proxies, or load balancers.

質問: **168**
ある企業が、顧客が自社の公開eコマースウェブサイトにPDF文書をアップロードできるようにしています。セキュリティアナリストが最も推奨すると思われるのは次のうちどれですか？
A. IDSにおける攻撃シグネチャの利用

B. UTMによるマルウェア検出の有効化
C. ロードバランサーを使用して影響を受けるサーバーを制限する
D. WAFによるコマンドインジェクションのブロック
正解: **(**正解を表示します**)**
PDFs can be used to deliver malware such as embedded scripts or exploits. Enabling malware detection through a UTM helps to scan and block malicious content within uploaded files before they reach the server.

質問: **169**
研究開発事業部門の従業員は、会社のデータを保護する最善の方法を理解できるよう、広範囲にわたるトレーニングを受けています。これらの従業員が日常業務で最もよく使用するデータの種類は次のどれですか。
A. 暗号化
B. 知的財産
C. クリティカル
D. 転送中のデータ
正解: **B (**コメントを発表する**)**
Intellectual property is a type of data that consists of ideas, inventions, designs, or other creative works that have commercial value and are protected by law. Employees in the research and development business unit are most likely to use intellectual property data in their day-to-day work activities, as they are involved in creating new products or services for the company. Intellectual property data needs to be protected from unauthorized use, disclosure, or theft, as it can give the company a competitive advantage in the market. Therefore, these employees receive extensive training to ensure they understand how to best protect this type of data.

質問: **170**
次のリスク管理戦略のうち、パッチ適用ではなくデバイスに補償制御を適用することを説明しているのはどれですか。
A. 承認
B. 緩和
C. 回避
D. 転移
正解: **(**正解を表示します**)**
Mitigation reduces risk by applying alternative controls - such as compensating controls - when patching is not possible, lowering the likelihood or impact of the vulnerability.

質問: **171**
運用サーバーの脆弱性を軽減する前に、次の手順のどれを実行する必要がありますか?
A. IR 計画を使用して変更を評価します。
B. 変更管理ポリシーを参照してください。

C. リスク評価を実行して脆弱性を分類します。
D. 問題を SDLC チームにエスカレートします。
正解: **B** (コメントを発表する)

質問: **172**
ある組織では、顧客データを、メインの企業ネットワーク上のユーザーがアクセスできないネットワークの別の部分に保存したいと考えています。この目的を達成するために、管理者は次のどれを使用する必要がありますか?
A. セグメンテーション
B. 孤立
C. パッチ適用
D. 暗号化
正解: (正解を表示します)
Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries. Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies. Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches.

質問: **173**
侵入テスト担当者は、エンゲージメント ルールに従ってクライアント環境に対してポートおよびサービスのスキャンを実行することでエンゲージメントを開始します。テスト担当者が実行する偵察の種類は次のどれですか。
A. アクティブ
B. パッシブ
C. 防御的
D. 攻撃的
正解: **A** (コメントを発表する)
Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information.

質問: **174**
従来のインフラストラクチャ モデルよりも IaC が優先されるセキュリティ アーキテクチャとなるのは次のどれですか。

A. 一般的な攻撃は効果が低くなります。
B. 構成をより適切に管理および複製できます。
C. ネットワーク防御の専門知識を持つ第三者へのアウトソーシングが可能です。
D. 最適化は複数のコンピューティングインスタンスにわたって実行できます
正解: **(**正解を表示します**)**
IaC stores infrastructure definitions as version-controlled code, so every change is reviewable, auditable, and repeatable. You can spin up identical, securely preconfigured environments from the same template, eliminating drift and undocumented tweaks that plague traditional, manually built infrastructure. This consistency and traceability are what make IaC the more secure choice.

質問: **175**
ユーザーが悪意のあるテキストメッセージを受信し、偽の銀行ログイン情報に誘導されます。このシナリオは、以下のどの種類の攻撃に当てはまりますか？
A. なりすまし
B. フィッシング
C. フィッシング
D. スミッシング
正解: **D (**コメントを発表する**)**
Smishing is phishing delivered via SMS/text messages; the malicious text lured the user to a fake bank site.

質問: **176**
ある集団が、最も大きな金銭的利益を得るために選ばれた標的に対し、複数のランサムウェア攻撃を実行するために協力しています。この種の活動を最もよく表しているのは次のうちどれですか？
A. 組織犯罪
B. 国民国家主体
C. シャドーIT
D. ハクティビズム
正解: **(**正解を表示します**)**
Coordinated ransomware campaigns for profit are characteristic of organized crime groups - criminal enterprises motivated by financial gain rather than ideology or national interest.

質問: **177**
最高経営責任者 (CEO) をターゲットにした電子メッセージ キャンペーンを使用するソーシャル エンジニアリング攻撃を最もよく表しているのは次のうちどれですか。
A. 捕鯨
B. スピアフィッシング
C. なりすまし
D. 個人情報詐欺

正解: (正解を表示します)
Whaling is a type of social engineering attack specifically targeting high-profile individuals such as CEOs or other executives. It is a form of spear phishing that focuses on these high-value targets with highly personalized and convincing messages.

質問: **178**
オフサイトにいる従業員は、割り当てられたタスクを完了するために会社のリソースにアクセスする必要があります。これらの従業員は、傍受の心配なくリモート アクセスを可能にするソリューションを活用します。このソリューションを最もよく表すのは次のどれですか。
A. プロキシサーバー
B. NGFW
C. VPN
D. セキュリティゾーン
正解: **C** (コメントを発表する)
A Virtual Private Network (VPN) is the best solution to allow remote employees secure access to company resources without interception concerns. A VPN establishes an encrypted tunnel over the internet, ensuring that data transferred between remote employees and the company is secure from eavesdropping.
Proxy server helps with web content filtering and anonymization but does not provide encrypted access.
NGFW (Next-Generation Firewall) enhances security but is not the primary tool for enabling remote access.
Security zone is a network segmentation technique but does not provide remote access capabilities.

質問: **179**
レガシー サーバーで実行されている重要なビジネス アプリケーションを処理するための最適な方法はどれですか?
A. セグメンテーション
B. 孤立
C. 強化
D. 廃止
正解: (正解を表示します)
The device is STILL running a critical application. therefore it needs to be connected to the network. a compensating mechanism for this scenario would be segmentation as this would limit the ability of an attacker to pivot from the vulnerable server to the rest of the network.as possible.

質問: **180**
セキュリティ管理者は、会社のデータ センターの攻撃対象領域を縮小する必要があります。このタスクを完了するために、セキュリティ管理者は次のどれを実行する必要がありますか。

A. ハニーネットを実装します。
B. サーバー上でグループ ポリシーを定義します。
C. 高可用性のためにサーバーを構成します。
D. サポートが終了したオペレーティング システムをアップグレードします。
正解: **D** (コメントを発表する)
Upgrading end-of-support operating systems ensures that the servers receive security patches and updates, significantly reducing vulnerabilities and thereby the overall attack surface.

質問: **181**
最近の社内安全対策会議で、サイバー意識向上チームがサイバー衛生の重要性についてプレゼンテーションを行いました。チームが取り上げたトピックの 1 つは、印刷センターのベスト プラクティスでした。印刷センターに関連する攻撃方法は、次のうちどれですか。
A. 捕鯨
B. 認証情報の収集
C. 先頭に追加
D. ゴミ漁り
正解: **D** (コメントを発表する)
Dumpster diving is an attack method where attackers search through physical waste, such as discarded documents and printouts, to find sensitive information that has not been properly disposed of. In the context of printing centers, this could involve attackers retrieving printed documents containing confidential data that were improperly discarded without shredding or other secure disposal methods. This emphasizes the importance of proper disposal and physical security measures in cyber hygiene practices.

質問: **182**
次のメトリックのうち、BIA の一部としてバックアップ スケジュールに影響を与えるものはどれですか。
A. RTO
B. RPO
C. MTTR
D. MTBF
正解: (正解を表示します)

The Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss in terms of time, directly influencing how frequently backups must be performed.

質問: **183**
クラウド プロバイダー内でリソースを簡単に展開できるようにするために、システム管理者は次のどれを使用する必要がありますか?
A. サービスとしてのソフトウェア
B. コードとしてのインフラストラクチャ
C. モノのインターネット
D. ソフトウェア定義ネットワーク
正解: **B (**コメントを発表する**)**
Infrastructure as code (IaC) is a method of using code and automation to manage and provision cloud resources, such as servers, networks, storage, and applications. IaC allows for easy deployment, scalability, consistency, and repeatability of cloud environments. IaC is also a key component of DevSecOps, which integrates security into the development and operations processes.

質問: **184**
最近、会社のシステムがランサムウェア攻撃を受けた後、管理者がログ ファイルを確認しました。管理者は次のどの制御タイプを使用しましたか?
A. 補償
B. 探偵
C. 予防的
D. 修正
正解: **B (**コメントを発表する**)**
Detective controls are security measures that are designed to identify and monitor any malicious activity or anomalies on a system or network. They can help to discover the source, scope, and impact of an attack, and provide evidence for further analysis or investigation. Detective controls include log files, security audits, intrusion detection systems, network monitoring tools, and antivirus software. In this case, the administrator used log files as a detective control to review the ransomware attack on the company's system. Log files are records of events and activities that occur on a system or network, such as user actions, system errors, network traffic, and security alerts. They can provide valuable information for troubleshooting, auditing, and forensics.

質問: **185**
脆弱性の重大度を判断する際に最も適したものは次のどれですか?
A. 飛翔
B. CVSS
C. CVE
D. OSINT

正解: (正解を表示します)

質問: **186**
データベースの SQL 更新中に、作成された一時フィールドが攻撃者によって置き換えられ、システムへのアクセスが許可されました。このタイプの脆弱性を最もよく表すのは次のどれですか。
A. メモリインジェクション
B. サイドローディング
C. 競合状態
D. 悪意のあるアップデート
正解: (正解を表示します)

質問: **187**
レガシー システムを識別するために最もよく使用される方法はどれですか。
A. バグ報奨金プログラム
B. 脆弱性スキャン
C. パッケージ監視
D. 動的解析
正解: (正解を表示します)
A vulnerability scan is the most likely method to identify legacy systems. These scans assess an organization's network and systems for known vulnerabilities, including outdated or unsupported software (i.e., legacy systems) that may pose a security risk. The scan results can highlight systems that are no longer receiving updates, helping IT teams address these risks.
Bug bounty programs are used to incentivize external researchers to find security flaws, but they are less effective at identifying legacy systems.
Package monitoring tracks installed software packages for updates or issues but is not as comprehensive for identifying legacy systems.
Dynamic analysis is typically used for testing applications during runtime to find vulnerabilities, but not for identifying legacy systems.

質問: **188**
データ管理者は SaaS アプリケーションの認証を構成しており、従業員が維持する必要がある資格情報の数を減らしたいと考えています。会社では、新しい SaaS アプリケーションにアクセスするためにドメイン資格情報を使用することを希望しています。次の方法のどれがこの機能を可能にしますか?
A. SSO
B. LEAP
C. MFA
D. PEAP
正解: (正解を表示します)

SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials.

質問: **189**
絶えず変化する環境に最も適しているのはどれでしょうか?
A. RTOS
B. コンテナ
C. 組み込みシステム
D. SCADA
正解: **B (**コメントを発表する**)**
Containers are a method of virtualization that allows applications to run in isolated environments with their own dependencies, libraries, and configurations. Containers are best suited for constantly changing environments because they are lightweight, portable, scalable, and easy to deploy and update. Containers can also support microservices architectures, which enable faster and more frequent delivery of software features.

質問: **190**
環境内の脆弱性のリストをまとめるには、まず次のどのアクティビティを実行する必要がありますか?
A. 自動スキャン
B. 侵入テスト
C. 脅威ハンティング
D. ログ集計
E. 敵対的エミュレーション
正解: **(**正解を表示します**)**
Automated scanning is the first step in identifying vulnerabilities in an environment. Tools that perform automated vulnerability scanning scan systems and networks for known vulnerabilities, missing patches, misconfigurations, and other security weaknesses. This helps create an initial list of vulnerabilities that can then be prioritized and addressed, often serving as the foundation for further in-depth activities like penetration testing or threat hunting.

質問: **191**
DDoS 攻撃に対する保護を提供する製品を実装する際に、次のセキュリティ概念のどれに従いますか?
A. 可用性

B. 否認防止
C. 誠実さ
D. 機密性
正解**: (**正解を表示します**)**
When implementing a product that offers protection against Distributed Denial of Service (DDoS) attacks, the security concept being followed is availability. DDoS protection ensures that systems and services remain accessible to legitimate users even under attack, maintaining the availability of network resources.
Availability: Ensures that systems and services are accessible when needed, which is directly addressed by DDoS protection.
Non-repudiation: Ensures that actions or transactions cannot be denied by the involved parties, typically achieved through logging and digital signatures.
Integrity: Ensures that data is accurate and has not been tampered with.
Confidentiality: Ensures that information is accessible only to authorized individuals.

質問**: 192**
ネットワーク上のさまざまなデバイスから統合レポートを受信できるようになるのは次のどれですか?
A. DLP
B. SIEM
C. IPS
D. ファイアウォール
正解**: (**正解を表示します**)**

質問**: 193**
不明なプログラムの実行をブロックする最善の方法は次のどれですか?
A. アクセス制御リスト
B. アプリケーション許可リスト。
C. ホストベースのファイアウォール
D. DLPソリューション
正解**: B (**コメントを発表する**)**
An application allow list is a security technique that specifies which applications are permitted to run on a system or a network. An application allow list can block unknown programs from executing by only allowing the execution of programs that are explicitly authorized and verified. An application allow list can prevent malware, unauthorized software, or unwanted applications from running and compromising the security of the system or the network. The other options are not the best ways to block unknown programs from executing:
Access control list: This is a security technique that specifies which users or groups are granted or denied access to a resource or an object. An access control list can control the permissions and privileges of users or groups, but it does not directly block unknown programs from executing. Host-based firewall: This is a security device that monitors and filters the incoming and

outgoing network traffic on a single host or system. A host-based firewall can block or allow network connections based on predefined rules, but it does not directly block unknown programs from executing.
DLP solution: This is a security system that detects and prevents the unauthorized transmission or leakage of sensitive data. A DLP solution can protect the confidentiality and integrity of data, but it does not directly block unknown programs from executing.

質問: **194**
システム管理者がファイルの権限を調整できるのは次のどれですか?
A. パッチ適用
B. アクセス制御リスト
C. 構成の強制
D. 最小権限
正解: **B (**コメントを発表する**)**
Access control lists (ACLs) allow administrators to fine-tune file permissions by specifying which users or groups have access to a file and defining the level of access.

質問: **195**
ソフトウェア開発マネージャーは、会社が作成したコードの信頼性を確保したいと考えています。次のオプションのうち、最も適切なものはどれですか。
A. ユーザー入力フィールドの入力検証をテストする
B. 自社開発ソフトウェアのコード署名の実行
C. ソフトウェアの静的コード解析を実行する
D. 安全なCookieが使用されていることを確認する
正解: **(**正解を表示します**)**
Code signing is a technique that uses cryptography to verify the authenticity and integrity of the code created by the company. Code signing involves applying a digital signature to the code using a private key that only the company possesses. The digital signature can be verified by anyone who has the corresponding public key, which can be distributed through a trusted certificate authority. Code signing can prevent unauthorized modifications, tampering, or malware injection into the code, and it can also assure the users that the code is from a legitimate source.

質問: **196**
脆弱性の優先順位付けに関する決定を行う際に、組織が最も重点を置くべきは次のどれですか?
A. 露出係数
B. CVSS
C. CVE
D. 業界への影響
正解: **(**正解を表示します**)**

The Common Vulnerability Scoring System (CVSS) is a standardized metric used to assess the severity of vulnerabilities, aiding organizations in prioritizing their response based on risk.

質問: **197**
設計変更を実施する前に、セキュリティ上の問題が発生しないことを確認するために、複数の手順を踏む必要があります。これらの手順のうち、最も可能性の高いものはどれですか？
A. 経営レビュー
B. 負荷テスト
C. メンテナンス通知
D. 手順の更新
正解: **A** (コメントを発表する)
Management review is a key step in the change management process, ensuring that proposed changes are properly evaluated for security and business impact before implementation.

質問: **198**
ある企業は、規制当局が定めるデータ保持ガイドラインの遵守を義務付けられている銀行に対し、長期コールドストレージサービスを提供しています。このサービスを利用する銀行は、規制上のデータ保持期間の閾値に達した時点で、特定の方法でデータを廃棄することを義務付けています。銀行にとって、このデータの破棄において最も重要なデータ管理の側面は、以下のどれですか？
A. 暗号化
B. 分類
C. 認証
D. 調達
正解: (正解を表示します)
Certification provides documented proof that data was destroyed in compliance with regulatory requirements. This is critical for banks to demonstrate adherence to data retention and disposal mandates imposed by regulators.

質問: **199**
インシデント対応の次のフェーズのうち、レポートの生成が含まれるのはどれですか?
A. 回復

B. 準備
C. 学んだ教訓
D. 封じ込め
正解: **(**正解を表示します**)**
The lessons learned phase of an incident response process involves reviewing the incident and generating reports. This phase helps identify what went well, what needs improvement, and what changes should be made to prevent future incidents. Documentation and reporting are essential parts of this phase to ensure that the findings are recorded and used for future planning.
* Recovery focuses on restoring services and normal operations.
* Preparation involves creating plans and policies for potential incidents, not reporting.
* Containment deals with isolating and mitigating the effects of the incident, not generating reports.

質問: **200**
調査中、インシデント対応チームはインシデントの原因を理解しようとします。次のインシデント対応活動のうち、このプロセスを説明するものはどれですか。
A. 分析
B. 学んだ教訓
C. 検出
D. 封じ込め
正解: **(**正解を表示します**)**
Analysis is the incident response activity that describes the process of understanding the source of an incident. Analysis involves collecting and examining evidence, identifying the root cause, determining the scope and impact, and assessing the threat actor's motives and capabilities. Analysis helps the incident response team to formulate an appropriate response strategy, as well as to prevent or mitigate future incidents. Analysis is usually performed after detection and before containment, eradication, recovery, and lessons learned.

質問: **201**
セキュリティアナリストがログを調査し、悪質なIPアドレスに類似したデータタイプが送信されていることに気付きました。これは、以下のどの攻撃タイプに最もよく当てはまりますか？
A. 論理爆弾
B. ワーム
C. スパイウェア
D. キーロガー
正解: **(**正解を表示します**)**
Spyware covertly collects and transmits data to external servers, often to IP addresses with known bad reputations, matching the described behavior in the logs.

質問: **202**

企業のインフラストラクチャの重要な部分であるレガシー システムを置き換えることができない場合、主に考慮すべき事項は次のどれですか。
A. 単一障害点
B. リソースのプロビジョニング
C. コスト
D. 複雑さ
正解: **A (**コメントを発表する**)**

質問: **203**
耐用年数が終了したビジネスクリティカルなシステムの悪用を最も効果的に防ぐには、次のうちどれが効果的でしょうか?
A. 監視
B. 隔離
C. 廃止
D. 暗号化
正解: **(**正解を表示します**)**
Isolation places the end-of-life system on a segmented network or removes its external connectivity, reducing exposure and preventing attackers from exploiting its vulnerabilities while it remains in use.

質問: **204**
ホットスポットに関する質問
各ドロップダウン リストから適切な攻撃と修復を選択して、対応する攻撃とその修復にラベルを付けます。
説明書
すべての攻撃と修復アクションが使用されるわけではありません。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack establishes a connection, which allows remote commands to be executed.	User	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Botnet RAT Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

正解:

Attack Description	Target	Attack Identified	BEST Preventative or Remediation Action
An attacker sends multiple SYN packets from multiple sources.	Web server	Botnet	Enable DDoS protection
The attack establishes a connection, which allows remote commands to be executed.	User	RAT	Implement a host-based IPS
The attack is self propagating and compromises a SQL database using well-known credentials as it moves through the network.	Database server	Worm	Change the default application password
The attacker uses hardware to remotely monitor a user's input activity to harvest credentials.	Executive	Keylogger	Implement 2FA using push notification
The attacker embeds hidden access in an internally developed application that bypasses account login.	Application	Backdoor	Conduct a code review

Botnet, RAT, Logic Bomb, Backdoor, Virus, Spyware, Worm, Adware, Ransomware, Keylogger, Phishing

Enable DDoS protection, Patch vulnerable systems, Disable vulnerable services, Change the default system password, Update the cryptographic algorithms, Change the default application password, Implement 2FA using push notification, Conduct a code review, Implement application fuzzing, Implement a host-based IPS, Disable remote access services

質問: **205**

サイドローディング時に導入される可能性のあるものはどれですか?
A. バッファオーバーフロー
B. ユーザーのなりすまし
C. オンパス攻撃
D. ルートキット
正解: **(**正解を表示します**)**

質問: **206**
インシデント対応チームのメンバーとその他の関係者がイベントをシミュレートする必要があるアクティビティは次のどれですか。
A. 学んだ教訓
B. デジタルフォレンジック
C. 卓上演習
D. 根本原因分析
正解: **(**正解を表示します**)**
A tabletop exercise is a simulated event in which the incident response team and other stakeholders walk through their roles and decision-making processes to evaluate readiness and improve response plans.

質問: **207**
最高経営責任者の企業アカウントから、予想外の、普段とは異なる内容の電子メールが届き、従業員に財務情報の提供と受信者の連絡先の変更を求めました。次の攻撃ベクトルのうち、最もよく使用されるのはどれですか。
A. ビジネスメール詐欺
B. フィッシング
C. ブランドのなりすまし
D. プリテキスティング
正解: **(**正解を表示します**)**
Business email compromise (BEC) involves the use of a legitimate or spoofed business email account, often from executives, to trick employees into performing unauthorized actions like transferring funds or revealing sensitive information.

質問: **208**
次世代 SIEM システムの機能は次のどれですか?
A. ウイルスシグネチャ
B. 自動応答アクション
C. セキュリティエージェントの展開
D. 脆弱性スキャン
正解: **B (**コメントを発表する**)**

The next-gen SIEM platforms can dynamically analyze vast datasets in real time, enabling the identification of subtle, evolving threats that traditional systems might overlook.

質問: **209**
システムレベルのデータの変更を防ぐために、次のどれを使用する必要がありますか?
A. NIDS
B. DLP
C. NAC
D. FIM
正解: **(正解を表示します)**
File Integrity Monitoring (FIM) detects any unauthorized modification to system-level files or data, ensuring those files remain unchanged unless properly authorized.

質問: **210**
システム管理者は、本番システムに変更を適用したいと考えています。パフォーマンス問題が発生した場合にシステムを正常な状態に復元できることを証明するために、管理者は次のどれを提出する必要がありますか？
A. バックアウト計画
B. 影響分析
C. テスト手順
D. 承認手続き
正解: **(正解を表示します)**
To demonstrate that the system can be restored to a working state in the event of a performance issue after deploying a change, the systems administrator must submit a backout plan. A backout plan outlines the steps to revert the system to its previous state if the new deployment causes problems.
Backout plan: Provides detailed steps to revert changes and restore the system to its previous state in case of issues, ensuring minimal disruption and quick recovery.
Impact analysis: Evaluates the potential effects of a change but does not provide steps to revert changes.
Test procedure: Details the steps for testing the change but does not address restoring the system to a previous state.
Approval procedure: Involves obtaining permissions for the change but does not ensure system recovery in case of issues.

質問: **211**
セキュリティ アナリストは、ネットワークに接続されている現在のエンドポイント資産の月次監査中に不正なデバイスを発見しました。企業ネットワークは、アクセス制御に 002.1X を使用しています。デバイスがネットワークにアクセスするには、既知のハードウェア アドレスを持ち、有効

なユーザー名とパスワードをキャプティブ ポータルに入力する必要があります。監査レポートは次のとおりです。

IP address	MAC	Host	Account
10.18.04.42	BE-AC-11-F1-E4-44	PC-NY	user1
10.18.04.38	EB-AC-11-82-42-F3	PC-CA	user3
10.18.04.59	28-BB-5A-11-52-29	PC-PA	user2
10.18.04.58	28-BB-5A-F0-E9-D1	PC-TX	user4
10.18.04.22	EB-AC-11-82-42-F3	WIN10	user3
10.18.04.26	BB-28-11-82-A2-33	PC-NJ	admin

不正なデバイスの接続が許可される可能性が最も高い方法はどれですか?

A. ユーザーが個人のデバイスを使用して MAC クローン攻撃を実行しました。

B. DMCP障害により誤ったIPアドレスが配布されました

C. 管理者がテストのためにセキュリティ制御をバイパスしました。

D. DNS ハイジャックにより、攻撃者はキャプティブ ポータルのトラフィックを傍受できます。

正解: **A** (コメントを発表する)

The most likely way a rogue device was able to connect to the network is through a MAC cloning attack. In this attack, a personal device copies the MAC address of an authorized device, bypassing the 802.1X access control that relies on known hardware addresses for network access. The matching MAC addresses in the audit report suggest that this technique was used to gain unauthorized network access.

質問: **212**

セキュリティ アナリストは、次のログを含む Web サーバーからアラートを受信します。

```
GET /image?filename= ../../../etc/passwd
Host: AcmeInc.web.net
useragent: python-request/ 2.27.1

GET /image?filename= ../../../etc/shadow
Host: AcmeInc.web.net
useragent: python-request/ 2.27.1
```

次の攻撃のうちどれが試みられているのでしょうか?

A. ファイルインジェクション

B. 権限昇格

C. ディレクトリトラバーサル
D. クッキー偽造
正解: **(**正解を表示します**)**
The "../../../etc/passwd" and "../../../etc/shadow" path sequences attempt to climb directories and read sensitive files, indicating a directory traversal attack.

質問: **213**
ヘルプデスクには、エンタープライズアプリケーションの実行時にマシンの動作が遅いという複数の電話が寄せられています。ヘルプデスクは、影響を受けているマシンが組織のOSベースラインに準拠していないと報告しています。また、複数のユーザーからウイルス検出アラートが表示されているとの報告も寄せられています。
ヘルプ デスクが最初に検討すべき軽減手法は次のどれですか。
A. パッチ適用
B. セグメンテーション
C. 監視
D. 分離
正解: **(**正解を表示します**)**
Isolation prevents potentially infected systems from interacting with the rest of the network, immediately containing the spread of malware and limiting further impact while remediation actions are planned and executed.

質問: **214**
デジタルフォレンジックを実行する際、最も不安定であると考えられ、最初にコンテンツを収集する必要があるのは次のどれですか?
A. ハードドライブ
B. RAM
C. SSD
D. 一時ファイル
正解: **B (**コメントを発表する**)**
When the computer powers off, anything in the RAM is going to be lost. Therefore, collecting potential evidence out of the RAM is the first thing that should be done out of these options.

質問: **215**
財務処理活動が行われる環境で実装することが適切な運用管理の例は次のどれですか? (2 つ選択してください。)
A. キーエスクロー
B. トークン化
C. デュアルコントロール
D. 必須休暇
E. バッジリーダーにアクセスする

F. 生体認証
正解: **(**正解を表示します**)**
Dual control ensures that no single individual can complete sensitive financial transactions alone, reducing the risk of fraud and error through enforced separation of duties.
Mandatory vacations help detect fraudulent activity by requiring employees to step away from their roles, increasing the likelihood that unauthorized or improper actions are discovered during their absence.

質問: **216**
セキュリティアナリストは、セキュリティ侵害により 15,000 ドルの経済的影響が生じ、3 年間に 2 回発生すると予測しています。このリスクの ALE は次のどれですか。
A. 10,000ドル
B. 30,000ドル
C. 7,500 ドル
D. 15,000ドル
正解: **(**正解を表示します**)**

質問: **217**
高リスクの Web サイトへのユーザー アクセスを提供するための補償制御は次のどれですか。
A. すべてのWebトラフィックをキャプチャするためのSIEMツールの設定
B. エンドポイント保護ソフトウェアでそのウェブサイトをブロックする
C. 任意のポートからその宛先へのトラフィックを許可するファイアウォールルールを設定する
D. ファイアウォールの脅威防止機能を有効にする
正解: **(**正解を表示します**)**

質問: **218**
システム管理者は、別の支社のピアに送信するメッセージを鍵で暗号化します。ピアは同じ鍵でメッセージを復号します。この例を説明するのは次のどれですか？
A. ハッシュ
B. 非対称
C. 塩漬け
D. 対称
正解: **(**正解を表示します**)**

質問: **219**
技術者は、本番システムに優先度の高いパッチを適用する必要があります。次の手順のうち、最初に実行する必要があるのはどれですか。
A. システムをエアギャップします。
B. システムを別のネットワーク セグメントに移動します。
C. 変更管理要求を作成します。

D. システムにパッチを適用します。
正解: **(**正解を表示します**)**
A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches.

質問: **220**
ネットワークへの侵入に成功した攻撃者を検出するために使用できる方法はどれですか? (2 つ選択してください。)
A. トークン化
B. CI/CD
C. ハニーポット
D. 脅威モデル
E. DNSシンクホール
F. データの難読化
正解: **(**正解を表示します**)**
Honeypot attracts and traps attacker and DNS sinkhole redirects malicious domain name queries to a controlled server to detect and block communication between compromised host and their C2 servers.

質問: **221**
ある会社の法務部門が SaaS アプリケーションで機密文書を作成し、高リスク国の個人がその文書にアクセスできないようにしたいと考えています。このアクセスを制限する最も効果的な方法はどれですか。
A. データマスキング
B. 暗号化
C. 地理位置情報ポリシー
D. データ主権規制
正解: **(**正解を表示します**)**
A geolocation policy is a policy that restricts or allows access to data or resources based on the geographic location of the user or device. A geolocation policy can be implemented using various methods, such as IP address filtering, GPS tracking, or geofencing. A geolocation policy can help the company's legal department to prevent unauthorized access to sensitive documents from individuals in high-risk countries.

質問: **222**

次のどれが、侵入テスト担当者が攻撃の初期段階で採用する一般的な受動偵察手法ですか?
A. オープンソースインテリジェンス
B. ポートスキャン
C. ピボット
D. エクスプロイトの検証
正解: **(正解を表示します)**
OSINT involves gathering information from publicly available sources, such as social media, websites, and online databases, without actively interacting with the target system. This technique helps in identifying potential vulnerabilities and understanding the target's environment before more intrusive methods are used.

質問: **223**
次のどれが脆弱性管理を自動化できますか?
A. CVE
B. SCAP
C. OSINT
D. CVSS
正解: **(正解を表示します)**
SCAP (Security Content Automation Protocol) is a standardized framework that enables automated vulnerability management, compliance checking, and security measurement.

質問: **224**
ある企業はコスト管理のため人員削減を進めています。最高情報セキュリティ責任者(CIO)は、内部脅威のリスク増大を懸念しています。セキュリティ意識向上チームがこの潜在的な脅威に対処するために、最も役立つと思われるのは次のうちどれですか？
A. 解雇される可能性のあるスタッフのアカウントを直ちに無効にします。
B. 不満を抱えた従業員を特定し、管理できるように管理者をトレーニングします。
C. 解雇されるスタッフを監視するように DLP を構成します。
D. 解雇されるスタッフを監視するように DLP を構成します。
正解: **(正解を表示します)**
Equipping supervisors to recognize signs of dissatisfaction and potential insider threats enables early intervention, addressing the human factors that awareness programs are designed to influence.

質問: **225**
さまざまな関係者が、セキュリティ インシデントや大規模災害などの特定の状況における仮想的な役割と責任について話し合うために会議を行っています。この会議を最もよく表すのは次のどれですか。
A. 侵入テスト
B. 業務継続計画

C. テーブルトップ演習
D. シミュレーション
正解: **(**正解を表示します**)**
A tabletop exercise is a discussion-based exercise where stakeholders gather to walk through the roles and responsibilities they would have during a specific situation, such as a security incident or disaster. This type of exercise is designed to identify gaps in planning and improve coordination among team members without the need for physical execution.

質問: **226**
ある企業は、フロントエンドWebサーバーへの過剰なトラフィックにより、可用性の低下を経験しています。このインシデントを調査するために、デジタルフォレンジックの専門家を雇用しました。このインシデントの詳細を診断するために、デジタルフォレンジックの専門家はまずどのログを確認すべきでしょうか？
A. ルーター
B. ロードバランサー
C. スイッチ
D. ファイアウォール
正解: **B (**コメントを発表する**)**
Load balancer logs provide detailed information about incoming web traffic and distribution to the front-end servers, making them the most relevant source to diagnose excessive traffic and availability issues.

質問: **227**
セキュリティ アナリストは、コマンド アンド コントロール サーバーへの送信通信が疑われるワークステーションを調査しています。調査中に、エンドポイントのログが削除されていることがアナリストによって発見されました。
アナリストが次に確認する可能性が高いログは次のどれですか?
A. IPS
B. ファイアウォール
C. ACL
D. Windows セキュリティ
正解: **(**正解を表示します**)**

Since the logs on the endpoint were deleted, the next best option for the analyst is to examine firewall logs. Firewall logs can reveal external communication, including outbound traffic to a command-and-control (C2) server. These logs would contain information about the IP addresses, ports, and protocols used, which can help in identifying suspicious connections.
IPS logs may provide information about network intrusions, but firewall logs are better for tracking communication patterns.
ACL logs (Access Control List) are useful for tracking access permissions but not for identifying C2 communication.
Windows security logs would have been ideal if they had not been deleted.

質問: **228**
セキュリティアナリストは、オフィスの支店に無許可の無線ルーターを設置した従業員を特定しました。調査の結果、当該ルーターは撤去され、当該従業員には再研修が義務付けられました。このインシデントについて最も適切な説明は次のどれですか？
A. 未熟な攻撃者
B. ハクティビスト
C. 国民国家
D. シャドーIT
正解: **D (**コメントを発表する**)**
Shadow IT refers to the use of unauthorized devices, software, or systems, such as an employee adding a wireless router without approval, outside of official IT processes.

質問: **229**
テーブルトップエクササイズを実行する最も適切な理由は次のうちどれですか?
A. 修復応答時間を収集する
B. IRPを更新するには
C. ROIを計算する
D. 監査結果に対処するため
正解: **B (**コメントを発表する**)**

質問: **230**
インシデントを調査している管理者は、ドライブの故障により重要なサーバーがダウンタイムに陥ることを懸念しています。管理者は、問題の解決に必要な時間を見積もるために、次のうちどれを使用しますか？
A. 平均所要時間
B. MTBF
C. RTO
D. RPO
正解: **A (**コメントを発表する**)**

MTTR (Mean Time to Repair) measures the average time required to repair a failed component or system and restore it to full functionality, making it the correct metric for estimating downtime due to a failed drive.

質問: **231**
次のどれが、エクスプロイトがオペレーティング システムによって検出されないことを可能にしますか?
A. ファームウェアの脆弱性
B. サイドローディング
C. メモリインジェクション
D. 暗号化されたペイロード
正解: **A (コメントを発表する)**
Firmware operates at a lower level than the operating system. It's the software embedded in hardware components like the BIOS/UEFI, network cards, hard drives, etc. If a vulnerability exists in the firmware, an exploit can run before the operating system even boots or can operate outside of the OS's control.

質問: **232**
セキュリティ エンジニアが安全なベースラインを実装する順序を最も正確に説明しているのは次のどれですか。
A. 展開、維持、確立
B. 確立、維持、展開
C. 確立、展開、維持
D. 展開、確立、維持
正解: **C (コメントを発表する)**
The correct sequence is to first establish secure baselines by determining the required configurations, deploy those configurations across systems, and finally maintain the configurations through regular updates and auditing.

質問: **233**
攻撃者がバッファ オーバーフローを悪用したため、組織のインターネット向け Web サイトが侵害されました。今後同様の攻撃から組織を保護するために、組織は次のどれを導入する必要がありますか。
A. NGFW
B. WAF
C. TLS
D. SD-WAN
正解: **(正解を表示します)**
A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory

locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data.

質問: **234**
システム管理者は境界ファイアウォールを設定しましたが、内部エンドポイント間の疑わしい接続が引き続き発生しています。疑わしいアクティビティによる脅威を軽減するには、次のうちどれを設定する必要がありますか?
A. ホストベースのファイアウォール
B. Web アプリケーション ファイアウォール
C. アクセス制御リスト
D. アプリケーション許可リスト
正解: **(**正解を表示します**)**
A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing.

質問: **235**
インフラの大部分をクラウドで運用している企業の開発環境が侵害を受けました。攻撃者は公開開発アプリケーションを介してアクセスし、本番環境への侵入に成功しました。このような事態の再発を防ぐには、以下のどのアーキテクチャ変更が最も効果的でしょうか？
A. 各環境を会社のクラウドアカウント内の個別のVPCに移動する
B. 会社のクラウドアカウントにファイアウォールを導入する
C. 開発環境をオンプレミス環境に移行する

D. 環境間のアクセスを制限するセキュリティグループの実装
正解: **(**正解を表示します**)**
Placing development and production environments in separate VPCs provides strong network isolation, preventing attackers from pivoting between them even if one environment is compromised.

質問: **236**
スイッチポートに接続するすべてのクライアントは、インターネットにアクセスする前にポスチャ分析を完了する必要があります。企業インフラストラクチャのセキュリティを確保するために、ITチームは以下のどれを設定する必要がありますか？
A. VPN
B. WAF
C. IPS
D. NAC
正解: **D (**コメントを発表する**)**
Network Access Control (NAC) enforces endpoint posture checks, such as antivirus status, patch levels, and configuration, before allowing devices on switchports to access the network or internet.

質問: **237**
デバイスがネットワークに接続されたリソースにアクセスできないようにするには、次のどれを使用する必要がありますか?
A. 使用されていないサービスの無効化
B. Web アプリケーション ファイアウォール
C. ホスト分離
D. ネットワークベースのIDS
正解: **(**正解を表示します**)**
Host isolation ensures that a device is separated from the network, preventing it from accessing or being accessed by other network resources. This is typically achieved by quarantining the device.

質問: **238**
ウェブサイトのユーザーが、電子メールのリンクをクリックして別のウェブサイトにアクセスした後にアカウントからロックアウトされました。ユーザーがパスワードを変更していないにもかかわらず、Web サーバーのログにはユーザーのパスワードが変更されたことが示されています。次のどれが最も可能性の高い原因ですか?
A. クロス訴訟リクエストの偽造
B. ディレクトリトラバーサル
C. ARP ポイズニング
D. SQLインジェクション

正解: **(**正解を表示します**)**
The scenario describes a situation where a user unknowingly triggers an unwanted action, such as changing their password, by clicking a malicious link. This is indicative of a Cross-Site Request Forgery (CSRF) attack, where an attacker tricks the user into executing actions they did not intend to perform on a web application in which they are authenticated.

質問: **239**
ある企業がプロバイダーに対し、サーバーとネットワークの稼働率を97%に維持することを期待しています。この期待に最も合致する項目は次のどれですか？
A. BPA
B. MOU
C. NDA
D. SLA
正解: **(**正解を表示します**)**
A service-level agreement (SLA) formally defines measurable performance targets - such as 97 % server and network uptime - that the provider commits to meet.

質問: **240**
ハイパーバイザーへの侵入テスト中に、セキュリティエンジニアはスクリプトを使用して悪意のあるペイロードを挿入し、ホストファイルシステムにアクセスすることができます。この脆弱性を最もよく表すものは次のうちどれですか？
A. VMエスケープ
B. クロスサイトスクリプティング
C. 悪意のあるアップデート
D. SQLインジェクション
正解: **(**正解を表示します**)**
VM escape occurs when an attacker exploits a vulnerability in the hypervisor, allowing them to break out of the virtual machine and access the underlying host system's resources.

質問: **241**
ある企業はカメラを設置し、訪問者に録画されていることを知らせる標識を設置した。
会社が実装した制御は次のうちどれですか? (2 つ選択してください。)
A. 探偵
B. ディレクティブ
C. テクニカル
D. 抑止力
E. 予防的
F. 修正
正解: **A,D (**コメントを発表する**)**

質問: **242**
セキュリティチームは、外部から細工された悪意のあるパケットに対するネットワークの強化を進めています。社内ネットワークを保護するための最も安全な方法は次のうちどれですか？
A. マルウェア対策ソリューション
B. ネットワーク許可リスト
C. ホストベースのファイアウォール
D. ネットワークアクセス制御
E. 侵入防止システム
正解: (正解を表示します)

質問: **243**
リスク管理における内部監査チームの機能はどれですか?
A. 組織の露出姿勢を定義します。
B. 組織の規制要件を実装します。
C. 組織のポリシーコンプライアンスを評価します。
D. 組織の制御監視を定義および更新します。
正解: (正解を表示します)
Internal audit teams assess whether the organization is complying with its established policies, ensuring controls are followed and effective.

質問: **244**
次の原則のうち、企業がファイルまたは記録を廃棄する前に、規定の期間保管しなければならないと定めているのはどれですか。
A. データ検証
B. データのバックアップ
C. データのアーカイブ
D. データ保持
正解: (正解を表示します)
Data retention is the principle that mandates an organization to keep files or records for a specified period before disposing of them, often to meet legal or regulatory requirements.

質問: **245**

次の技術のうち、転送中にデータが変更されたかどうかを識別できるのはどれですか?
A. ハッシュ
B. トークン化
C. マスキング
D. 暗号化
正解: **A** (コメントを発表する)
Hashing creates a unique fixed-length value based on the data, allowing verification of integrity by comparing the hash before and after transit to detect any modifications.

質問: **246**
MDM プラットフォームを設定することで軽減される可能性のある脆弱性は次のどれですか?
A. TPM
B. バッファオーバーフロー
C. 脱獄
D. SQLインジェクション
正解: (正解を表示します)
An MDM platform can detect devices that have been jailbroken and enforce policies - such as blocking access or wiping the device - to prevent compromised, unsupported mobile operating systems from accessing organizational resources.

質問: **247**
最近のアップグレード (WLAN インフラストラクチャ) 以来、複数のモバイル ユーザーがロビーからインターネットにアクセスできなくなっています。ネットワーク チームは建物のヒート マップ調査を実施し、そのエリアに複数の WAP があることを発見しました。これらの WAP は、高出力設定で同様の周波数を使用しています。セキュリティ チームが次に評価する必要があるインストールに関する考慮事項は次のどれですか。
A. チャネルの重複
B. 暗号化の種類
C. 新しいWLANの展開
D. WAP 配置
正解: (正解を表示します)
When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.

質問: **248**
セキュリティ エンジニアがワークステーションとサーバー上で不正な変更やソフトウェアが適切に監視されていることを確認するために実行できるアクションは次のどれですか。

A. スケジュールされたタスクをログに記録するようにすべてのシステムを構成します。
B. ネットワークから出るすべてのトラフィックを収集して監視します。
C. 既知の悪意のあるシグネチャに基づいてトラフィックをブロックします。
D. すべてのシステムにエンドポイント管理ソフトウェアをインストールします。
正解: **(**正解を表示します**)**
Endpoint management software is a tool that allows security engineers to monitor and control the configuration, security, and performance of workstations and servers from a central console. Endpoint management software can help detect and prevent unauthorized changes and software installations, enforce policies and compliance, and provide reports and alerts on the status of the endpoints. The other options are not as effective or comprehensive as endpoint management software for this purpose.

質問: **249**
最近の脆弱性スキャンの後、セキュリティ エンジニアは企業ネットワーク内のルーターを強化する必要があります。次のうち、無効にするのに最も適切なものはどれですか。
A. コンソールアクセス
B. ルーティングプロトコル
C. VLAN
D. Webベースの管理
正解: **(**正解を表示します**)**
Web-based administration is a feature that allows users to configure and manage routers through a web browser interface. While this feature can provide convenience and ease of use, it can also pose a security risk, especially if the web interface is exposed to the internet or uses weak authentication or encryption methods. Web-based administration can be exploited by attackers to gain unauthorized access to the router's settings, firmware, or data, or to launch attacks such as cross-site scripting (XSS) or cross-site request forgery (CSRF). Therefore, disabling web-based administration is a good practice to harden the routers within the corporate network. Console access, routing protocols, and VLANs are other features that can be configured on routers, but they are not the most appropriate to disable for hardening purposes. Console access is a physical connection to the router that requires direct access to the device, which can be secured by locking the router in a cabinet or using a strong password. Routing protocols are essential for routers to exchange routing information and maintain network connectivity, and they can be secured by using authentication or encryption mechanisms. VLANs are logical segments of a network that can enhance network performance and security by isolating traffic and devices, and they can be secured by using VLAN access control lists (VACLs) or private VLANs (PVLANs).

質問: **250**
組織の最高情報セキュリティ責任者は、ランサムウェアからの復旧が組織が合意した RPO および RTO 内で確実に行われるようにする必要があります。次のバックアップ シナリオのうち、最も確実に復旧できるのはどれですか。

A. ローカルSANアレイに保存された1時間ごとの差分バックアップ
B. 磁気オフラインメディアにオンプレミスで保存されたDallyフルバックアップ
C. サードパーティのクラウドプロバイダーによって維持される毎日の差分バックアップ
D. 毎週の完全バックアップと毎日の増分バックアップをNASドライブに保存します
正解: **(**正解を表示します**)**
A backup strategy that combines weekly full backups with daily incremental backups stored on a NAS (Network Attached Storage) drive is likely to meet an organization's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). This approach ensures that recent data is regularly backed up and that recovery can be done efficiently, without significant data loss or lengthy downtime.

質問: **251**
次の攻撃のうち、Web サイトを使用して組織内の開発者グループを集団的に標的とするものはどれですか。
A. タイプミススクワッティング
B. 水飲み場
C. サービス拒否
D. 資格情報の再生
正解: **B (**コメントを発表する**)**
A watering hole attack compromises a website commonly visited by a specific group, such as developers, so when they visit the site, they are collectively targeted and potentially infected.

質問: **252**
ある会社の幹部が出張中に、ホテルの宿泊客用Wi-Fiなど、様々なネットワークに接続しています。セキュリティアナリストは、幹部が社内リソースに安全にアクセスできるようにするソリューションを提供する必要があります。こ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. EAP
B. ジャンプサーバー
C. 境界ネットワーク
D. VPN
正解: **D (**コメントを発表する**)**
A VPN establishes an encrypted tunnel over untrusted networks, ensuring the executive can securely access corporate internal resources from any location.

質問: **253**
セキュリティアナリストは、データベースバックエンドに接続されたフロントエンドWebサーバーからアラートを受信しました。アラートには以下のログが含まれています。

```
SELECT * FROM users WHERE UserID = 1=1
SELECT * FROM users WHERE username = 'admin'--' AND password = 'password'
IF 1=1 THEN dbms_lock.sleep(20) ELSE dbms_lock.sleep(0); END IF; END
```

次の攻撃のうちどれが発生していますか?
A. バッファオーバーフロー
B. ブルートフォース
C. インジェクション
D. リプレイ
正解: **(**正解を表示します**)**
The log shows classic SQL injection techniques-tautology (1=1), comment injection ('--), and a time-based payload (dbms_lock.sleep(20)), all indicative of an SQL injection attack.

質問: **254**
セキュリティ オペレーション センターがインシデント対応手順を改善するために使用すべきものは次のどれですか?
A. プレイブック
B. フレームワーク
C. ベースライン
D. ベンチマーク
正解: **A (**コメントを発表する**)**
A playbook is a documented set of procedures that outlines the step-by-step response to specific types of cybersecurity incidents. Security Operations Centers (SOCs) use playbooks to improve consistency, efficiency, and accuracy during incident response. Playbooks help ensure that the correct procedures are followed based on the type of incident, ensuring swift and effective remediation.
Frameworks provide general guidelines for implementing security but are not specific enough for incident response procedures.
Baselines represent normal system behavior and are used for anomaly detection, not incident response guidance.
Benchmarks are performance standards and are not directly related to incident response.

質問: **255**
ある会社では、従業員が仕事で個人の機器を使用できるようにするポリシーを導入しています。ただし、会社が承認したアプリケーションのみをインストールできるようにしたいと考えています。この懸念に対処するのは次のどれですか。
A. MDM
B. コンテナ化
C. DLP
D. 完璧
正解: **(**正解を表示します**)**
Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used.

質問: **256**
経営陣から、会社支給のタブレットで従業員が利用できない機能があり、生産性が低下しているとの報告がありました。経営陣はITチームに対し、48時間以内に問題を解決するよう指示しました。このシナリオにおいて、ITチームが活用すべき最適な解決策は次のうちどれでしょうか？
A. EDR
B. 対処する
C. FDE
D. MDM
正解: **(**正解を表示します**)**

質問: **257**
大規模な多国籍企業のセキュリティ アーキテクトは、マルチクラウド プロバイダー環境で複数の暗号化キーを安全に管理することの複雑さとオーバーヘッドを懸念しています。
セキュリティアーキテクトは、組織の既存の鍵を統合し、データの場所に関わらず一貫した集中管理と制御を維持するために、レイテンシを低減したソリューションを探しています。次のうち、アーキテクトの目的に最も適したものはどれですか？
A. トラステッド プラットフォーム モジュール
B. IaaS
C. HMaaS
D. PaaS
正解: **C (**コメントを発表する**)**
HSM as a Service (HSMaaS), Hardware security modules (HSMs) are fortified, tamper-resistant hardware components that produce, safeguard, and manage keys for encrypting and decrypting data and establishing digital signatures and certificates.

質問: **258**
セキュリティアナリストはネットワーク上で異常な動作に気づきました。ネットワーク上のIDSは、このアクティビティを検出できませんでした。セキュリティアナリストは、今後IDSがこのような攻撃を検出できるようにするために、以下のどれを使用すべきでしょうか？
A. 署名
B. 評判

C. トレンド
D. ハニーポット
正解: **(**正解を表示します**)**

質問: **259**
アプリケーションの重要なバックエンドコンポーネントにCVEが発見されました。システム管理者は、環境内でこのリスクの影響を受ける可能性のあるすべてのシステムを特定しています。
システム管理者は次のどれを実行する必要がありますか?
A. メタデータ分析
B. パケットキャプチャ
C. 脆弱性スキャン
D. 自動レポート
正解: **C (**コメントを発表する**)**

質問: **260**
ヒートマップを作成するときにアナリストが最初に実行する必要がある手順は次のどれですか? (2つ選択してください。)
A. アクセス ログを確認して、最もアクティブなデバイスを特定します。
B. オフィスのレイアウトを作成または取得します。
C. 各アクセスポイントにログインし、設定を確認します。
D. アクセス ポイント間のケーブルの長さを測定します。
E. オフィス内を計画的に歩き回り、Wi-Fi 信号強度を確認します。
F. 無線通信の障害となる可能性のあるものを取り除きます。
正解: **(**正解を表示します**)**

質問: **261**
ソフトウェア会社の最終的なソフトウェア リリースに脆弱なコードが不正または意図せず組み込まれ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. 証明書の不一致
B. 侵入テストユーティリティの使用
C. 弱いパスワード
D. 含まれているサードパーティのライブラリ
E. ベンダー/サプライチェーン
F. 古いマルウェア対策ソフトウェア
正解: **(**正解を表示します**)**
Software that is outsourced to vendors and third parties is vulnerable to malware being injected into the product from the supply chain.

質問: **262**

ある組織ではクラウド サービスを急速に導入しており、現在複数の SaaS アプリケーションを使用しています。
各アプリケーションには個別のログインがあります。そのため、セキュリティ チームは各従業員が保持しなければならない資格情報の数を減らしたいと考えています。セキュリティ チームが最初に実行すべきステップは次のどれですか。
A. SAMLを有効にする
B. OAuth トークンを作成します。
C. パスワード保管機能を使用します。
D. IdPを選択
正解**: (**正解を表示します**)**
The first step in reducing the number of credentials each employee must maintain when using multiple SaaS applications is to select an Identity Provider (IdP). An IdP provides a centralized authentication service that supports Single Sign-On (SSO), enabling users to access multiple applications with a single set of credentials.
Enabling SAML would be part of the technical implementation but comes after selecting an IdP.
OAuth tokens are used for authorization, but selecting an IdP is the first step in managing authentication.
Password vaulting stores multiple passwords securely but doesn't reduce the need for separate logins.

質問**: 263**
会社の幹部は、従業員が通常の職務とは関係のない会社の機密プロジェクトに関するシステムや情報にアクセスすることを懸念しています。セキュリティ チームがそのアクティビティを検出するために導入する可能性が高いエンタープライズ セキュリティ機能は、次のどれでしょうか。
A. EDR
B. DLP
C. NAC
D. UBA
正解**: (**正解を表示します**)**

質問**: 264**
攻撃者が悪意のあるアドレスでレジスタを上書きすると、次の脆弱性のうちどれが悪用されますか?
A. VMエスケープ
B. SQLインジェクション
C. バッファオーバーフロー
D. 競合状態
正解**: C (**コメントを発表する**)**
A buffer overflow is a vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. A

register is a small storage area in the CPU that holds temporary data or instructions. An attacker can exploit a buffer overflow to overwrite a register with a malicious address that points to a shellcode, which is a piece of code that gives the attacker control over the system. By doing so, the attacker can bypass the normal execution flow of the application and execute arbitrary commands.

質問: **265**
法務部門は、第三者によってシュレッダー処理されリサイクルされたすべてのデバイスのバックアップを保持する必要があります。この要件を最もよく表しているのは次のうちどれですか。
A. サニタイズ
B. データ保持
C. 認定
D. 破壊
正解: **(**正解を表示します**)**

質問: **266**
アプリケーション開発チームには、次の質問に答えるよう求められています。
- このアプリケーションは外部ソースからパッチを受信しますか?
- このアプリケーションにはオープンソース コードが含まれていますか?
- このアプリケーションは外部ユーザーからアクセス可能ですか?
- このアプリケーションは企業のパスワード標準を満たしていますか?
これらの質問は次のどれから来ているのでしょうか?
A. リスク管理自己評価
B. リスク管理戦略
C. リスク受容
D. リスクマトリックス
正解: **(**正解を表示します**)**
The questions listed are part of a Risk Control Self-Assessment (RCSA), which is a process where teams evaluate the risks associated with their operations and assess the effectiveness of existing controls. The questions focus on aspects such as patch management, the use of open-source code, external access, and compliance with corporate standards, all of which are critical for identifying and mitigating risks.

質問: **267**
銀行環境で監査を完了する最も適切な理由はどれですか?
A. 規制要件
B. 組織変更
C. 自己評価の要件
D. サービスレベル要件
正解: **(**正解を表示します**)**

A regulatory requirement is a mandate imposed by a government or an authority that must be followed by an organization or an individual. In a banking environment, audits are often required by regulators to ensure compliance with laws, standards, and policies related to security, privacy, and financial reporting. Audits help to identify and correct any gaps or weaknesses in the security posture and the internal controls of the organization.

質問: **268**
継続的なリスクに対する治療戦略の例は次のどれですか?
A. 新入社員の身元調査
B. 電信送金に関する二重管理要件
C. CI/CDパイプラインの一部としてのブランチ保護
D. フィッシング攻撃をブロックするメールゲートウェイ
正解: **D (**コメントを発表する**)**

質問: **269**
セキュリティ アナリストは、サーバー上で悪意のある可能性のあるビデオ ファイルを見つけ、作成日とファイルの作成者の両方を特定する必要があります。セキュリティ アナリストに必要な情報を提供する可能性が最も高いアクションは次のどれですか。
A. ファイルの SHA-256 ハッシュを取得します。
B. ファイルの内容に 16 進ダンプを使用します。
C. エンドポイント ログを確認します。
D. ファイルのメタデータを照会します。
正解: **D (**コメントを発表する**)**
Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes. Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file. To query the file's metadata, a security analyst can use various tools, such as MediaInfo, ffprobe, or hexdump, to extract and display the metadata from the video file. By querying the file's metadata, the security analyst can most likely identify both the creation date and the file's creator, as well as other relevant information. Obtaining the file's SHA-256 hash, checking endpoint logs, or using hexdump on the file's contents are other possible actions, but they are not the most appropriate to answer the question. The file's SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file's creation date or creator. Checking endpoint logs can provide some clues about the file's origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete. Using hexdump on the file's contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted.

質問: **270**

セキュリティアナリストは、インシデント発生時の証拠を収集しています。裁判で証拠の許容性を確保するために、アナリストは次のうちどれを維持する必要がありますか？
A. 保管の連鎖
B. 法的保留
C. 電子情報開示
D. 卓上演習
正解: **(**正解を表示します**)**
Chain of custody is the documented process of handling and tracking evidence from collection to presentation in court, ensuring its integrity and admissibility.

質問: **271**
セキュリティアナリストは、パスワード監査の結果を受けて、会社の認証ポリシーを改善する必要があります。ポリシーに含めるべき項目は次のどれですか？(2つ選択してください。)
A. 長さ
B. 複雑さ
C. 最小権限
D. あなたが持っているもの
E. セキュリティキー
F. 生体認証
正解: **(**正解を表示します**)**
Emphasizing password length over complexity is a best practice. The National Institute of Standards and Technology (NIST) recommends a minimum password length of 8 characters, with a preference for longer passphrases, such as 12 characters or more, to increase security and memorability.
Implementing multi-factor authentication (MFA) by requiring a physical item, like a security key or smartphone, adds a robust layer of security. This "something you have" factor ensures that even if a password is compromised, unauthorized access is still prevented.
Incorporating these elements aligns with current security best practices and strengthens your organization's defense against unauthorized access.

質問: **272**

ある企業がMFAを導入したいと考えています。スマートカード使用時に追加要素を有効にするのは次のどれですか？
A. PIN
B. ハードウェアトークン
C. ユーザーID
D. SMS
正解: **A (**コメントを発表する**)**
When using a smart card as part of MFA, the additional factor is typically a PIN. The smart card provides something you have and the PIN provides something you know, which together constitutes two factors of authentication.

質問: **273**
攻撃者は企業のウェブサイトを改ざんし、企業が製品から特定の有害化学物質を除去するまで制御権を放棄しません。このタイプの脅威アクターを最もよく表しているのは次のうちどれですか？
A. 未熟な攻撃者
B. ハクティビスト
C. 組織犯罪
D. スパイ活動
正解: **(**正解を表示します**)**
A hacktivist uses cyberattacks, such as website defacement, to advance a political or social agenda. In this case, the attacker's demand to remove harmful chemicals reflects an ideological motive, characteristic of hacktivism.

質問: **274**
特定された潜在的な脆弱性によって悪用される可能性のあるシステムが企業に存在するかどうかを判断するのに最適なチームは次のうちどれですか?
A. 白チーム
B. 青チーム
C. レッドチーム
D. 紫チーム
正解: **(**正解を表示します**)**

質問: **275**
組織では単一のオペレーティング システムのバリエーションが多すぎるため、システム イメージをユーザーにプッシュする前に配置を標準化する必要があります。組織が最初に実装する必要があるのは次のうちどれですか。
A. 標準的な命名規則
B. マッシュ
C. ネットワーク図

D. ベースライン構成
正解: **(**正解を表示します**)**
Baseline configuration is the process of standardizing the configuration settings for a system or network. In this scenario, the organization needs to standardize the operating system configurations before deploying them across the network. Establishing a baseline configuration ensures that all systems adhere to the organization's security policies and operational requirements.

質問: **276**
脅威アクターは、ユーザー名とパスワードを使用して、盗難された会社のモバイルデバイスにログインすることができました。全従業員の会社のモバイルデバイスにおけるモバイルデータのセキュリティを強化するための最適なソリューションは次のうちどれですか？
A. アプリケーション管理
B. フルディスク暗号化
C. リモートワイプ
D. コンテナ化
正解: **(**正解を表示します**)**
The question was not asking about the single phone that was stolen (in which case a remote wipe may work after the fact); rather, it asks for "the best solution to increase mobile data security on all employees' company mobile devices".

質問: **277**
システム管理者は、ベンダーからのサポートが受けられなくなったシステムを発見しました。しかし、このシステムとその環境は事業運営に不可欠であり、変更はできず、オンライン状態を維持する必要があります。この状況において、以下のリスク対策のうち最も適切なものはどれでしょうか？
A. 転送
B. 受け入れる
C. 拒否
D. 避ける
正解: **(**正解を表示します**)**

質問: **278**
セキュリティアナリストは、企業ネットワークのエッジにおけるポートスキャンの増加に気づきました。攻撃者の送信元IPアドレスを取得するために、アナリストは次のどのログを確認すべきでしょうか？
A. OSセキュリティ
B. ファイアウォール
C. アプリケーション
D. エンドポイント

正解: **(**正解を表示します**)**
A firewall log records inbound and outbound network traffic, including source and destination IP addresses, port numbers, and connection attempts. Since port scans involve probing various ports on a network, the firewall logs will provide visibility into the attacker's source IP address and help the analyst assess the nature of the scanning activity.

質問: **279**
管理者は、企業のLDAPディレクトリ内のオブジェクトを表示するためにLDAPブラウザツールをインストールしています。LDAPサーバーへの安全な接続が必要です。ブラウザがサーバーに接続すると、証明書エラーが表示され、その後接続が切断されます。最も可能性の高い解決策は次のどれですか？
A. 管理者はブラウザ設定で SAN 証明書を許可する必要があります。
B. 管理者は、サーバー証明書をローカル トラストストアにインストールする必要があります。
C. 管理者は、安全な LDAP ポートをサーバーに開くように要求する必要があります。
D. 管理者は、組織の RA の TLS バージョンを上げる必要があります。
正解: **B (**コメントを発表する**)**
The administrator needs to the server's certificate in the local trust store of the machine where LDAP browser tool is being used. This will allow the client to trust the server's certificate and establish a secure connection.

質問: **280**
ある企業は、自社のデータがダークウェブ上で販売されていることを知りました。初期調査の結果、そのデータは機密データであると判断しました。次に企業が取るべきステップは次のうちどれですか？
A. 攻撃者の侵入方法を特定します。
B. 会社のシステムの脆弱性スキャンを実施します。
C. 違反行為を地元当局に報告します。
D. 違反について関係当事者に通知します。
正解: **(**正解を表示します**)**

質問: **281**
管理者は、限られた予算内で、製造施設内の複数の耐用年数を経たSCADAデバイスのセキュリティを確保する必要があります。これらのデバイスを最も効果的に保護するために、セキュリティ管理者は次のうちどれを実施すべきでしょうか。
A. SCADAデバイスを独自のサブネットにセグメント化します
B. SCADAデバイスをネットワーク監視ツールに追加する
C. SCADAデバイスにセキュリティパッチを適用する
D. SCADAデバイスへのインターネットアクセスをブロックします
正解: **A (**コメントを発表する**)**

Network segmentation isolates end-of-life SCADA devices from other systems, reducing the attack surface and limiting lateral movement, which is critical when patching or direct security updates are not possible.

質問: **282**
企業ネットワークから切断されている間に、企業システム上の悪意のある動作を検出してブロックするエージェントベースのアプリケーションについて説明しているものは次のうちどれですか?
A. エンドポイント保護
B. システムパッチ
C. HIDS
D. NGFW
正解: **A (**コメントを発表する**)**
Endpoint protection is an agent-based solution installed on devices that can detect and block malicious activity locally, allowing it to function even when the system is disconnected from the corporate network.

質問: **283**
次の契約のうち、応答時間、エスカレーション ポイント、パフォーマンス メトリックを定義しているものはどれですか。
A. BPA
B. MOA
C. NDA
D. SLA
正解: **D (**コメントを発表する**)**
An SLA spells out exactly how fast a provider must respond and resolve issues, what thresholds and KPIs will be measured (uptime, throughput, MTTR), and when/whom to escalate to if those targets aren't met, making it the formal document for response times, escalation paths, and performance metrics.

質問: **284**
セキュリティエンジニアは、既知の悪意のあるファイルのシグネチャを迅速に識別する必要があります。セキュリティエンジニアが最もよく使用する分析手法は次のうちどれですか？
A. サンドボックス
B. ネットワークトラフィック
C. 静的
D. パッケージ監視
正解: **(**正解を表示します**)**

質問: **285**

管理者は、ユーザーが勤務時間外にリモートでログインし、大量のデータを個人のデバイスにコピーしたという通知を受けました。
ユーザーのアクティビティを最もよく表すものはどれですか?
A. 侵入テスト
B. フィッシング キャンペーン
C. 外部監査
D. 内部脅威
正解: **(**正解を表示します**)**
An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data.

質問: **286**
ある組織は、建物の入口と機密エリアを監視するためにクラウド管理の IP カメラを導入しました。
サービス プロバイダーは、各カメラからのライブ ビデオ映像をストリーミングするために、直接 TCP/IP 接続を有効にします。組織は、このストリームが暗号化され、認証されることを保証したいと考えています。この目的を最もよく満たすには、次のどのプロトコルを実装する必要がありますか。
A. SSH
B. SRTP
C. S/MIME
D. PPTP
正解: **(**正解を表示します**)**
Secure Real-Time Transport Protocol (SRTP) is a security protocol used to encrypt and authenticate the streaming of audio and video over IP networks. It ensures that the video streams from the IP cameras are both encrypted to prevent unauthorized access and authenticated to verify the integrity of the stream, making it the ideal choice for securing video surveillance.

質問: **287**
ネットワークチームは、サポート終了間近の重要なサーバーを、特定のデバイスのみがアクセスでき、境界ネットワークからはアクセスできないVLANにセグメント化しました。チームが実装した制御について、最も適切な説明は次のうちどれですか(2つ選択してください)。
A. 管理職
B. 物理
C. 修正
D. 探偵
E. 補償
F. テクニカル
G. 抑止力
正解: **(**正解を表示します**)**
Technical controls involve the use of technology to manage or mitigate risks. By segmenting the server into VALN and restricting access to specific devices, the network team has employed a technical control here.
Compensating controls are alternative measures in place to address a risk when the primary control is not feasible which in these case segmenting the server into VLAN and limiting access can be seen as compensating control.

質問: **288**
設計変更を実施する前に、セキュリティ上の問題が発生しないことを確認するために、複数の手順を踏む必要があります。これらの手順のうち、最も可能性の高いものはどれですか？
A. メンテナンス
B. ボードレビュー
C. サービスの再起動
D. バックアウト計画
正解: **(**正解を表示します**)**

質問: **289**
管理者は、ネットワークに接続するすべてのゲストデバイスに対して検疫サブネットを設定しました。企業リソースへのアクセスを許可する前に、セキュリティチームがMDM上で設定するのに最適な項目は次のうちどれですか？
A. デバイスフィンガープリンティング
B. コンプライアンス証明
C. NAC
D. 802.1X
正解: **(**正解を表示します**)**

Compliance attestation via MDM verifies device posture (OS version, policies, certificates) before granting access, ensuring only compliant devices leave the quarantine subnet and reach corporate resources.

質問: **290**
ある企業が保険契約に加入することを決定しました。この企業は以下のどのリスク管理戦略を実施していますか？
A. 軽減
B. 受け入れる
C. 避ける
D. 転送
正解: **D (コメントを発表する)**
Purchasing an insurance policy is a risk transfer strategy, as the financial impact of a risk is shifted from the company to the insurance provider.

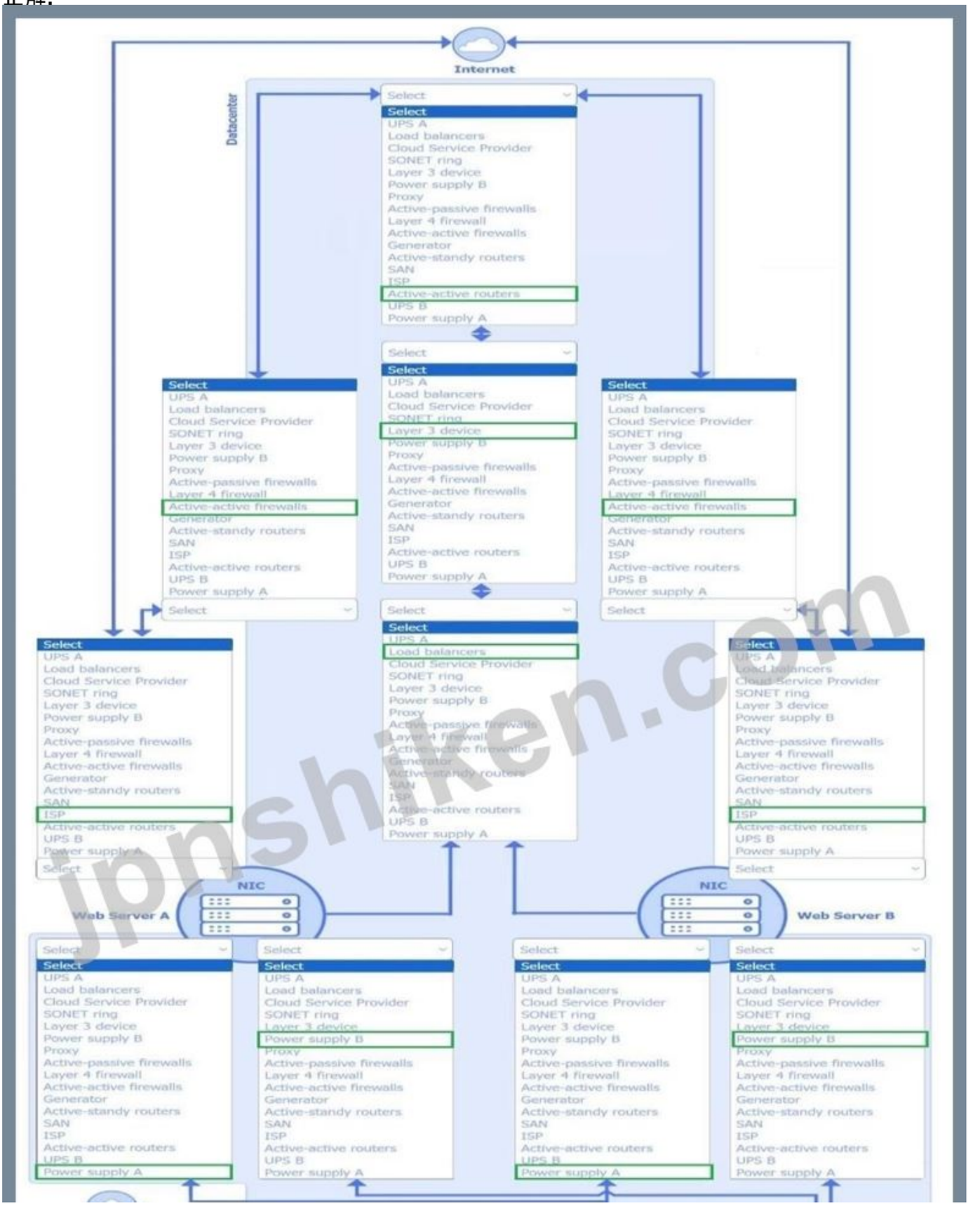
質問: **291**
次のトピックのうち、組織の SDLC に含まれる可能性が高いのはどれですか?
A. サービスレベル契約
B. 情報セキュリティポリシー
C. 侵入テストの方法論
D. ブランチ保護要件
正解: **(正解を表示します)**
Branch protection requirements are related to the version control and development process within the SDLC, ensuring that code changes are reviewed, tested, and approved before being merged into main branches. This helps maintain code quality and security throughout the development process.
Penetration testing is usually conducted as part of the testing phase or after deployment to identify vulnerabilities and security weaknesses. It is a separate process from the core stages of the SDLC but is an important aspect of ensuring the security and robustness of the application once development is completed.

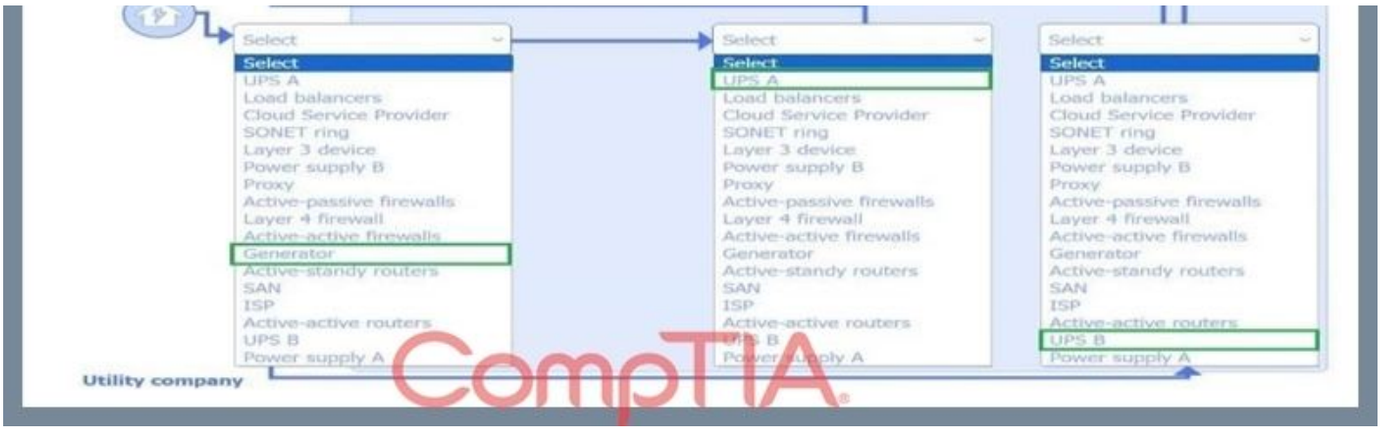
質問: **292**
ある組織は最近、顧客が Web ポータルを通じてアクセスする新しいサービスのホスティングを開始しました。セキュリティ エンジニアは、この新しいサービスを保護するために、既存のセキュリティ デバイスに新しいソリューションを追加する必要があります。エンジニアが最も導入する可能性が高いのは次のどれですか。
A. レイヤー4ファイアウォール
B. NGFW
C. WAF
D. UTM

正解: **(**正解を表示します**)**
The security engineer is likely to deploy a Web Application Firewall (WAF) to protect the new web portal service. A WAF specifically protects web applications by filtering, monitoring, and blocking HTTP requests based on a set of rules. This is crucial for preventing common attacks such as SQL injection, cross-site scripting (XSS), and other web-based attacks that could compromise the web service.
* Layer 4 firewall operates primarily at the transport layer, focusing on IP address and port filtering, making it unsuitable for web application-specific threats.
* NGFW (Next-Generation Firewall) provides more advanced filtering than traditional firewalls, including layer 7 inspection, but the WAF is tailored specifically for web traffic.
* UTM (Unified Threat Management) offers a suite of security tools in one package (like antivirus, firewall, and content filtering), but for web application-specific protection, a WAF is the best fit.

質問: **293**
シミュレーション3
セキュリティアーキテクトは、高い耐障害性を備えたビジネスクリティカルなアプリケーションの設計を担います。アプリケーションのSLAは99.999%です。
説明書
アプリケーションの回復力を実現するために、適切な場所のネットワーク、電源、およびサーバーコンポーネントを選択します。
場所ごとにコンポーネントを選択する必要があり、コンポーネントは複数回選択できます。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。

正解:





質問: **294**
ソフトウェアエンジニアがパブリックリポジトリからサードパーティ製アプリケーションをダウンロードする際に、そのアプリケーションが悪意を持って改変されていないことを確認したいとします。エンジニアは次のうちどの手法を用いるべきでしょうか？
A. 動的解析
B. コード署名
C. 転送中の暗号化
D. 静的解析
正解: **(**正解を表示します**)**
Code signing provides a cryptographic signature that verifies the software's authenticity and integrity, ensuring it has not been tampered with before download or installation.

質問: **295**
ある銀行が顧客の個人情報(PII)を保管する新しいサーバーを設置しました。機密データが改ざんされないようにするために、銀行は次のどれを採用すべきでしょうか？
A. フルディスク暗号化
B. ネットワークアクセス制御
C. ユーザー行動分析
D. ファイル整合性監視
正解: **(**正解を表示します**)**

質問: **296**
企業がインターネットからのシステムへのアクセスを最も効果的に防止できるのは次のうちどれですか?
A. コンテナ化
B. 仮想化
C. SD-WAN
D. エアギャップ
正解: **D (**コメントを発表する**)**
An air-gapped system is physically and logically isolated from any external (internet-facing) network, so packets from the internet simply have no path to reach it. This architectural

separation is the most definitive way to prevent internet access altogether, rather than just limiting or monitoring it.

質問: **297**
ある企業は、パイプ内のガスの物理的な流れを制御する特殊なレガシープラットフォームを保護したいと考えています。この目標を最も効果的に達成するために、企業が保護する必要がある環境は次のうちどれですか？
A. IaaS
B. SCADA
C. SDN
D. IoT
正解: **B** (コメントを発表する)
SCADA systems are industrial control environments designed to monitor and manage processes like the physical flow of gas in pipelines, so securing the SCADA environment protects the legacy platform that controls those operations.

質問: **298**
複数の地理的拠点を持つ組織は、各拠点にMPLS、4G/5G、ブロードバンド、ダイヤルアップなど、様々なインターネット回線を導入しています。アーキテクトは、拠点間の一貫性を保ち、特定の基準に基づいてリンクを活用できるソリューションを構築しています。
アーキテクトが構成するのに最適なソリューションは次のどれですか?
A. SD-WAN
B. UTM
C. VPN
D. SASE
正解: (正解を表示します)
Software-defined wide area networking centrally manages multiple types of WAN links and dynamically selects paths based on performance, cost, and policy criteria, ensuring consistent connectivity and optimized use of all available circuits across geographically distributed locations.

質問: **299**
弱い暗号化アルゴリズムを使用してシステムに直接アクセスすることによって生じる潜在的な脆弱性を悪用する攻撃は次のどれですか?
A. パスワードクラッキング
B. パス上
C. デジタル署名
D. サイドチャネル
正解: (正解を表示します)
Password cracking attacks exploit weak cryptographic algorithms by attempting to guess or decrypt passwords through direct access to systems or password hashes, making use of vulnerabilities in the cryptography.

質問: **300**
転送中のデータを保護するのに最もよく使用されるデータ保護方法は次のうちどれですか?
A. 暗号化
B. 難読化
C. 権限制限
D. ハッシュ
正解: (正解を表示します)
Encryption transforms data into ciphertext before transmission, ensuring that intercepted information remains unreadable to unauthorized parties and thus securing data in transit.

質問: **301**
入力フィールドを使用して、データを表示または操作できるコマンドを実行できるようにするのは次のどれですか。
A. クロスサイトスクリプティング
B. サイドローディング
C. バッファオーバーフロー
D. SQLインジェクション
正解: (正解を表示します)
SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server. SQL injection is one of the most common and dangerous web application vulnerabilities.

質問: **302**
ユーザーがウェブページを閲覧中に、別のサイトに移動するように指示するリンクを含むポップアップが表示されます。このサイトは次のうちどれに対して脆弱ですか？
A. DoS
B. XSS
C. SQLi
D. 目次
正解: (正解を表示します)

Cross-Site Scripting (XSS) allows attackers to inject malicious scripts into a web page, which can display pop-ups or redirect users to other sites without their consent.

質問: **303**
セキュリティ アナリストは、人事部門が実装しようとしている SaaS アプリケーションを評価しています。アナリストは、SaaS ベンダーに SOC 2 レポートを要求します。アナリストが実行する可能性が高いプロセスは次のどれですか。
A. 内部監査
B. 侵入テスト
C. 証明
D. デューデリジェンス
正解: **D (コメントを発表する)**
Due diligence in this context involves evaluating the security, availability, processing integrity, confidentiality, and privacy of the SaaS application by reviewing the SOC 2 report provided by the vendor. This process helps ensure that the vendor meets the required security and operational standards before the SaaS application is implemented.

質問: **304**
社内セキュリティチームは、不審な添付ファイルを調査しており、隔離された環境で動作分析を実施したいと考えています。セキュリティチームが最も使用する可能性が高いのは次のうちどれですか？
A. サンドボックス
B. ジャンプサーバー
C. 仕事用コンピュータ
D. コンテナ
正解: **(正解を表示します)**
A sandbox provides an isolated environment where suspicious files can be safely executed and monitored for malicious behavior without risking the security of the production network or systems.

質問: **305**
エアギャップ ネットワークで最も一般的なデータ損失パスは次のどれですか?
A. 要塞ホスト
B. 保護されていない Bluetooth
C. パッチ未適用の OS
D. リムーバブルデバイス
正解: **D (コメントを発表する)**
An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks.

Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air- gapped network.

質問: **306**
ある会社のエンドユーザーから、外部の Web サイトにアクセスできないという報告がありました。アナリストは、DNS サーバーのパフォーマンス データを調べたところ、CPU、ディスク、メモリの使用量は最小限であるものの、ネットワーク インターフェイスが受信トラフィックであふれていることを発見しました。ネットワーク ログには、このサーバーに送信された DNS クエリの数がわずかしか表示されていません。セキュリティ アナリストが見ている状況を最もよく表しているのは、次のどれですか。
A. 同時セッションの使用
B. セキュアDNS暗号化のダウングレード
C. パス上のリソース消費
D. 反射型サービス拒否
正解: **(正解を表示します)**
A reflected denial of service (RDoS) attack is a type of DDoS attack that uses spoofed source IP addresses to send requests to a third-party server, which then sends responses to the victim server. The attacker exploits the difference in size between the request and the response, which can amplify the amount of traffic sent to the victim server. The attacker also hides their identity by using the victim's IP address as the source. A RDoS attack can target DNS servers by sending forged DNS queries that generate large DNS responses. This can flood the network interface of the DNS server and prevent it from serving legitimate requests from end users.

質問: **307**
SOC アナリストは、エンド ユーザーのマシン上でリモート コントロール セッションを確立し、ファイル内で次のことを発見します。
gmail.com[ENT]my.name@gmail.com[ENT]NoOneCanGuessThis123! [ENT]スーザンさん、こんにちは。先日はお会いできて嬉しかったです！近いうちにフォローアップミーティングを開催しましょう。[BACKSPACE]こちらが登録リンクです。[RTN][CTRL]c [CTRL]v [RTN]after[BACKSPACE]登録後、私の携帯電話にお電話ください。
SOC アナリストが最初に実行する必要があるアクションは次のうちどれですか。
A. ユーザーにパスワードを変更するようアドバイスします。
B. 職場での個人用メールに関するポリシーを確認します。
C. エンド ユーザーのマシンのイメージを再作成します。
D. ホストのファイアウォール ログを確認します。
正解: **(正解を表示します)**

質問: **308**
セキュリティ アナリストが複数の会社のファイアウォールを評価しています。アナリストが評価

中に使用するカスタム パケットを生成するために使用する可能性が高いのは次のどのツールでしょうか。
A. hping
B. Wireshark
C. PowerShell
D. netstat
正解: **(**正解を表示します**)**
Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

質問: **309**
セキュリティアナリストは、最近のインシデントで使用された攻撃ベクトルが、IoTデバイスの既知のエクスプロイトであったことを知りました。アナリストは、最初のエクスプロイトの発生時刻を特定するためにログを確認する必要があります。アナリストが最初に確認すべきログは次のうちどれですか？
A. 無線アクセスポイント
B. スイッチ
C. ファイアウォール
D. NAC
正解: **C (**コメントを発表する**)**
The firewall is the choke point that records every inbound/outbound session to the IoT device; its timestamps on the first suspicious connection will most reliably show when the exploit traffic first hit the network. Reviewing those entries pinpoints the initial compromise time before diving into more granular device or segment logs.

質問: **310**
次のどれがクラウド環境における高可用性として分類されますか?
A. アクセスブローカー
B. クラウド HSM
C. WAF
D. ロードバランサー
正解: **D (**コメントを発表する**)**
In a cloud environment, high availability is typically ensured through the use of a load balancer. A load balancer distributes network or application traffic across multiple servers, ensuring that no single server becomes overwhelmed and that services remain available even if one or more servers fail. This setup enhances the reliability and availability of applications.
Load balancer: Ensures high availability by distributing traffic across multiple servers or instances, preventing overload and ensuring continuous availability.
Access broker: Typically refers to a service that facilitates secure access to resources, not directly related to high availability.

Cloud HSM (Hardware Security Module): Provides secure key management in the cloud but does not specifically ensure high availability.
WAF (Web Application Firewall): Protects web applications by filtering and monitoring HTTP traffic but is not primarily focused on ensuring high availability.

質問: **311**
顧客が新しい携帯電話の基盤となるファイル構造を変更し、管理者権限でキーロガーをインストールしました。これは次のうちどれに当てはまりますか？
A. リソースの再利用
B. ブロートウェアのインストール
C. サイドローディング
D. 脱獄
正解: **(**正解を表示します**)**
Modifying the device's file structure to gain root access and install unauthorized software describes jailbreaking.

質問: **312**
次のシナリオのうち、トークン化がプライバシー技術として最も適しているのはどれですか?
A. ソーシャルメディアのユーザーアカウントに疑似匿名化を提供する
B. 認証リクエストの2番目の要素として機能する
C. 既存の顧客がクレジットカード情報を安全に保管できるようにする
D. データをセグメント化してデータベース内の個人情報をマスキングする
正解: **(**正解を表示します**)**
Tokenization is a process that replaces sensitive data, such as credit card information, with a non- sensitive equivalent (token) that can be used in place of the actual data. This technique is particularly useful in securely storing payment information because the token can be safely stored and transmitted without exposing the original credit card number.

質問: **313**
レッドチームのプロバイダーが組織の施設に同行しました。以下のどれが発生しましたか？
A. 内部脅威
B. ブルートフォース攻撃
C. 物理的侵入テスト
D. 積極的偵察
正解: **C (**コメントを発表する**)**
Tailgating into a facility during a red-team exercise is a form of physical penetration testing, where security is evaluated by attempting to bypass physical access controls.

質問: **314**
次のどれが、データベースの誤った構成を悪用しようとする試みに関係していますか?
A. バッファオーバーフロー

B. SQLインジェクション
C. VMエスケープ
D. メモリインジェクション
正解: **B** (コメントを発表する)
SQL injection is a type of attack that exploits a database misconfiguration or a flaw in the application code that interacts with the database. An attacker can inject malicious SQL statements into the user input fields or the URL parameters that are sent to the database server. These statements can then execute unauthorized commands, such as reading, modifying, deleting, or creating data, or even taking over the database server. SQL injection can compromise the confidentiality, integrity, and availability of the data and the system.

質問: **315**
クラウド サービス プロバイダーと顧客間の構成、保守、およびセキュリティの役割を概説しているのは次のうちどれですか。
A. サービスレベル契約
B. 責任マトリックス
C. 覚書
D. 秘密保持契約
正解: (正解を表示します)
A responsibility matrix clearly defines and outlines the division of configuration, maintenance, and security roles between a cloud service provider and the customer.

質問: **316**
最も一般的なアプリケーション活用方法に関する情報を参照するのに最適なリソースは次のどれですか?
A. OWASP
B. スティックス
C. 楕円
D. 脅威情報フィード
E. 共通脆弱性情報
正解: (正解を表示します)
OWASP (Open Web Application Security Project). OWASP provides extensive resources, guidelines, and tools related to web application security, including the OWASP Top 10, which lists the most critical security risks to web applications.

質問: **317**
ある学区が州の試験を実施していた際、セキュリティアナリストはすべてのインターネットサービスが利用できないことに気付きました。アナリストはネットワーク上でARPポイズニングが発生していることを発見し、該当ホストへのアクセスを遮断しました。この悪意ある活動に最も関連していると思われるのは次のうちどれですか？
A. 未熟な攻撃者
B. シャドーIT
C. クレデンシャルスタッフィング
D. DMARC失敗
正解: **(**正解を表示します**)**
ARP poisoning is a basic attack that does not require advanced skills or tools, making it a common method used by unskilled attackers (also known as "script kiddies") to disrupt network operations.

質問: **318**
ネットワーク管理者は、ネットワーク トラフィックが転送中に高度に安全であることを保証したいと考えています。次のアクションのうち、ネットワーク管理者が実行すべきアクションを最もよく表すものはどれですか。
A. 境界 IPS を構成して、受信 HTTPS ディレクトリ トラバーサル トラフィックをブロックし、署名が毎日更新されることを確認します。
B. EDR ソフトウェアが脅威の攻撃者が使用する可能性のある不正なアプリケーションを監視し、セキュリティ チームにアラートを構成することを確認します。
C. ネットワークで使用するために TLS およびその他の暗号化されたプロトコルのみが選択されていることを確認し、安全なプロトコルを介して承認されたトラフィックのみを許可します。
D. すべてのネットワーク セグメントで NAC が適用されていることを確認し、ファイアウォールのポリシーが更新されて不正なトラフィックがブロックされていることを確認します。
正解: **(**正解を表示します**)**

質問: **319**
セキュリティ アナリストは、展開のために新しいデバイスを強化するときにサーバー チームが従うベースを作成しています。
アナリストが作成しているものを説明するビートは次のどれですか?
A. 変更管理手順
B. 情報セキュリティポリシー
C. サイバーセキュリティフレームワーク
D. セキュアな構成ガイド
正解: **(**正解を表示します**)**

The security analyst is creating a "secure configuration guide," which is a set of instructions or guidelines used to configure devices securely before deployment. This guide ensures that the devices are set up according to best practices to minimize vulnerabilities and protect against potential security threats.

質問: **320**
企業の取締役会は、事業運営においてどの活動がリスクが高すぎるかを経営陣に伝える必要があります。取締役会は、以下のどのリスク管理戦略を経営陣に説明する必要がありますか？
A. 会社のリスク評価
B. 企業のリスク受容
C. 会社のリスクレジスター
D. 企業のリスク許容度
正解: **(正解を表示します)**
Risk tolerance defines the threshold of risk the organization is willing to accept. Activities that exceed this threshold are deemed too risky to pursue during normal operations.

質問: **321**
セキュリティ エンジニアがすべての送信メールで S/MIME デジタル署名を使用するように設定する理由として最も適切なのは次のどれですか。
A. コンプライアンス基準を満たすため
B. 配達率を上げるため
C. フィッシング攻撃をブロックする
D. 否認防止を確保するため
正解: **(正解を表示します)**
S/MIME digital signatures provides a way to ensure that the email has not been altered and that it genuinely comes from the sender (Non-repudiation).

質問: **322**
システム設計の年次レビュー中に、エンジニアが現在リリースされている設計にいくつかの問題点を発見しました。ベストプラクティスに従えば、次に実行すべき対策は次のどれですか？
A. リスク管理プロセス
B. 製品設計プロセス
C. 設計レビュープロセス
D. 変更管理プロセス
正解: **D (コメントを発表する)**
Change control process: The change control process ensures that any modifications to the design are systematically evaluated, approved, and documented. This helps in maintaining the integrity of the system and ensures that changes are implemented in a controlled and coordinated manner.
質問: **323**
経理部門の従業員が、ベンダーが実行したサービスに対する支払い要求を含む電子メールを受信

しますが、ベンダーはベンダー管理データベースに存在しません。このシナリオの例は次のどれですか。
A. プリテキスティング
B. なりすまし
C. ランサムウェア
D. 請求書詐欺
正解: (正解を表示します)
The scenario describes an instance where an employee receives a fraudulent invoice from a vendor that is not recognized in the company's vendor management system. This is a classic example of an invoice scam, where attackers attempt to trick organizations into making payments for fake or non- existent services. These scams often rely on social engineering tactics to bypass financial controls.

質問: **324**
ある組織はソフトウェア開発環境に欠陥を発見し、外部からの脅威からシステムをより適切に保護するために、代替的な対策を導入しています。次のうち、最も効果的な対策はどれですか？(2つ選択してください。)
A. プラットフォームの強化
B. 拡張ログ
C. ネットワークセグメンテーション
D. アクセス制御
E. データ暗号化
F. アプリケーション許可リスト
正解: (正解を表示します)
Platform hardening locks down development hosts, removing unnecessary services and closing unused ports, so attackers have fewer vulnerabilities to exploit. An application allow list ensures only approved, vetted software can run in the environment, preventing malicious or untested code from executing.

質問: **325**
実行時にデプロイされたアプリケーションで実行できる識別方法の種類は次のどれですか?
A. 動的解析
B. コードレビュー
C. パッケージ監視
D. バグバウンティ
正解: (正解を表示します)
Dynamic analysis is performed on software during execution to identify vulnerabilities based on how the software behaves in real-world scenarios. It is useful in detecting security issues that only appear when the application is running.

質問: **326**

システム管理者は、クラウドベースの低コストのアプリケーション ホスティング ソリューションを探しています。
次のどれがこれらの要件を満たしていますか?
A. SDN
B. SD-WAN
C. Type 1 hvpervisor
D. Serverless framework
正解: **(**正解を表示します**)**

質問: **327**
組織は特定の情報を非表示にする必要があります。このタスクを達成するために、組織は次のどれを使用すべきでしょうか？
A. 難読化
B. 分類ポリシー
C. 検証
D. ブロックルール
正解: **A (**コメントを発表する**)**
Obfuscation hides or masks sensitive information so it is not easily understood or readable by unauthorized individuals while still allowing authorized processing or use when required.

質問: **328**
セキュリティアナリストは、ネットワークへのアクセスを強化する必要があります。要件の一つとして、スマートカードによるユーザー認証が挙げられます。この要件を最も適切に満たすために、アナリストは次のどれを有効にすべきでしょうか？
A. チャップ
B. PEAP
C. MS-CHAPv2
D. EAP-TLS
正解: **(**正解を表示します**)**
EAP-TLS is a strong and secure authentication method that involves the use of digital certificates, typically stored on smart cards, for user authentication. It requires the user to present a valid certificate, which is verified by the authentication server, providing a high level of security.

質問: **329**
企業は、従業員が意図せずネットワークにマルウェアを持ち込むことを懸念しています。
同社は、社内IT部門から送信されたメールに埋め込まれたリンクをクリックした従業員50名を特定しました。セキュリティ体制を最も効果的に改善するために、会社が実施すべき対策は次のうちどれですか？
A. ソーシャルエンジニアリングトレーニング
B. SPF設定
C. 模擬フィッシングキャンペーン

D. 内部脅威の認識
正解: **(**正解を表示します**)**
IT department already conducted a phishing camping, Social engineering would be best to improve security posture.

質問: **330**
ヘルプデスクには、古いバージョンのOSを搭載したマシンの動作が遅いという問い合わせが複数寄せられています。複数のユーザーからウイルス検出アラートが表示されています。以下の緩和策のうち、まずどれを検討すべきでしょうか？
A. パッチ適用
B. セグメンテーション
C. 監視
D. 分離
正解: **A (**コメントを発表する**)**
The best first step is to review patching. Outdated OS versions often contain vulnerabilities that can be exploited by malware. Ensuring systems are up-to-date is a foundational cybersecurity practice.

質問: **331**
会社の Web フィルターは、URL をスキャンして文字列を検索し、一致するものが見つかった場合はアクセスを拒否するように設定されています。暗号化されていない Web サイトへのアクセスを禁止するには、アナリストは次のどの検索文字列を使用する必要がありますか。
A. encryption=off\
B. http://
C. www.*.com
D. :443
正解: **(**正解を表示します**)**
http:// is an insecure protocol running on port 80 that uses unencrypted traceable data for communication on uncertified, & unprotected websites. It is indicated that you are on one of these insecure websites by a warning, or lack of padlock in your web search URL.

質問: **332**
大企業のサイバーセキュリティ インシデント対応チームは、複数の企業デスクトップにマルウェアが存在するという通知を受け取りました。ネットワーク上で既知の侵害の兆候は見つかりませんでした。環境を保護するために、チームが最初に行うべきことは次のうちどれですか。

A. 影響を受けるホストを封じ込める
B. マルウェアをアプリケーション ブロックリストに追加します。
C. コア データベース サーバーをセグメント化します。
D. ファイアウォールルールを実装して、送信ビーコンをブロックする
正解: **(**正解を表示します**)**
The first step in responding to a cybersecurity incident, particularly when malware is detected, is to contain the impacted hosts. This action prevents the spread of malware to other parts of the network, limiting the potential damage while further investigation and remediation actions are planned.

質問: **333**
提供される内容と、企業にリソースを提供するために必要な許容時間に関する企業と顧客間の合意を説明したものはどれですか。
A. SLA
B. MOU
C. MOA
D. BPA
正解: **(**正解を表示します**)**
A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.
* MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.
* BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.

質問: **334**
データベース サーバーによってアクティブに処理されているデータに適用されるデータ状態は次のどれですか。
A. 使用中
B. ハッシュ化中
C. 休止中
D. 輸送中
正解: **(**正解を表示します**)**

質問: **335**
組織内の誠実性と倫理的行動に関連する期待を確立し、伝達するために最も頻繁に使用される組織文書は次のどれですか?
A. MOA
B. AUP

C. EULA
D. SLA
正解: **(**正解を表示します**)**

質問: **336**
次のデータ復旧戦略のうち、低コストで迅速な復旧を実現するものはどれですか?
A. Hot
B. Cold
C. Manual
D. Warm
正解: **(**正解を表示します**)**
A cold site is the least expensive recovery option, providing space and infrastructure but no active systems, allowing for recovery at a lower cost-though with slower setup compared to hot or warm sites.

質問: **337**
ネットワークエンジニアは、システムの可用性を向上させるために冗長スイッチスタックを導入しました。しかし、予算では1つのISP接続の費用しか賄えません。潜在的なリスク要因を最もよく表しているのは次のうちどれですか？
A. 機器の MTBF は不明です。
B. ISP には SLA がありません。
C. RPO が決定されていません。
D. 単一障害点があります。
正解: **(**正解を表示します**)**
Since the budget only allows for one ISP connection, this create a single point of failure for the network connectivity.
質問: **338**
あるユーザーがカフェで政府支給のノートパソコンを使っています。見知らぬ人がユーザーと会話を始め、勤務先や部署、その他の個人情報について質問し始めました。この見知らぬ人の行動を最もよく表しているのは次のうちどれですか？
A. 内部脅威
B. フィッシング
C. ソーシャルエンジニアリング
D. 危険
正解: **(**正解を表示します**)**
The stranger is manipulating a casual conversation to elicit sensitive details (employer, division, personal info). This intentional information-gathering through interpersonal interaction is classic social engineering - exploiting human trust rather than technical flaws.

質問: **339**
ある会社では、財務データを第三者に転送するためにレガシー FTP サーバーを使用しています。

レガシー システムは SFTP をサポートしていないため、転送中の機密性の高い財務データを保護するための補償制御が必要です。次のどれが会社にとって最も適切な使用方法でしょうか。
A. Telnet接続
B. SSHトンネリング
C. フルディスク暗号化
D. パッチのインストール
正解: **B** (コメントを発表する)

質問: **340**
セキュリティ アナリストは、潜在的な悪意のあるアクティビティを可視化するために、ユーザーとデバイスの動作をより深く理解したいと考えています。アナリストは、アクションが共通のベースラインから逸脱したときにそれを検出するためのコントロールを必要としています。アナリストは次のどれを使用する必要がありますか。
A. 侵入防止システム
B. ウイルス対策
C. エンドポイントの検出と応答
D. サンドボックス
正解: (正解を表示します)

質問: **341**
会社のマーケティング部門は、機密性の高い顧客データを収集、変更、保存します。インフラストラクチャ チームは、転送中および保存中のデータのセキュリティ保護を担当します。次のデータロールのどれが顧客を表していますか?
A. プロセッサ
B. オーナー
C. 件名
D. 管理者
正解: (正解を表示します)

質問: **342**
システム障害が発生した場合にシステム状態を最も効率的に維持するオプションは次のどれですか?
A. ハイブリッドクラウド
B. コールドサイト
C. 完全バックアップ
D. 負荷分散
正解: (正解を表示します)
Full backup captures the entire system including the operating system, installed applications, system settings, and user data. This allows for complete system recovery to the exact previous state, which is critical after a failure.
While system state backups focus only on critical OS components and configuration data (like

boot files, registry, Active Directory), they do not include user data and applications. System state recovery is quicker, but less comprehensive and requires the original hardware and OS version to restore properly.

質問: **343**
暗号化とハッシュの違いを説明しているのは次のうちどれですか?
A. 暗号化は転送中のデータを保護し、ハッシュは保存中のデータを保護します。
B. 暗号化によりデータの整合性が確保され、ハッシュによりデータの機密性が確保されます。
C. 暗号化では公開鍵交換が使用され、ハッシュでは秘密鍵が使用されます。
D. 暗号化では平文が暗号文に置き換えられ、ハッシュではチェックサムが計算されます。
正解: **(**正解を表示します**)**

質問: **344**
セキュリティ意識向上プログラムのコミュニケーション要素として含まれる可能性が最も高いのは次のどれですか?
A. フィッシング詐欺やその他の疑わしい行為を報告する
B. 異常行動認識による内部脅威の検出
C. サードパーティの侵入テストの一環としてソーシャルエンジニアリングを実行する
D. 電信送金データを変更する際の情報の確認
正解: **(**正解を表示します**)**

質問: **345**
許容使用ポリシーは、次のセキュリティ制御タイプのうちどれを最もよく表していますか?
A. 探偵
B. 補償
C. 修正
D. 予防的
正解: **(**正解を表示します**)**
Preventive - an acceptable use policy enforces rules to users to use company resources. example - company A states that in order to access files in the company server you must connect to your company VPN when working from home. This prevents you from connecting from an insecure network.

質問: **346**
政府職員が、防衛戦術情報を含む機密ファイルを秘密裏に外付けドライブにコピーしました。その後、その外付けドライブを腐敗組織に渡しました。この職員の動機を最もよく表しているのは次のうちどれですか。
A. スパイ活動
B. データの流出
C. 金銭的利益
D. 脅迫

正解: **A** (コメントを発表する)
When an insider steals classified defense information and passes it to a hostile organization, their primary motivation is intelligence gathering on behalf of that organization - classic espionage.

質問: **347**
アナリストが、システムアカウントを使用せずにインターネットに公開されているウェブサーバーに対して脆弱性スキャンを実行しています。最もよく実行されるのは次のうちどれですか？
A. システム列挙
B. 権限昇格
C. パッシブスキャン
D. 非認証スキャン
E. パケットキャプチャ
正解: **D** (コメントを発表する)

質問: **348**
セキュリティアナリストがアプリケーションのソースコードをレビューし、設定ミスや脆弱性を特定しようとしています。このレビューに最も適した分析は次のうちどれですか？
A. ダイナミック
B. 静的
C. ギャップ
D. 影響
正解: (正解を表示します)
Reviewing the source code of an application to identify misconfigurations and vulnerabilities is best described as static analysis. Static analysis involves examining the code without executing the program. It focuses on finding potential security issues, coding errors, and vulnerabilities by analyzing the code itself.
Static analysis: Analyzes the source code or compiled code for vulnerabilities without executing the program.
Dynamic analysis: Involves testing and evaluating the program while it is running to identify vulnerabilities.
Gap analysis: Identifies differences between the current state and desired state, often used for compliance or process improvement.
Impact analysis: Assesses the potential effects of changes in a system or process.

質問: **349**
アーキテクトから、外部の JSON リクエストを使用してデータ転送速度を上げたいという要望があります。
現在、組織ではデータファイルの転送にSFTPを使用しています。要件を満たす可能性が高いのは次のうちどれですか？
A. ウェブサイトホスト型ソリューション
B. クラウド共有ストレージ
C. 安全な電子メールソリューション
D. APIを使用したマイクロサービス
正解: **(正解を表示します)**
By using APIs will allow for increased speed of data transfer compared to file based transfer methods liker SFTP.

質問: **350**
セキュリティ管理者は、基本的な脅威を特定し、封じ込めるために必要な手順の数を減らしたいと考えています。この目標を達成するために役立つのは次のどれですか。
A. 飛翔
B. DMARC
C. NIDS
D. SIEM
正解: **A (コメントを発表する)**

質問: **351**
セキュリティ アナリストは、従業員の会社のラップトップから送信される悪意のあるネットワーク トラフィックの可能性に関する SIEM のアラートを確認しています。セキュリティ アナリストは、調査を継続するには、マシンで実行されている実行可能ファイルに関する追加データが必要であると判断しました。
アナリストは、次のログのうちどれをデータ ソースとして使用する必要がありますか?
A. アプリケーション
B. IPS/IDS
C. ネットワーク
D. エンドポイント
正解: **(正解を表示します)**
Endpoint logs are the most suitable data source for gathering additional information about the executable running on the employee's corporate laptop. These logs contain detailed information about processes, executables, and activities occurring on the endpoint, enabling the security analyst to understand the behavior of the executable and its potential impact on the system and network.

質問: **352**

ある企業は、複数のアカウント乗っ取り事件を受けて、ユーザーログインを強制するオプションを検討しています。この解決策には、以下の条件を満たす必要があります。
- 従業員がリモートワークや指定されたオフィスから勤務できるようにする
世界。
- シームレスなログインエクスペリエンスを提供します。
- 必要な機器の量を制限します。
これらの条件を最もよく満たすのは次のどれですか?
A. 信頼できるデバイス
B. ジオタグ
C. スマートカード
D. 時間ベースのログイン
正解**: A (**コメントを発表する**)**
Trusted devices allow users to log in seamlessly from devices that are already recognized and trusted by the system. It supports remove and global access as the device does not need to be in a specific location or equipped with extra hardware. It minimizes the need for additional equipment and provides for a streamlined login experience.

質問**: 353**
ある企業が、インフラストラクチャをオフプレミス ソリューションに移行するための小額の助成金を受け取りました。最初に検討すべきは次のうちどれですか。
A. クラウドプロバイダーのセキュリティ
B. 実装コスト
C. エンジニアの能力
D. アーキテクチャのセキュリティ
正解**: (**正解を表示します**)**
Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud infrastructure.

質問**: 354**
企業がすべての COPE デバイスに MDM を展開する際に対処している課題は次のどれですか。
A. マルウェアの発生
B. フィッシング攻撃
C. サポートされていないアプリケーション

D. データマスキング
正解: **C** (コメントを発表する)
Mobile Device Management (MDM) on Corporate-Owned, Personally Enabled (COPE) devices enforces application control policies, helping prevent the installation and use of unsupported or unauthorized applications.

質問: **355**
インシデントをクローズする前に、インシデントが発生した理由を特定するために使用されるアクティビティは次のどれですか。
A. 根本原因分析
B. 検出
C. 電子情報開示
D. 学んだ教訓
正解: **A** (コメントを発表する)
Root cause analysis is the process of identifying the fundamental reason an incident occurred, ensuring that underlying issues are addressed before the incident is closed.

質問: **356**
IoT 管理にクラウドベースのプラットフォームを使用する場合、次のセキュリティ対策のどれが必要ですか?
A. 暗号化された接続
B. フェデレーションID
C. ファイアウォール
D. シングルサインオン
正解: (正解を表示します)
IOT devices often transmit sensitive data over networks and encryption ensures that this data is securely transmitted and protected from interception or tampering.

質問: **357**
ランサムウェア攻撃を利用して金銭的利益を得ようとする可能性が最も高い脅威アクターは次のうちどれですか?
A. 組織犯罪
B. 内部脅威
C. 国民国家
D. ハクティビスト
正解: (正解を表示します)
Organized crime groups are primarily motivated by financial gain. Ransomware attacks are a popular tool for these groups because they can encrypt a victim's data and demand a ransom payment (often in cryptocurrency) to restore access. This form of attack can yield a high financial return if victims choose to pay.

質問: **358**
脱獄を防止するために MDM ソリューションを使用する理由を説明しているのは次のうちどれですか。
A. 互換性のないファームウェアアップデートからサポート終了デバイスを保護する
B. VMエスケープによるハイパーバイザー攻撃を回避する
C. アプリケーション層でのバッファオーバーフローを排除する
D. ユーザーがモバイルデバイスのOSを変更できないようにするため
正解: **D (**コメントを発表する**)**
An MDM solution can enforce device policies that block attempts to modify or replace the mobile OS, preventing users from jailbreaking their devices.

質問: **359**
大規模オフィス ネットワークにインストールされた NAS のゼロデイ脆弱性の影響を軽減するのに役立つのは次のうちどれですか。
A. 暗号化
B. パッチ適用
C. セグメンテーション
D. フィルタリング
正解: **(**正解を表示します**)**
Segmentation isolates the NAS from the broader network, limiting an attacker's ability to exploit the zero-day vulnerability and reducing the potential impact on other systems.

質問: **360**
ハードウェアとインターネット アクセスを含む低コストのスタンバイ サイトを展開するための最適なソリューションは次のどれですか。
A. コールドサイト
B. ホットサイト
C. 回復サイト
D. 温かいサイト
正解: **(**正解を表示します**)**

質問: **361**
小売業者が PCI DSS に準拠していない場合、小売チェーンが顧客から受ける可能性のある結果は次のうちどれですか?
A. 制裁
B. 契約上の影響
C. 罰金
D. 評判の失墜
正解: **(**正解を表示します**)**

質問: **362**
組織がデータ プライバシー プログラムを確立および維持する際に評価する上で最も重要な考慮事項は次のどれですか。
A. データプライバシー担当者の報告体制
B. データ主体のアクセス要求プロセス
C. コントローラーまたはプロセッサーとしての役割
D. 会社の所在地
正解: (正解を表示します)
This is one of the most important considerations because it involves how individuals can access, correct or delete their personal data as required by data protection regulations such as GDPR.

質問: **363**
エンドユーザーのデバイスを強化するための最適な方法はどれですか? (2 つ選択してください。)
A. フルディスク暗号化
B. グループレベルの権限
C. アカウントロックアウト
D. エンドポイント保護
E. プロキシサーバー
F. セグメンテーション
正解: (正解を表示します)
Full disk encryption ensures that all data on the device remains confidential if the device is lost or stolen. Endpoint protection (antivirus/EDR) continuously defends against malware, exploits, and other active threats, directly hardening the device against attacks.

質問: **364**
管理者は、特定のアドレスで送受信されるすべてのメールが変更不可能な形式で保存されていることを確認する必要があります。このフォレンジックの概念を最もよく表しているのは次のうちどれですか？
A. 電子情報開示
B. 取得
C. 法的保留
D. 保管の連鎖
正解: (正解を表示します)
Acquisition refers to the process of capturing and preserving digital evidence in a forensically

sound, non-alterable format (e.g., bit-for-bit imaging or write-once storage), ensuring the integrity of the emails for later analysis.

質問: **365**
ハッカーは、ユーザーが疑わしいリンクをクリックしたことによるフィッシング攻撃を通じてシステムにアクセスしました。このリンクによって、数週間にわたって潜伏していたランサムウェアがネットワーク全体に横展開されました。次のどれが拡散を緩和したでしょうか。
A. IPS
B. IDS
C. WAF
D. UAT
正解: **(**正解を表示します**)**
IPS stands for intrusion prevention system, which is a network security device that monitors and blocks malicious traffic in real time. IPS is different from IDS, which only detects and alerts on malicious traffic, but does not block it. IPS would have mitigated the spread of ransomware by preventing the hacker from accessing the system via the phishing link, or by stopping the ransomware from communicating with its command and control server or encrypting the files.

質問: **366**
次のセキュリティ概念のうち、RADIUS サーバーのインストールによって実現されるものはどれですか。
A. CIA
B. AAA
C. ACL
D. PEM
正解: **B (**コメントを発表する**)**
The installation of a RADIUS server (Remote Authentication Dial-In User Service) is primarily associated with the security concept of AAA, which stands for Authentication, Authorization, and Accounting. RADIUS servers are used to manage user credentials and permissions centrally, ensuring that only authenticated and authorized users can access network resources, and tracking user activity for accounting purposes.
Authentication: Verifies the identity of a user or device. When a user tries to access a network, the RADIUS server checks their credentials (username and password) against a database.
Authorization: Determines what an authenticated user is allowed to do. After authentication, the RADIUS server grants permissions based on predefined policies.
Accounting: Tracks the consumption of network resources by users. This involves logging session details such as the duration of connections and the amount of data transferred.

質問: **367**
ソフトウェアエンジニアリングマネージャーは、コードを本番環境にリリースする前に、セキュリティ上の脆弱性がないかコードをスキャンしたいと考えています。マネージャーは、以下のど

の種類の分析を選択すべきでしょうか。
A. 静的
B. 脅威
C. パケット
D. ダイナミック
E. パッケージ
正解: **(**正解を表示します**)**
Static analysis inspects source code at rest, prior to execution, to identify security vulnerabilities, coding errors, and insecure patterns before the software is deployed.

質問: **368**
次のベスト プラクティスのうち、可用性を確保し、ビジネスへの影響を最小限に抑えるために、管理者が運用システムに変更を加えるための一定期間を与えるものはどれですか。
A. 影響分析
B. 予定されたダウンタイム
C. バックアウト計画
D. 変更管理委員会
正解: **B (**コメントを発表する**)**
Scheduled downtime is a planned period of time when a system or service is unavailable for maintenance, updates, upgrades, or other changes. Scheduled downtime gives administrators a set period to perform changes to an operational system without disrupting the normal business operations or affecting the availability of the system or service. Scheduled downtime also allows administrators to inform the users and stakeholders about the expected duration and impact of the changes.

質問: **369**
組織のリスク管理プログラムの監査を実施する際に、内部監査人が最初に確認する必要があるのは次のうちどれですか?
A. ポリシーと手順
B. 資産管理
C. 脆弱性評価
D. ビジネス影響分析
正解: **(**正解を表示します**)**
When conducting an audit of an organization's risk management program, the internal auditor should first review the policies and procedures. These documents form the foundation of the risk management program by outlining the organization's approach, goals, roles, responsibilities, and processes for managing risks.

質問: **370**
企業が新しく購入したデバイスを消去し、オペレーティング システムとアプリケーションを含む独自のイメージをインストール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. 新しいオペレーティングシステムをインストールすると、機器が徹底的にテストされます
B. 不要なアプリケーションを削除すると、システムの攻撃対象領域が縮小されます。
C. システムを再イメージ化すると、コンピュータイメージの更新されたベースラインが作成されます。
D. デバイスをワイプすることで、企業はそのパフォーマンスを評価できる
正解: **(**正解を表示します**)**
Removing the vendor's default software and installing a clean company image eliminates unnecessary applications and services, reducing the overall attack surface and improving security.

質問: **371**
サポートが終了したソフトウェアを実行しているアプリケーション サーバーをネットワークの脅威から保護するための最も効果的な方法はどれですか?
A. エアギャップ
B. バリケード
C. ポートセキュリティ
D. スクリーンサブネット
正解: **(**正解を表示します**)**
One of the most effective ways to protect an application server is to use a screened subnet. A screened subnet is a network segment that is isolated from both the internet and the internal network by two firewalls. The application server is placed in the screened subnet, also known as the demilitarized zone (DMZ), and only the necessary ports are opened for communication. This way, the application server is shielded from external attacks and internal breaches, and the impact of a compromise is minimized.

質問: **372**
ある組織で、コマンド アンド コントロール サーバーに関連するサイバーセキュリティ インシデントが発生しました。
影響を受けたホストを特定するために分析する必要があるログは次のどれですか? (2 つ選択してください。)
A. アプリケーション
B. 認証
C. DHCP
D. ネットワーク
E. ファイアウォール
F. データベース
正解: **(**正解を表示します**)**
Network logs (Option D): These logs can help identify network connections to the command-and-control server and provide information about source IP addresses (the impacted host) and destination IP addresses (the command-and-control server).
Firewall logs (Option E): Firewall logs also track network traffic and can provide valuable

information about source and destination IP addresses, helping identify the impacted host and its communication with the command-and-control server.

質問: **373**
ある企業は、従業員がモバイル デバイスのオペレーティング システムを変更できないという条項を AUP に追加しています。組織が対処しようとしている脆弱性は次のどれですか。
A. クロスサイトスクリプティング
B. バッファオーバーフロー
C. 脱獄
D. サイドローディング
正解: **C (**コメントを発表する**)**
Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network.

質問: **374**
新しい企業ポリシーでは、すべてのスタッフが会社のリソースにアクセスする際に多要素認証を使用することが義務付けられています。
この形式の ID およびアクセス管理を設定するために利用できるのは次のどれですか? (2 つ選択してください)
A. 認証トークン
B. SAML
C. パスワード保管
D. LDAP
E. 最小権限
F. 生体認証
正解: **(**正解を表示します**)**

質問: **375**
ユーザーが電子メールを確認している間に、ホストに接続された外付けハードドライブからマルウェアがホストに感染します。マルウェアは、ブラウザに保存されているユーザーの資格情報をすべて盗みます。この状況が再発しないようにするには、ユーザーは次のトレーニング トピックのどれを確認する必要がありますか?
A. 運用セキュリティ
B. リムーバブルメディアとケーブル
C. パスワード管理
D. ソーシャルエンジニアリング

正解: (正解を表示します)
This scenario highlights the need for training on the secure use of removable media. Users should learn to avoid using untrusted external storage devices to prevent malware infections.

質問: **376**
ある組織は、常時可用性が求められる顧客アプリケーションとデータをホストする単一の仮想環境を構築しています。この環境をホストするデータセンターは、発電機とISPサービスを提供します。この組織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. NICチーミング
B. クラウドバックアップ
C. ロードバランサアプライアンス
D. UPS
正解: (正解を表示します)
While NIC teaming, cloud backups, and load balancer appliances are all important for different aspects of an IT infrastructure, they do not directly address the need for continuous power availability, which is the primary concern in this scenario. UPS, in combination with backup generators and ISP services, helps ensure that the data center remains operational even during power-related issues.

質問: **377**
セキュリティアナリストは、エンドポイント保護ソフトウェアによって生成されたアラートを調査しています。アナリストは、このイベントは従業員がファイルのダウンロードを試みた際に発生した誤検知であると判断しました。ダウンロードがブロックされた理由として最も可能性が高いのは次のうちどれですか？
A. エンドポイント保護ソフトウェアの設定ミス
B. ファイルにゼロデイ脆弱性がある
C. エンドポイント保護ベンダーに対するサプライチェーン攻撃
D. ファイルの権限が正しくありません
正解: (正解を表示します)
The most likely reason the download was blocked, resulting in a false positive, is a misconfiguration in the endpoint protection software. False positives occur when legitimate actions are incorrectly identified as threats due to incorrect settings or overly aggressive rules in the security software.

Misconfiguration in the endpoint protection software: Common cause of false positives, where legitimate activities are flagged incorrectly due to improper settings.
Zero-day vulnerability: Refers to previously unknown vulnerabilities, which are less likely to be associated with a false positive.
Supply chain attack: Involves compromising the software supply chain, which is a broader and more severe issue than a simple download being blocked.
Incorrect file permissions: Would prevent access to files but not typically cause an alert in endpoint protection software.

質問: **378**
企業が HIPS を導入して実装しているセキュリティ制御は次のどれですか?
(2つ選択してください。)
A. ディレクティブ
B. 予防
C. 物理
D. 修正
E. 補償
F. 探偵
正解: **B,F (**コメントを発表する**)**
HIPS (Host-based Intrusion Prevention System) is a preventive control because it actively blocks or prevents malicious activities on a host.
It is also a detective control, as it monitors and detects suspicious activities or policy violations on the host system.

質問: **379**
企業は、セキュリティ境界を通過するトラフィックを最小限に抑えながら、内部リソースへの管理アクセスを提供する必要があります。次の方法のうち、最も安全なのはどれですか。
A. 要塞ホストの実装
B. 境界ネットワークの展開
C. WAFのインストール
D. シングルサインオンの活用
正解: **A (**コメントを発表する**)**
Implementing a bastion host provides a highly secure method for administrative access to internal resources while minimizing traffic through the security boundary. It serves as a single entry point for remote administrative access, enforcing strong authentication and access controls before allowing access to internal systems.

質問: **380**
セキュリティアナリストは、大量の従業員の認証情報が盗まれ、ダークウェブで販売されていることを発見しました。アナリストは調査を行い、一部の時間給従業員の認証情報が侵害されたものの、正社員の認証情報は影響を受けていないことを発見しました。

ほとんどの従業員は、建物内にいる間に、ネットワークに接続されたキオスク端末を使用して出退勤を記録していました。しかし、帰宅後に退勤記録を取った従業員もいました。認証情報が盗まれたのは、建物内にいる間に出勤・退勤を記録した従業員のみでした。各キオスクは異なるフロアに設置されており、業務機能ごとに環境をセグメント化しているため、複数のルーターが設置されています。
時間給従業員は、acmetimekeeping.com という Web サイトを使用して出勤と退勤を記録する必要があります。このウェブサイトはインターネットからアクセスできます。この侵害の原因として最も可能性が高いのは次のうちどれですか？
A. 時刻管理ウェブサイトに対してブルートフォース攻撃が行われ、一般的なパスワードがスキャンされました。
B. 悪意のある人物が、サイト上のパッチ未適用の脆弱性を利用して悪意のあるコードで時間管理 Web サイトを侵害し、資格情報を盗みました。
C. 内部 DNS サーバーが汚染され、acmetimkeeping.com を悪意のあるドメインにリダイレクトしていました。悪意のあるドメインは資格情報を傍受し、それを実際のサイトに渡していました。
D. ARP ポイズニングが建物内のマシンに影響を与え、キオスクが送信されたすべての資格情報のコピーをマシンに送信しました。
正解: **(**正解を表示します**)**
The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.

質問: **381**
大企業の顧客が、その企業に勤めていると主張する人物から電話を受け、顧客のクレジットカード情報を尋ねられます。顧客は、発信者番号が企業の代表電話番号と同じであることに気づきました。次のどの攻撃が顧客を最も狙う攻撃でしょうか?
A. 捕鯨
B. フィッシング
C. スミッシング
D. ヴィッシング
正解: **(**正解を表示します**)**

質問: **382**
データベース ログ ファイル内のクレジットカード情報を隠すために使用されるのは次のうちどれですか。
A. トークン化
B. マスキング
C. ハッシュ
D. 難読化

正解: **B** (コメントを発表する)
Masking involves altering the credit card information in such a way that it is not easily readable or identifiable while still retaining some format or structure for processing or display purposes. This is particularly useful for ensuring sensitive data is protected in log files or other records.

質問: **383**
レガシー デバイスが廃止され、更新やパッチを受信しなくなりました。このシナリオを説明するのは次のどれですか。
A. 営業終了
B. テスト終了
C. サポート終了
D. 寿命の終わり
正解: **D** (コメントを発表する)
When a legacy device is no longer receiving updates or patches, it is considered to be at the end of life (EOL). This means the manufacturer has ceased support for the device, and it will no longer receive updates, security patches, or technical assistance. EOL devices pose security risks and are often decommissioned or replaced.
End of support may seem similar but typically refers to the cessation of technical support, whereas EOL means the device is fully retired.
End of business and End of testing do not apply in this context.

質問: **384**
セキュリティ マネージャーは、さまざまな種類のセキュリティ インシデントに対応するために使用する新しいドキュメントを作成しました。マネージャーが次に取るべきステップは次のどれですか。
A. 最大データ保持ポリシーを設定します。
B. ドキュメントをエアギャップネットワーク上に安全に保存します。
C. ドキュメントのデータ分類ポリシーを確認します。
D. チームで卓上演習を実施します。
正解: **D** (コメントを発表する)
A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents.

質問: **385**
集中システム内の複数のソースからシステム、アプリケーション、およびネットワーク ログを収集するセキュリティ警告および監視ツールについて説明しているものはどれですか。
A. SIEM
B. DLP

C. IDS
D. SNMP
正解: **(**正解を表示します**)**
SIEM stands for Security Information and Event Management. It is a security alerting and monitoring tool that collects system, application, and network logs from multiple sources in a centralized system. SIEM can analyze the collected data, correlate events, generate alerts, and provide reports and dashboards. SIEM can also integrate with other security tools and support compliance requirements. SIEM helps organizations to detect and respond to cyber threats, improve security posture, and reduce operational costs.

質問: **386**
人事ファイル共有の権限が最小権限の原則に従うべき最も適切な理由は、次のセキュリティ概念のうちどれですか。
A. 誠実さ
B. 可用性
C. 機密性
D. 否認防止
正解: **(**正解を表示します**)**
Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure. The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data. Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare. Integrity, availability, and non-repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems.

質問: **387**
クライアントは、サービス プロバイダーがホストするセキュリティ サービスに対して、少なくとも 99.99% の稼働率を要求します。
次の文書のうち、サービス プロバイダーがクライアントに返す必要がある情報が含まれているのはどれですか。
A. モア

B. 種をまく
C. 覚書
D. SLA
正解: **D** (コメントを発表する)
A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does.

質問: **388**
企業にはリカバリ サイトが必要ですが、即時のフェイルオーバーは必要ありません。また、企業は停止からの回復に必要な作業負荷を軽減したいと考えています。次のリカバリ サイトのうち、最適なオプションはどれですか。
A. ホット
B. 寒い
C. 暖かい
D. 地理的に分散している
正解: **C** (コメントを発表する)
A warm site is the best option for a business that does not require immediate failover but wants to reduce the workload required for recovery. A warm site has some pre-installed equipment and data, allowing for quicker recovery than a cold site, but it still requires some setup before becoming fully operational.
* Hot sites provide immediate failover but are more expensive and require constant maintenance.
* Cold sites require significant time and effort to get up and running after an outage.
* Geographically dispersed sites refer to a specific location strategy rather than the readiness of the recovery site.

質問: **389**
ソフトウェアエンジニアは新しいビジネスアプリケーションを開発しており、コンパイルしてテストに送る前に、エラーやセキュリティ上の欠陥がないか確認する必要があります。エンジニアはこのタスクを完了するために、次のうちどれを使用すべきでしょうか。
A. 脆弱性スキャナー
B. 静的コード解析
C. 入力検証
D. サンドボックステスト
正解: (正解を表示します)
Static code analysis examines source code before compilation to identify errors and security

weaknesses early in the development process.

質問: **390**
次の契約のうち、応答時間、エスカレーション、およびパフォーマンス メトリックを定義しているものはどれですか。
A. BPA
B. MOA
C. NDA
D. SLA
正解: **(**正解を表示します**)**
An SLA or Service Level Agreement is a formal contract that defines performance standards, including response times, escalation procedures, uptime guarantees, and other service-related metrics.

質問: **391**
攻撃者は、人気のあるファイル共有ウェブサイトに似た新しいドメイン名を作成しました。次のどの脅威ベクトルが利用されていますか？
A. 水飲み場攻撃
B. ブランドのなりすまし
C. フィッシング
D. タイプミススクワッティング
正解: **(**正解を表示します**)**
Typosquatting involves registering domain names that are visually or typographically similar to legitimate sites to trick users into visiting the malicious site, matching the scenario described.

質問: **392**
経理担当者が最近、会社が承認していないソフトウェアを使用しました。これは以下のどのリスクに該当すると考えられますか？
A. 未熟な攻撃者
B. ハクティビスト
C. シャドーIT
D. サプライチェーン
正解: **C (**コメントを発表する**)**

The use of unauthorized software by an internal employee is a classic example of Shadow IT, where unsanctioned applications introduce unvetted security and compliance risks.

質問: **393**
データベースに保存されている機密データを最も効果的に保護する戦略は次のどれですか?
A. ハッシュ
B. マスキング
C. トークン化
D. 難読化
正解: **(**正解を表示します**)**
Tokenization replaces sensitive data with non-sensitive, unique tokens while storing the actual data securely in a separate location, effectively protecting data at rest in a database.

質問: **394**
ある従業員が、個人的な使用目的で会社のシステムから個人情報(PII)データを収集することにしました。従業員は、データを単一の暗号化ファイルに圧縮し、個人用メールアドレスに送信しました。セキュリティ部門は、この不正使用の試みに気づき、添付ファイルが社内環境から外部に流出するのをブロックしました。このような問題の発生を減らすために、従業員へのトレーニングとして最も効果的なものはどれですか？(2つ選択してください。)
A. プライバシー法
B. ソーシャルエンジニアリング
C. リスク管理
D. 企業コンプライアンス
E. フィッシング
F. リモートワーク
正解: **(**正解を表示します**)**
Privacy legislation - Teaching employees the legal obligations for handling PII (e.g., GDPR, HIPAA) makes them aware that personal use/transfer is prohibited and punishable.
Company compliance - Training on internal policies and acceptable-use rules reinforces exactly what the organization allows or forbids with company data, reducing intentional misuse.

質問: **395**
ある企業のウイルス対策ソリューションはマルウェアのブロックには効果的ですが、誤検知が頻繁に発生します。セキュリティチームは調査に多大な時間を費やしましたが、根本原因を特定できません。同社はヒューリスティックな解決策を探しています。ウイルス対策ソリューションに代わるべきものは次のうちどれでしょうか？
A. SIEM
B. EDR
C. DLP
D. IDS
正解: **(**正解を表示します**)**
EDR (Endpoint Detection and Response) uses advanced heuristic and behavioral analysis to

detect, investigate, and respond to threats, reducing false positives and providing deeper insight than traditional antivirus.

質問: **396**
低電圧イベントに対する保護としてデータセンターに導入できるのは次のどれですか?
A. リソース管理
B. ロードバランサー
C. サージプロテクター
D. 無停電電源装置
正解: **D (**コメントを発表する**)**
A UPS provides battery-backed power and voltage regulation, protecting equipment from undervoltage (brownout) conditions by supplying stable power until normal levels are restored or a generator comes online. Surge protectors, by contrast, guard against overvoltage, and the other options don't address voltage dips.

質問: **397**
次のインシデント対応活動のうち、証拠が適切に渡されることを保証するものはどれですか?
A. 電子証拠開示
B. 保管の連鎖
C. 法的保留
D. 保存
正解: **B (**コメントを発表する**)**
Chain of custody is the process of documenting and preserving the integrity of evidence collected during an incident response. It involves recording the details of each person who handled the evidence, the time and date of each transfer, and the location where the evidence was stored. Chain of custody ensures that the evidence is admissible in legal proceedings and can be traced back to its source. E-discovery, legal hold, and preservation are related concepts, but they do not ensure evidence is properly handled.

質問: **398**
内部監査チームは、ソフトウェアアプリケーションが外部報告要件の対象外になったと判断しました。以下のどれが、そのアプリケーションがもはや適用されないことを裏付けるでしょうか?
A. データのインベントリと保持
B. 忘れられる権利
C. 十分な注意と十分な努力
D. 承認と証明
正解: **(**正解を表示します**)**

質問: **399**
ゼロデイエクスプロイトに関連する攻撃に関するアラートが発生しました。アナリストは、エクスプロイトのリスクを軽減するために、ネットワークに要塞ホストを設置しました。アナリスト

は、以下のどの種類の制御を実施していますか？
A. 運用中
B. 探偵
C. 補償
D. 物理
正解: **C** (コメントを発表する)

質問: **400**
最高経営責任者(CEO)は、セキュリティツール、意識向上トレーニング、SOC人材への投資を検証するため、社内ITチームを介入させずにベンダーに侵入テストを実施するよう依頼しました。以下の侵入テスト手法のうち、最もよく使用されていると思われるものはどれですか？
A. 不明
B. 既知
C. 統合
D. 統合
正解: (正解を表示します)
An "unknown" (black-box) test gives the testers no prior information or coordination with internal teams, mimicking an external attacker and validating defenses without internal assistance.

質問: **401**
ある組織が顧客に独自のソフトウェアを輸出する準備をしています。知的財産の損失を防ぐ最善の方法は次のうちどれでしょうか？
A. コード署名
B. 難読化
C. トークン化
D. ブロックチェーン
正解: (正解を表示します)

質問: **402**
セキュリティ エンジニアは、環境内でシグネチャベースの攻撃をブロックするために IPS をインストールしています。このタスクを最も効果的に達成できるモードは次のうちどれですか。
A. モニター
B. センサー
C. 監査
D. アクティブ
正解: (正解を表示します)
To block signature-based attacks, the Intrusion Prevention System (IPS) must be in active mode. In this mode, the IPS can actively monitor and block malicious traffic in real time based on predefined signatures. This is the best mode to prevent known attack types from reaching the internal network.
Monitor mode and sensor mode are typically passive, meaning they only observe and log traffic

without actively blocking it.
Audit mode is used for review purposes and does not actively block traffic.

質問: **403**
ある企業は、サーバーの交換や追加が必要になった場合に最小限の労力で済むソリューションでアプリケーションの可用性を向上したいと考えています。これらの目的を達成するための最適なソリューションは次のどれでしょうか。
A. 負荷分散
B. フォールトトレランス
C. プロキシサーバー
D. レプリケーション
正解: **(正解を表示します)**
Load balancing improves application availability by distributing traffic across multiple servers. If one server fails, traffic is automatically routed to other available servers with minimal intervention.

質問: **404**
ある企業がベンダーと協力して侵入テストを実施しています。次のどれに、契約を完了するために必要な時間数の見積もりが含まれていますか?
A. 種をまく
B. BPA
C. サービスレベル保証
D. 秘密保持契約
正解: **(正解を表示します)**
A statement of work (SOW) is a document that defines the scope, objectives, deliverables, timeline, and costs of a project or service. It typically includes an estimate of the number of hours required to complete the engagement, as well as the roles and responsibilities of the parties involved. A SOW is often used for penetration testing projects to ensure that both the client and the vendor have a clear and mutual understanding of what is expected and how the work will be performed. A business partnership agreement (BPA), a service level agreement (SLA), and a non-disclosure agreement (NDA) are different types of contracts that may be related to a penetration testing project, but they do not include an estimate of the number of hours required to complete the engagement.

質問: **405**
新入社員が初めてメール システムにログインすると、人事部からオンボーディングに関するメッセージが届いていることに気付きます。社員はメール内のいくつかのリンクにマウスを移動し、そのリンクが会社に関連するリンクと一致していないことに気付きます。次の攻撃ベクトルのうち、最もよく使用されるのはどれですか。
A. ビジネスメール
B. ソーシャルエンジニアリング
C. 安全でないネットワーク

D. デフォルトの資格情報
正解: **(**正解を表示します**)**
The employee notices that the links in the email do not correspond to the company's official URLs, indicating that this is likely a social engineering attack. Social engineering involves manipulating individuals into divulging confidential information or performing actions that may compromise security. Phishing emails, like the one described, often contain fraudulent links to trick the recipient into providing sensitive information or downloading malware.
Business email refers to business email compromise (BEC), which typically involves impersonating a high-level executive to defraud the company.
Unsecured network is unrelated to the email content.
Default credentials do not apply here, as the issue is with suspicious links, not login credentials.

質問: **406**
データが変更されていないことを確認するために実行されるアルゴリズムは次のどれですか?
A. ハッシュ
B. コードチェック
C. 暗号化
D. チェックサム
正解: **(**正解を表示します**)**
A hash is an algorithm used to verify data integrity by generating a fixed-size string of characters from input data. If even a single bit of the input data changes, the hash value will change, allowing users to detect any modification to the data. Hashing algorithms like SHA-256 and MD5 are commonly used to ensure data has not been altered.

質問: **407**
エンジニアは、スクリプトがリリース前に変更されていないことを確認する必要があります。この機能を提供する最も優れた方法は次のうちどれですか？
A. 難読化
B. 暗号化
C. ハッシュ
D. マスキング
正解: **C (**コメントを発表する**)**

質問: **408**
請負業者は、購入されたすべての新規サーバーのマザーボードを目視検査し、改ざんの有無を確認することが義務付けられています。請負業者が軽減しようとしているリスクは次のどれですか？
A. ファームウェア障害
B. サプライチェーン
C. 埋め込まれたルートキット
D. RFIDキーロガー
正解: **(**正解を表示します**)**

質問: **409**
残酷な情報セキュリティ責任者 (CISO) が、セキュリティ アナリストに、99% の稼働率 SLA を持つ運用 VM に OS アップデートをインストールするように依頼しました。CISO は、インストールをできるだけ早く行う必要があるとアナリストに伝えました。セキュリティ アナリストが最初に実行する必要があるのは次のうちどのアクション コースですか。
A. サーバーにログインし、VM のヘルス チェックを実行します。
B. パッチをすぐにインストールします。
C. バックアップ サービスが実行されていることを確認します。
D. VM のスナップショットを作成します。
正解: **D (**コメントを発表する**)**
Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.

質問: **410**
最高セキュリティ責任者 (CSO) が、インターネットから単一のVLANへの受信SMBおよびRDPを許可するリクエストを承認しました。このアクティビティの最も可能性の高い説明はどれですか？
A. 会社は新しいファイル共有サイトを構築しました。
B. 組織は侵入テストの準備をしています。
C. セキュリティ チームは SASE プラットフォームと統合しています。
D. セキュリティ チームがハニーネットを作成しました。
正解: **(**正解を表示します**)**
Exposing high-value targets like SMB and RDP to the internet on an isolated VLAN is characteristic of a honeynet, allowing the security team to lure and observe attackers while keeping production systems protected.

質問: **411**

セキュリティ管理者がファイル共有を設定しています。管理者はデフォルトの権限を削除し、職務上ファイル共有にアクセスする必要があるユーザーのみに権限を追加しました。管理者がこれらの操作を実行した理由として最も適切なのは次のうちどれですか。
A. 暗号化標準準拠
B. データ複製要件
C. 最小権限
D. アクセス制御監視
正解**: C (**コメントを発表する**)**
The security administrator's actions of removing default permissions and adding permissions only for users who need access as part of their job duties best describe the principle of least privilege. This principle ensures that users are granted the minimum necessary access to perform their job functions, reducing the risk of unauthorized access or data breaches.
Least privilege: Limits access rights for users to the bare minimum necessary for their job duties, enhancing security by reducing potential attack surfaces.
Encryption standard compliance: Involves meeting encryption requirements, but it does not explain the removal and assignment of specific permissions.
Data replication requirements: Focus on duplicating data across different systems for redundancy and availability, not related to user permissions.
Access control monitoring: Involves tracking and reviewing access to resources, but the scenario is about setting permissions, not monitoring them.

質問**: 412**
データ管理ライフサイクルの次の側面のうち、地域および国際規制によって最も直接的に影響を受けるのはどれですか?
A. 破壊
B. 認定
C. 保持
D. サニタイズ
正解**: (**正解を表示します**)**
Retention policies dictate how long data must be stored to comply with local and international regulations. Non-compliance can result in legal and financial penalties.

質問**: 413**
顧客から、公開ウェブサイトからダウンロードしたソフトウェアにマルウェアが含まれているとの報告がありました。しかし、ソフトウェアを開発した会社は、納品時にソフトウェアにマルウェアが含まれていないことを否定しました。この懸念に対処するには、以下のどの方法が有効でしょうか。
A. 安全な保管
B. 静的コード解析
C. 入力検証
D. コード署名

正解: **(**正解を表示します**)**
Code signing uses digital certificates to verify the authenticity and integrity of software, ensuring it has not been tampered with after being created and delivered by the vendor.

質問: **414**
レガシー システムを使用して本番サービスを提供する場合に最も重要なセキュリティ上の懸念事項は次のどれですか。
A. 不安定性
B. ベンダーサポートの不足
C. 可用性の喪失
D. 安全でないプロトコルの使用
正解: **D (**コメントを発表する**)**
Legacy systems often utilize outdated communication protocols that lack modern security features, such as encryption. For instance, protocols like HTTP, Telnet, and early versions of SMB are commonly found in older systems and are known for their vulnerabilities. The continued use of these insecure protocols exposes organizations to significant risks, including data interception, unauthorized access, and exploitation by cyber attackers. A report by Cato Networks highlights that many enterprises still rely on such protocols, leaving their networks susceptible to threats.

質問: **415**
次のオプションのうち、データベースの RTO と RPO が最も低くなるのはどれですか?
A. ホットサイト
B. ジャーナリング
C. スナップショット
D. オンサイトバックアップ
正解: **(**正解を表示します**)**

質問: **416**
システム管理者は、外部Webサーバーが正常に機能していないという報告を受けました。管理者は、Webサーバーへのトラフィックを含む以下のファイアウォールログを確認します。

Date	Time	SourceIP	SPort	Flag	DestIP	DPort
2023-01-25	01:45:09.102	98.123.45.100	4560	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	95.123.45.101	3361	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	99.123.45.102	3662	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	89.123.45.103	5663	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	98.123.45.104	4064	SYN	100.50.20.7	443
2023-01-25	01:45:09.102	80.123.45.105	4365	SYN	100.50.20.7	443

次の攻撃のうち、どれが発生する可能性が高いでしょうか?
A. DDoS
B. HTTPS ダウングレード

C. ブルートフォース
D. ディレクトリトラバーサル
正解: **A (**コメントを発表する**)**

質問: **417**
モノリシック アーキテクチャと比較した場合のマイクロサービス アーキテクチャの利点を最もよく表しているのは次のうちどれですか (2 つ選択してください)。
A. システムの所有コストの削減
B. システムの区分化の強化
C. システムのデバッグが容易になります
D. システムのより強力な認証
E. システムのスケーラビリティの向上
F. システムの複雑さの軽減
正解: **(**正解を表示します**)**

質問: **418**
企業環境の最高情報セキュリティ責任者(CISO)は、ユーザーが既知の悪意のあるドメインにアクセスできないようにしたいと考えています。また、ネットワーク上のWebトラフィックに悪意のあるアクティビティがないか検査したいと考えています。CISOが実施すべき対策は次のうちどれですか？
A. 侵入システムを IPS モードにして、悪意のあるドメインの受信をブロックし、すべてのネットワーク セグメントで安全なプロトコル選択が確実に適用されるようにします。
B. すべての社内システムに EDR ソフトウェアを導入し、ユーザー行動分析を実行して、異常なドメインにアクセスするユーザーを検出します。
C. 会社のネーム サーバーが DNS フィルタリングを使用していることを確認し、集中型の TLS プロキシを使用してすべての HTTP および HTTPS トラフィックを検査するようにシステムを構成します。
D. 企業ネットワークのすべてのセグメントに NAC を設定し、境界で既知の悪意のあるポート番号をブロックするようにネットワーク ファイアウォールを設定します。
正解: **(**正解を表示します**)**
A DNS filter blocks lookups to known bad domains, stopping users from reaching them, and a centralized TLS (HTTPS) inspection proxy lets the organization decrypt/inspect HTTP/HTTPS traffic for malicious content before re-encrypting it outbound.

質問: **419**
コーヒーショップのオーナーは、レシート番号の入力を求めることで、インターネットへのアクセスを有料会員のみに制限したいと考えています。この要件を満たす最適な方法は次のうちどれですか？
A. WPA3
B. キャプティブポータル

C. PSK
D. IEEE 802.1X
正解**: (**正解を表示します**)**
This will allow the coffee shop to restrict internet access by redirecting users to a web page where they must enter the receipt information to gain access.

質問**: 420**
ある会社のユーザーから、新しい小売ウェブサイトの URL がギャンブルとフラグ付けされてブロックされているため、アクセスできないという報告がありました。
次のどの変更により、ユーザーはサイトにアクセスできるようになりますか?
A. HTTPS トラフィックを許可するファイアウォール ルールの作成
B. ショッピングを許可するようにIPSを設定する
C. クレジットカードデータを検出するDLPルールの調整
D. コンテンツフィルタの分類を更新しています
正解**: (**正解を表示します**)**
A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.

質問**: 421**
ある企業が、企業ネットワークから30GBのデータが流出するという重大なインシデントに見舞われました。システムデータがどこから流出し、攻撃者がデータを送信した場所を特定する最も効率的な方法は、次のうちどれですか？
A. 外部の脆弱性スキャンと自動レポートを分析して、攻撃者がリモート コードの脆弱性を悪用した可能性があるシステムを特定します。
B. エンドポイントとアプリケーションのログを分析して、ファイル共有プログラムが会社のシステムで実行されていたかどうかを確認します。
C. IPS および IDS ログを分析して、攻撃者が偵察スキャンに使用した IP アドレスを見つけます。
D. ファイアウォールとネットワーク ログを分析して、外部 IP アドレスまたはドメインへの大量の送信トラフィックを検出します。
正解**: D (**コメントを発表する**)**

質問: **422**
企業の公開ウェブサイト https://www.organization.com の IP アドレスは 166.18.75.6 です。しかし、過去1時間にわたり、SOC はサイトのホームページに誤った情報が表示されているという報告を受けています。nslookup で簡単に検索してみると、https://www.organization.com が 151.191.122.115 を指していることがわかります。以下のどれが発生しているのでしょうか？
A. DoS攻撃
B. ARPポイズニング
C. DNSスプーフィング
D. NXDOMAIN攻撃
正解: **C** (コメントを発表する)
Domain Name Server (DNS) spoofing, or DNS cache poisoning, is an attack involving manipulating DNS records to redirect users toward a fraudulent, malicious website that may resemble the user's intended destination.

質問: **423**
ある企業は、次のような方法でシステムのセキュリティを確保することを計画しています。
- ユーザーが企業のメールで機密データを送信するのを防ぐ
- 潜在的に有害なウェブサイトへのアクセスを制限する
会社が設定すべき機能は次のどれですか? (2 つ選択してください。)
A. ガードレール
B. DLPソフトウェア
C. ステートフルファイアウォール
D. ウイルス対策シグネチャ
E. ファイル整合性監視
F. DNSフィルタリング
正解: (正解を表示します)

質問: **424**
技術者が、SaaS プロバイダーによって導入およびサポートされている新しいシステム用にファイアウォールのポートを開いています。新しいシステムのリスクは次のどれですか。
A. 脆弱なソフトウェア
B. セグメント化されていないネットワーク
C. サプライチェーンベンダー

D. デフォルトの資格情報
正解: **(**正解を表示します**)**

質問: **425**
使用期限切れのハードウェアの脆弱性に関する懸念事項は次のどれですか?
A. ハードウェアの廃棄手順に従わないと、意図しないデータが漏洩する可能性があります。
B. サプライチェーンに交換用ハードウェアがない可能性があります。
C. 新しくリリースされたソフトウェアでは、従来のハードウェアでは利用できないコンピューティング リソースが必要になる場合があります。
D. ベンダーはパッチやアップデートの提供を停止する場合があります。
正解: **(**正解を表示します**)**
Once hardware reaches end of life, manufacturers typically end security support. Without new firmware/microcode patches or drivers, newly discovered vulnerabilities remain unpatched, leaving the device exposed indefinitely - this is the core security concern with EOL gear.

質問: **426**
ある組織は、サードパーティベンダーに特定のデバイスを対象とした侵入テストを実施してもらいたいと考えています。
組織はデバイスに関する基本情報を提供しています。この種の侵入テストを最もよく表すのは次のどれですか?
A. 部分的に既知の環境
B. 不明な環境
C. 統合
D. 既知の環境
正解: **(**正解を表示します**)**
A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test.

質問: **427**
ある企業はファイルストレージにクラウドベースのサーバーを使用しており、転送中のデータのセキュリティを確保したいと考えています。このタイプの通信を保護するために、企業は次のうちどれを使用すべきでしょうか?
(2つ選択してください。)
A. TLS証明書
B. WPA2暗号化
C. HTTPS
D. 仮想プライベートネットワーク
E. 暗号化キー管理
F. デジタル署名
正解: **(**正解を表示します**)**

TLS certificates:
TLS (Transport Layer Security) is the standard protocol for encrypting data in transit over networks. Certificates authenticate the server and establish a secure, encrypted channel.
HTTPS:
HTTPS is HTTP over TLS/SSL. It ensures that data sent between clients (like web browsers) and the cloud server is encrypted and protected from eavesdropping or tampering.

質問: **428**
大規模なIT運用を行う企業が、管理の強化、標準化、そして新規サーバー構築にかかる時間の短縮を目指しています。この企業の目標達成に最も適したアーキテクチャは次のうちどれでしょうか？
A. IoT
B. ICS
C. IaC
D. IaaS
正解: **(正解を表示します)**

質問: **429**
セキュリティ エンジニアがリモート アクセス VPN を構成しました。リモート アクセス VPN を使用すると、エンド ユーザーはエンドポイントにインストールされたエージェントを使用してネットワークに接続し、暗号化されたトンネルを確立できます。エンジニアが実装した可能性が高いプロトコルは次のどれですか。
A. GO
B. IPSec
C. SD-WAN
D. EAP
正解: **(正解を表示します)**

質問: **430**
次のデータ ロールのうち、リスクの特定とデータへの適切なアクセスを担当するのはどれですか。
A. 所有者
B. 管理者
C. スチュワード
D. コントローラー
正解: **A (コメントを発表する)**
The data owner is the role responsible for identifying risks to data and determining who should have access to that data. The owner has the authority to make decisions about the protection and usage of the data, including setting access controls and ensuring that appropriate security measures are in place.

質問: **431**
セキュリティ管理者は、会社のノートパソコンが盗難に遭った場合に備えて、ノートパソコン内の企業データを保護しようとしています。管理者は次のどの解決策を検討すべきでしょうか。
A. オペレーティングシステムの強化
B. ディスク暗号化
C. ブートセキュリティ
D. データ損失防止
正解: **B** (コメントを発表する)

質問: **432**
セキュリティ担当者が会社のネットワークの脆弱性評価を完了し、いくつかの脆弱性を発見しました。運用チームがそれを修正します。次に行うべきことはどれですか?
A. ネットワークを再スキャンします。
B. 監査を実施します。
C. レポートを送信します。
D. 侵入テストを開始します。
正解: (正解を表示します)

質問: **433**
アナリストは、データ プレーン内でのゼロ トラスト原則の実装を評価しています。アナリストが評価するのに最も関連性の高いのは次のどれでしょうか。
A. 保護されたゾーン
B. 主体の役割
C. 適応型アイデンティティ
D. 脅威範囲の縮小
正解: (正解を表示します)
It asks about the Data plane not the control plane, which includes implicit trust zones, systems and subjects, and policy enforcement points.

質問: **434**
攻撃者の活動や手法を入手して分析するために、最もよく使用されるのは次のどれですか?
A. レイヤー3スイッチ
B. ファイアウォール
C. ハニーポット
D. IDS
正解: **C** (コメントを発表する)

質問: **435**
ある企業は、ランサムウェア攻撃に対する補償を削除することで、年間サイバー保険のコストを削減することを決定しました。

企業がこの決定を下す際に最も使用した分析要素は次のどれでしょうか?
A. 次回
B. RTO
C. MTBF
D. ARO
正解: **(**正解を表示します**)**

質問: **436**
侵入テスト担当者は、オンサイト侵入テスト中に未使用のイーサネットポートを発見しました。その未使用ポートにデバイスを接続すると、そのマシンにIPアドレスが割り当てられていることに気づき、ローカルネットワークを列挙することができました。このような事態を今後防ぐために、管理者は次のうちどれを実施すべきでしょうか？
A. ポートセキュリティ
B. セキュリティゾーン
C. プロキシサーバー
D. トランスポート層セキュリティ
正解: **(**正解を表示します**)**

質問: **437**
ある企業は、ログイン情報を取得し、毎週レビューすることで、過剰なログイン試行や頻繁なロックアウトなどの状況を特定しています。セキュリティコンプライアンス監視を改善するために、セキュリティアナリストが推奨すべき対策は次のうちどれですか？
A. レポートに情報を確認した日付と担当者を含める
B. 異常発生時に自動アラートを追加する
C. プライバシー保護のためレポート内のユーザー名をマスクする
D. 毎週、例外がなかったという声明を求める
正解: **B (**コメントを発表する**)**

質問: **438**
推測しやすいパスワードが原因でアカウントが侵害されました。現在のパスワードポリシーでは、英数字12文字以上、大文字1文字、小文字1文字以上、パスワード履歴2件、パスワードの最小有効期間1日、最大有効期間90日が求められています。このインシデントの再発リスクを軽減するには、次のうちどれが効果的でしょうか？(2つ選択してください。)
A. パスワードの最小文字数を 14 文字に増やします。

B. パスワード ハッシュ アルゴリズムを MD5 から SHA-512 にアップグレードします。
C. パスワードの最大有効期間を 120 日に増やします。
D. パスワードの最小文字数を 10 文字に短縮します。
E. パスワードの最小有効期間を 0 日に短縮します。
F. 少なくとも 1 つの特殊文字の要件を含みます。
正解: **(**正解を表示します**)**
Since the issue is with the passwords being easy to guess, the solution would be one that addresses password complexity (and not password history or age necessarily). Increasing the minimum length of the password and introducing a special character would be the best options for this.

質問: **439**
ある組織は、2度にわたる監査に不合格となったため、政府の規制当局から罰金の支払いを命じられました。この措置の原因は次のどれですか？
A. 不適合
B. 政府の制裁
C. 契約違反
D. 交戦規則
正解: **(**正解を表示します**)**

質問: **440**
会社のハードウェア攻撃対象領域を減らすために、システム管理者は次のどれを使用する必要がありますか?
A. レプリケーション
B. 隔離
C. 集中化
D. 仮想化
正解: **(**正解を表示します**)**
Virtualization reduces a company's hardware attack surface by consolidating multiple physical systems into virtual machines (VMs) running on fewer physical servers. This minimizes the number of physical devices that need to be secured and maintained, reducing potential entry points for attackers.

質問: **441**
ビジネス継続性の机上演習を実施しているときに、セキュリティ チームは、フェイルオーバー中にジェネレータが故障した場合の潜在的な影響について懸念を抱きます。リスク管理活動に関して、チームが最も考慮する可能性が高いのは次のどれですか。
A. RPO
B. ARO
C. BIA

D. MTTR
正解: **(**正解を表示します**)**
Business Impact Analysis (BIA) is the process of identifying and evaluating the potential effects of disruptions to critical business operations. In this scenario, the concern about a generator fault during failover directly relates to understanding the impact on business operations and continuity. A BIA would help the team assess the severity of such an event and prioritize risk management activities accordingly.

質問: **442**
通知を受ける権利、アクセス権、忘れられる権利などの個人の権利について言及しているのは次のうちどれですか?
A. ISO
B. GDPR
C. NIST
D. PCI DSS
正解: **B (**コメントを発表する**)**

質問: **443**
ユーザーは https://comptiatraining.com でトレーニングを完了する必要があります。URL を手動で入力した後、アクセスした Web サイトが標準の会社の Web サイトとは明らかに異なることに気付きました。この違いの原因として最も可能性が高いのは次のどれですか。
A. タイプミススクワッティング
B. ヴィッシング
C. プリテキスティング
D. クロスサイトスクリプティング
正解: **(**正解を表示します**)**

質問: **444**
企業ネットワークの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. 有線接続にポート セキュリティを使用します。
B. ネットワーク プリンターのデフォルト パスワードを変更します。
C. サーバー上の未使用のネットワーク サービスを無効にします。
D. 訪問者用のゲスト ワイヤレス ネットワークを作成します。
正解: **B (**コメントを発表する**)**

質問: **445**
ソフトウェア開発者が新しいアプリケーションをリリースし、開発者のウェブサイトを通じてアプリケーションファイルを配布しています。ダウンロードしたファイルの整合性をユーザーが確認できるようにするために、開発者はウェブサイトに次のどれを掲載すべきでしょうか？
A. ハッシュ
B. 証明書

C. アルゴリズム
D. 塩漬け
正解**: A (**コメントを発表する**)**
To verify the integrity of downloaded files, a software developer should post hashes on the website. A hash is a fixed-length string or number generated from input data, such as a file. When users download the application files, they can generate their own hash from the downloaded files and compare it with the hash provided by the developer. If the hashes match, it confirms that the files have not been altered or corrupted during the download process.
Hashes: Ensure data integrity by allowing users to verify that the downloaded files are identical to the original ones. Common hashing algorithms include MD5, SHA-1, and SHA-256.
Certificates and Algorithms: Are more related to ensuring authenticity and securing communications rather than verifying file integrity.
Salting: Is a technique used in hashing passwords to add an additional layer of security, not for verifying file integrity.

質問**: 446**
許容されるリスクの最大許容度を説明するのは次のどれですか?
A. リスク指標
B. リスクレベル
C. リスクスコア
D. リスク閾値
正解**: D (**コメントを発表する**)**
Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk.

質問**: 447**
ある組織は、機密データを含む重要なビジネスアプリケーションを購入しました。このアプリケーションが一般的なデータ窃盗攻撃に悪用されないよう、セキュリティ対策を講じたいと考えています。この要件を満たすには、以下のどのアプローチが最も効果的でしょうか。
A. URLスキャン
B. リバースプロキシ
C. NAC
D. WAF
正解**: D (**コメントを発表する**)**

質問**: 448**
独自の制御を使用し、リモート アクセス管理が制限された状態で長年にわたって厳しい環境で機能するように設計されているのは次のどれですか。

A. ICS
B. マイクロサーバー
C. コンテナ
D. IoT
正解: **(**正解を表示します**)**
Industrial Control Systems (ICS) use proprietary controls and are built to operate reliably in harsh environments for extended periods, often with limited remote access and management capabilities.

質問: **449**
サイバー攻撃により、ある企業のITシステムは長期間にわたり運用不能となりました。同社は、業務の混乱を最小限に抑えるために、システムをどれだけ迅速に復旧させる必要があるかを測定したいと考えています。同社が使用する可能性のある指標は次のうちどれでしょうか？
A. リスク選好
B. リスク許容度
C. 平均故障間隔
D. 回復時間目標
E. 回復ポイント目標
正解: **(**正解を表示します**)**

質問: **450**
マネージャーは、最近解決されたセキュリティ インシデントに関係するさまざまな関係者と会います。
会議では、将来のインシデントへの対応を改善するために、環境の改善の可能性について話し合います。これは、以下のインシデント対応活動のうちどれに該当しますか？
A. 回復
B. 分析
C. 学んだ教訓
D. 封じ込め
正解: **C (**コメントを発表する**)**
The lessons learned phase occurs after an incident is resolved and involves reviewing the response process, identifying improvements, and implementing changes to enhance future incident handling.

質問: **451**
ネットワーク セグメンテーションによって得られる最大の利点は次のどれですか?
A. エンドツーエンドの暗号化
B. リソース使用率の低下
C. 強化されたエンドポイント保護
D. 構成の強制
E. セキュリティゾーン

正解: (正解を表示します)
By dividing a network into distinct security zones, segmentation isolates traffic flows and contains breaches, preventing attackers from moving laterally across the entire environment.

質問: **452**
セキュリティ管理者は、機密データを第三者に転送するために暗号化されていないプロトコルを使用してデータを通信するレガシー システムの問題に対処しています。暗号化されたプロトコルを使用するソフトウェア アップデートは利用できないため、補償制御が必要です。管理者が提案するのに最も適切なのは次のうちどれですか。(2 つ選択してください。)
A. トークン化
B. 暗号化のダウングレード
C. SSHトンネリング
D. セグメンテーション
E. パッチのインストール
F. データマスキング
正解: (正解を表示します)
SSH tunneling can secure the unencrypted protocol by encapsulating traffic in an encrypted tunnel. Segmentation isolates the legacy system, reducing the risk of unauthorized access.

質問: **453**
従業員が、CEOを名乗る見知らぬ番号からギフトカードの購入を依頼するテキストメッセージを受け取りました。この例に当てはまる攻撃の種類は次のうちどれですか？
A. 水飲み場
B. 偽情報
C. フィッシング
D. なりすまし
正解: (正解を表示します)
Impersonation involves an attacker pretending to be a trusted individual, such as a CEO, to trick someone into taking an action - in this case, purchasing gift cards - often seen in social engineering attacks via text or email.

有効的な**SY0-701-JPN**問題集はJPNTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-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/SY0-701-JPN-mondaishu **765**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」