CompTIA.SY0-701.v2024-11-30.q247

試験コード:	SY0-701
試験名称:	CompTIA Security+ Certification Exam
認定資格:	CompTIA
無料問題数:	247
バージョン:	v2024-11-30
アクセス数:	10691
ページビュー数:	2470
https://www.jpnpdf.com/CompTIA.SY0-701.v2024-11-30.q247-mondaishu.html	

最新問題: **1**
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
Answer: B (メーッセージを残す**)**
VPN は、パブリック ネットワークを介して 2 台以上のデバイス間に安全なトンネルを作成する仮想プライベート ネットワークです。VPN は、データの暗号化と認証を行うほか、デバイスの IP アドレスと場所を隠すことができます。ジャンプ サーバーは、ユーザーとターゲット サーバー (運用サーバーなど) の間の仲介役として機能するサーバーです。ジャンプ サーバーは、追加のセキュリティ レイヤーとアクセス制御、およびログ機能と監査機能を提供できます。ファイアウォールは、事前定義されたルールに基づいて不要なネットワーク トラフィックをフィルタリングしてブロックするデバイスまたはソフトウェアです。ファイアウォールは、内部ネットワークを外部の脅威から保護し、機密性の高いサービスとポートの露出を制限できます。セキュリティ アナリストは、運用ネットワークへのリモート デスクトップ アクセスのセキュリティを強化するために、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ことを推奨する必要があります。この方法では、リモート デスクトップ サービスはパブリック ネットワークに公開されず、VPN 資格情報を持つ承認済みユーザーのみがジャンプ サーバーにアクセスし、運用サーバーにアクセスできます。

最新問題: **2**

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
Answer: C,E (メーッセージを残す**)**
セキュリティ意識向上プログラムのトレーニング カリキュラム計画では、次の要素を考慮する必要があります。
組織が運営する業界に基づいた脅威ベクトル。これにより、従業員は組織が直面している特定のリスクと課題を理解し、サイバー攻撃から自分自身と組織を保護する方法を知ることができます。たとえば、ヘルスケア組織は、ランサムウェア、データ侵害、医療機器のハッキングなど、金融機関とは異なる脅威ベクトルに直面する可能性があります1。
トレーニング イベントの頻度と期間。これにより、従業員は学習した情報とスキルを維持し、セキュリティ環境の変化に対応できるようになります。トレーニング イベントは、主要な概念と行動を強化するのに十分な頻度で実施する必要がありますが、従業員の注意や関心を失わせるほど長すぎたり短すぎたりしてはなりません。たとえば、セキュリティ意識向上プログラムには、月刊ニュースレター、四半期ごとのウェビナー、年次ワークショップ、定期的なクイズなどが含まれます2。

最新問題**: 3**
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
Answer: (解答を表示する**)**
保存時の暗号化は、ノート PC などのデバイスに保存されているデータを、復号化キーまたはパスワードでのみアクセスできる読み取り不可能な形式に変換することで保護する戦略です。保存時の暗号化は、デバイスが物理的に侵害された場合でも、データへの不正アクセスを防止することで、盗難されたノート PC のデータ損失を防ぐことができます。保存時の暗号化は、データ保護を必要とするデータ プライバシー規制および標準に準拠するのにも役立ちます。マスキング、データ分類、およびアクセス許可の制限は、データ保護に役立つその他の戦略ですが、ノート PC に保存されているデータには十分ではないか、適用できない可能性があります。マスキングは、クレジットカード番号などの機密データ要素をランダムな文字または記号で隠す手法ですが、通常は転送中または使用中のデータに使用され、保存中のデータには使用されません。データ分類は、機密性とビジネスへの影響に基づ

いてデータにラベルを割り当てるプロセスですが、データ自体を保護するものではありません。アクセス許可の制限は、データにアクセス、変更、または削除できるユーザーを定義するルールですが、ノート PC が盗まれ、セキュリティ制御がバイパスされた場合、不正アクセスを防ぐことができない可能性があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、17-18 ページ、372-373

最新問題**: 4**
ある企業が政府向けの重要なシステムを開発しており、プロジェクト情報をファイル共有に保存しています。このデータがどのように分類される可能性が高いかを説明するのは次のうちどれですか? (2 つ選択してください)。
A. プライベート
B. 機密
C. パブリック
D. 運用中
E. 緊急
F. 制限あり
Answer: B,F (メーッセージを残す**)**
データ分類とは、データの機密性とビジネスへの影響に基づいてデータにラベルを割り当てるプロセスです。組織やセクターによってデータ分類スキームは異なりますが、一般的なスキームは次のとおりです。
公開: 害やリスクなしに誰にでも自由に開示できるデータ。非公開: 社内使用のみを目的としており、開示されると害やリスクを引き起こす可能性があるデータ。
機密: 許可された使用のみを目的としており、開示されると重大な損害やリスクを引き起こす可能性があるデータ。
制限付き: 非常に限定された使用のみを目的としており、公開されると重大な損害やリスクを引き起こす可能性があるデータ。
このシナリオでは、企業が政府向けの重要なシステムを開発しており、プロジェクト情報をファイル共有に保存しています。このデータは、公的または私的使用を意図したものではなく、公開されると国家安全保障または公共の安全に重大な損害を与える可能性があるため、機密および制限付きとして分類される可能性があります。また、政府は、暗号化、アクセス制御、監査など、このようなデータの取り扱いに関して特定の要件または規制を設けている場合もあります。

最新問題**: 5**
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
Answer: (解答を表示する**)**
フル パケット キャプチャは、ルーターやファイアウォールなどのデバイスを通過するすべてのネットワーク トラフィックを記録する手法です。パケットの完全な内容とコンテキストを提供することで、SQLi 攻撃などのネットワーク イベントの詳細な分析と調査が可能になります。フル パケット キャプチャは、SQLi 攻撃のソース、宛先、ペイロード、タイミング、およびサーバーとデータベースへの影響の特定に役立ちます。NetFlow トラフィック、ネットワーク トラフィック センサー、エンドポイントおよび OS 固有のセキュリティ ログをログに記録すると、ネットワーク アクティビティに関する情報が得られますが、パケットの完全な内容はキャプチャされないため、調査の範囲と深さが制限される可能性があります。

最新問題**: 6**
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にアクセスを拒否するように構成されています。
暗号化されていない Web サイトへのアクセスを禁止するためにアナリストが使用する必要がある検索文字列は次のどれですか。
A. 暗号化=オフ\
B. http://
C. www.*.com
D. :443
Answer: B (メーッセージを残す**)**
ウェブフィルタは、定義済みのルールやポリシーに基づいてウェブトラフィックを監視、ブロック、または許可できるデバイスまたはソフトウェアです。ウェブフィルタリングの一般的な方法の1つは、URLをスキャンして文字列を検索し、一致するものがあった場合にアクセスを拒否することです。たとえば、ウェブフィルタは 「ギャンブル」という単語を含むウェブサイトへのアクセスをブロックできます。
URL に 「ポルノ」、「マルウェア」などのキーワードが含まれていないこと。URL は、Web リソースの場所とプロトコルを識別する Uniform Resource Locator です。URL は通常、次のコンポーネントで構成されます: protocol://domain:port/path?query#fragment。プロトコルは、HTTP、HTTPS、FTP、SMTP など、Web リソースへのアクセスに使用される通信方法を指定します。ドメインは、www.google.com や www.bing.com など、Web リソースをホストする Web サーバーの名前です。ポートは、Web サーバーで実行されている特定のサービスまたはアプリケーションを識別するオプションの番号です。たとえば、HTTP の場合は 80、HTTPS の場合は 100 です。
HTTPSの場合は443。パスは、/index.htmlや

/images/logo.png。クエリは、?q=security や ?lang=en など、Web リソースの追加情報またはパラメータを含むオプションの文字列です。フラグメントは、#introduction や #summary など、Web リソースの特定の部分またはセクションを識別するオプションの文字列です。
に
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、アナリストは暗号化されていない Web トラフィックのプロトコル (HTTP) に一致する検索文字列を使用する必要があります。HTTP はハイパーテキスト転送プロトコルの略で、Web サーバーと Web ブラウザー間でデータを転送するための標準プロトコルです。ただし、HTTP ではデータの暗号化やセキュリティが提供されないため、Web トラフィックを傍受した人は誰でもデータを読み取ったり変更したりできます。したがって、暗号化されていない Web サイトは、盗聴、改ざん、またはなりすまし攻撃に対して脆弱です。
暗号化されていない Web サイトにアクセスする場合、URL は通常 http:// で始まり、その後にドメイン名とオプションでポート番号が続きます。たとえば、http://www.example.com または http://www.example.com:80 です。URL で文字列 http:// をスキャンすることにより、Web フィルターは暗号化されていない Web サイトを識別してブロックできます。
他のオプションは、暗号化されていない Web トラフィックのプロトコルと一致しないため、正しくありません。
Encryption=off は、Web リソースの暗号化ステータスを示すクエリ文字列として使用できますが、標準または必須のパラメータではありません。Https:// は暗号化された Web トラフィックのプロトコルで、データの暗号化とセキュリティのためにハイパーテキスト転送プロトコル セキュア (HTTPS) を使用します。Www.*.com は、www で始まり .com で終わるすべての Web サイトに一致するドメイン名として使用できますが、プロトコルは指定しません。:443 は暗号化された Web トラフィックのプロトコルである HTTPS のポート番号です。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 2 章: ネットワークのセキュリティ保護、ページ
69. Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 2.1: ネットワーク デバイスとテクノロジ、ビデオ: Web フィルター (5:16)。

最新問題**: 7**
ネットワーク管理者は、会社のクラウド環境にロード バランサーを展開するプロジェクトに取り組んでいます。このプロジェクトは次の基本的なセキュリティ要件のどれを満たしていますか?
A. プライバシー
B. 誠実さ
C. 機密性
D. 可用性
Answer: D (メーッセージを残す**)**
企業のクラウド環境にロード バランサを導入することで、可用性という基本的なセキュリティ要件が主に満たされます。ロード バランサは、着信ネットワーク トラフィックを複数

のサーバーに分散し、単一のサーバーが過負荷になることを防ぎ、一部のサーバーで障害が発生してもサービスが利用可能であることを保証します。
可用性: 必要なときにサービスとリソースにアクセスできることを保証します。これは、負荷分散によって直接サポートされます。
プライバシー: 個人情報や機密情報を不正アクセスから保護しますが、負荷分散とは直接関係ありません。
整合性: データが正確であり、改ざんされていないことを保証しますが、負荷分散では主にデータの整合性に重点が置かれていません。
機密性: 情報には許可された個人のみがアクセスできるようにします。これは負荷分散の主な懸念事項ではありません。

最新問題: **8**
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
Answer: C (メーッセージを残す**)**
国民国家とは、政府または政治団体の支援を受けて他の国や組織に対してサイバー攻撃を行う脅威アクターです。国民国家は、軍事、エネルギー、インフラストラクチャなどの重要なシステムを標的とする可能性のある、多額の資金、高度な技術スキル、および戦略目標を持っています。国民国家は、スパイ活動、破壊活動、または戦争を動機としていることがよくあります12。参考資料 = 1: CompTIA Security+ SY0-701 認定学習ガイド、542 ページ: 脅威アクター - CompTIA Security+ SY0-701 - 2.1、メッサー教授によるビデオ。

最新問題: **9**
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
Answer: A (メーッセージを残す**)**
エンゲージメント ルールは、侵入テストなどの情報セキュリティ テストの実行に関する詳細なガイドラインと制約です。テストの範囲、目的、方法、境界、およびテスト担当者とクライアントの役割と責任を定義します。エンゲージメント ルールは、テストが合法的、倫理的、専門的な方法で実施され、結果が正確で信頼できるものであることを保証するのに役立ちます。エンゲージメント ルールには通常、次の要素が含まれます。

* テストの種類と範囲（ブラック ボックス、ホワイト ボックス、グレー ボックスなど）、および対象のシステム、ネットワーク、アプリケーション、データ。
* テスト中に問題、インシデント、緊急事態を報告するためのクライアントの連絡先の詳細と通信チャネル。
* テスト チームの資格情報と、使用できる承認済みのツールとテクニック。
* テスト中に取得されたデータの保存、転送、廃棄方法など、機密データの取り扱いと暗号化の要件。
* ステータス会議とレポートのスケジュール、形式、受信者、およびテスト結果の機密保持契約と非開示契約。
* テストのタイムラインと期間、および運用時間とテスト期間。
* 不必要な損害、混乱、情報の漏洩を避けるなど、テスターに期待される専門的かつ倫理的な行動。
サプライ チェーン分析、監査権条項、デュー デリジェンスは、サード パーティの侵入テスターによるテストの条件とは関係ありません。サプライ チェーン分析は、ビジネス ネットワーク内のサプライヤとパートナーのセキュリティとリスクの状況を評価するプロセスです。監査権条項は、契約の条項で、一方の当事者にもう一方の当事者を監査して契約条件への準拠を確認する権利を与えるものです。デュー デリジェンスは、潜在的なベンダーまたはパートナーが組織にもたらすサイバー リスクを特定して対処するプロセスです。
参考資料 = 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

最新問題: **10**
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、次の点に気付きました。
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 のアカウントをブルートフォース攻撃しようとしています。
D. ドメインにランサムウェアが展開されました。
Answer: C (メーッセージを残す**)**
ブルート フォースは、多数の可能な組み合わせを使用して、ユーザー アカウントのパスワードやその他の資格情報を推測しようとするタイプの攻撃です。攻撃者は自動化されたツールまたはスクリプトを使用してブルート フォース攻撃を実行し、アカウントへの不正アクセスを取得することができます。ドメイン アクティビティ ログには、ユーザー ismith が短期間に 10 回連続してログインに失敗したことが示されています。これは、ブルート フォース攻撃の強力な指標です。ログには、失敗したログインのソース IP アドレスが ismith の通常の IP アドレスと異なることも示されています。これは、攻撃者が別のデバイスまたは場所を使用して攻撃を開始していることを示唆しています。セキュリティ アナリ

ストは、攻撃者の IP アドレスをブロックし、ismith のパスワードをリセットし、ismith にインシデントを通知するために、直ちに行動を起こす必要があります。参考資料 = 500 以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 1 章、14 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 1.1、2 ページ。脅威アクターと属性 - SY0-601 CompTIA Security+: 1.1

最新問題: **11**
従業員が、支払いウェブサイトからの電子メールで連絡先情報の更新を求めるリンクをクリックしました。従業員はログイン情報を入力しましたが、「ページが見つかりません」というエラー メッセージが表示されました。
次のどのタイプのソーシャル エンジニアリング攻撃が発生しましたか?
A. ブランドのなりすまし
B. プリテキスティング
C. タイプミススクワッティング
D. フィッシング
Answer: D (メーッセージを残す**)**
説明
フィッシングはソーシャル エンジニアリング攻撃の一種で、支払い Web サイト、銀行、その他の信頼できる組織などの正当なソースから送信されたように見える不正なメールを送信します。フィッシングの目的は、受信者を騙して悪意のあるリンクをクリックさせたり、悪意のある添付ファイルを開かせたり、ログイン認証情報、個人データ、財務情報などの機密情報を提供させたりすることです。このシナリオでは、従業員は支払い Web サイトから連絡先情報の更新を求めるメールを受け取りました。メールには、本物の Web サイトの外観を模倣した偽の Web サイトに従業員を誘導するリンクが含まれていました。
従業員はログイン情報を入力しましたが、「ページが見つかりません」というエラー メッセージが表示されました。これは、従業員がフィッシング攻撃の被害者となり、攻撃者が支払い Web サイトの従業員の資格情報を入手した可能性があることを示しています。参考資料 = その他のソーシャル エンジニアリング攻撃 - CompTIA Security+ SY0-701 - 2.2、CompTIA Security+: ソーシャル エンジニアリング手法とその他の攻撃... - NICCS、[500 以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版]

最新問題: **12**
絶えず変化する環境に最も適しているのはどれでしょうか?
A. RTOS
B. コンテナ
C. 組み込みシステム
D. SCADA
Answer: (解答を表示する**)**
コンテナは、アプリケーションを独自の依存関係、ライブラリ、および構成を持つ分離された環境で実行できるようにする仮想化の方法です。コンテナは軽量で、移植性があり、拡張

性があり、展開と更新が容易であるため、常に変化する環境に最適です。また、コンテナはマイクロサービス アーキテクチャをサポートできるため、ソフトウェア機能をより迅速かつ頻繁に提供できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 10 章: モバイル デバイス セキュリティ、512 ページ 1

最新問題: **13**
ユーザーが重要なシステムにパッチを適用しようとしましたが、パッチの転送に失敗しました。次のアクセス制御のうち、転送を阻害する可能性が高いのはどれですか。
A. 属性ベース
B. 時刻
C. ロールベース
D. 最小権限
Answer: D (メーッセージを残す**)**
説明
最小権限の原則では、ユーザーとプロセスは、タスクを実行するために必要な最小限のアクセス レベルのみを持つべきであると規定されています。これにより、セキュリティを侵害する可能性のある不正なアクションや不要なアクションを防止できます。この場合、ユーザーまたはプロセスが、転送に必要な重要なシステムまたはネットワーク リソースにアクセスするための適切な権限を持っていないため、パッチ転送が失敗する可能性があります。最小権限の原則を適用すると、ユーザーまたはプロセスにパッチ適用アクティビティに必要なアクセス権が付与され、この問題を回避できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、931 ページ

最新問題: **14**
ある会社の法務部門が SaaS アプリケーションで機密文書を作成し、高リスク国の個人がその文書にアクセスできないようにしたいと考えています。このアクセスを制限する最も効果的な方法はどれですか。
A. データマスキング
B. 暗号化
C. 地理位置情報ポリシー
D. データ主権規制
Answer: C (メーッセージを残す**)**
ジオロケーション ポリシーは、ユーザーまたはデバイスの地理的な場所に基づいて、データまたはリソースへのアクセスを制限または許可するポリシーです。ジオロケーション ポリシーは、IP アドレス フィルタリング、GPS 追跡、ジオフェンシングなどのさまざまな方法を使用して実装できます。ジオロケーション ポリシーは、企業の法務部門が、高リスク国の個人による機密文書への不正アクセスを防止するのに役立ちます12。
その他のオプションは、場所に基づいてアクセスを制限する効果的な方法ではありません。

* データ マスキング: 機密データを架空データまたは匿名データで隠したり置き換えたりする手法です。データ マスキングはデータのプライバシーと機密性を保護できますが、場所に基づいてデータへのアクセスを防ぐことはできません3。
* 暗号化: 秘密鍵またはアルゴリズムを使用してデータを読み取り不可能な形式に変換するプロセスです。暗号化によりデータの整合性と機密性が保護されますが、場所に基づいてデータへのアクセスを防ぐことはできません。また、復号化キーまたは復号化方法を持つ攻撃者によって暗号化がバイパスされる可能性もあります4。
* データ主権規制: これは、特定の管轄区域または国内でのデータの保存、処理、転送を規定する一連の法律または規則です。データ主権規制は、データの可用性とコンプライアンスに影響を与える可能性がありますが、場所に基づいてデータへのアクセスを禁止することはありません。データ主権規制は、国や地域によっても異なります。
参考資料 = 1: CompTIA Security+ SY0-701 認定試験学習ガイド、972 ページ: アカウント ポリシー - SY0-
601 CompTIA Security+: 3.7、Messer教授によるビデオ3: CompTIA Security+ SY0-701 認定試験学習ガイド、1004ページ: CompTIA Security+ SY0-701 認定試験学習ガイド、101 ページ。: CompTIA Security+ SY0-701 認定試験学習ガイド、102ページ。

最新問題**: 15**
システム管理者は、2 つのブランチ オフィス間のサイト間 VPN を構成しています。一部の設定は既に正しく構成されています。構成を完了するために、システム管理者には次の要件が提供されています。
* 最も安全なアルゴリズムを選択する必要があります
* すべてのトラフィックはVPN経由で暗号化される必要があります
* 2つのVPNコンセントレータを認証するために秘密のパスワードが使用されます

Answer:
すべての解決策については説明部分を参照してください。
Explanation:
提供された要件に従って 2 つのブランチ オフィス間のサイト間 VPN を構成するには、VPN コンセントレータに適用する必要がある詳細な手順と設定を次に示します。
要件：
* 最も安全なアルゴリズムを選択する必要があります。
* すべてのトラフィックは VPN 経由で暗号化される必要があります。
* 2 つの VPN コンセントレータを認証するために秘密のパスワードが使用されます。
VPN コンセントレータ 1 の構成:
フェーズ1:
* ピア IP アドレス: 5.5.5.10 (VPN コンセントレータ 2 の IP アドレス)
* 認証方法: PSK (事前共有キー)
* 交渉モード: MAIN
* 暗号化アルゴリズム: AES256
* ハッシュアルゴリズム: SHA256

* DHキーグループ: 14
フェーズ2:
* モード: トンネル
* プロトコル: ESP (Encapsulating Security Payload)
* 暗号化アルゴリズム: AES256
* ハッシュアルゴリズム: SHA256
* ローカルネットワーク/マスク: 192.168.1.0/24
* リモートネットワーク/マスク: 192.168.2.0/24
VPN コンセントレータ 2 の構成:
フェーズ1:
* ピア IP アドレス: 5.5.5.5 (VPN コンセントレータ 1 の IP アドレス)
* 認証方法: PSK (事前共有キー)
* 交渉モード: MAIN
* 暗号化アルゴリズム: AES256
* ハッシュアルゴリズム: SHA256
* DHキーグループ: 14
フェーズ2:
* モード: トンネル
* プロトコル: ESP (Encapsulating Security Payload)
* 暗号化アルゴリズム: AES256
* ハッシュアルゴリズム: SHA256
* ローカルネットワーク/マスク: 192.168.2.0/24
* リモートネットワーク/マスク: 192.168.1.0/24
まとめ：
* ピア IP アドレス: リモート VPN コンセントレータの IP アドレスに設定します。
* 認証方法: 事前共有キーを使用するための PSK。
* ネゴシエーション モード: 初期設定では MAIN です。
* 暗号化アルゴリズム: 強力で安全なアルゴリズムである AES256。
* ハッシュアルゴリズム: 強力なハッシュを提供する SHA256。
* DH キー グループ: 強力な Diffie-Hellman キー交換の場合は 14。
* フェーズ 2 プロトコル: 暗号化と整合性のための ESP。
* ローカルおよびリモート ネットワーク: 各ブランチ オフィスのサブネットに一致するように、ローカルおよびリモート ネットワーク アドレスを適切に構成します。
両方の VPN コンセントレータでこれらの設定を構成することにより、サイト間 VPN は強力なセキュリティ アルゴリズム、すべてのトラフィックの暗号化、事前共有キーを使用した認証の要件を満たすようになります。

最新問題**: 16**
数人の従業員が、最高経営責任者 (CEO) を名乗る人物から詐欺のテキスト メッセージを受け取りました。メッセージには次のように書かれていました。

私は今、空港にいて、メールにアクセスできません。従業員表彰賞用のギフト カードを購入していただく必要があります。ギフト カードを次のメール アドレスに送ってください。」この状況に対する最適な対応は次のうちどれですか? (2 つ選択してください)。
A. 現在の従業員表彰ギフトカードをキャンセルします。
B. 毎年の社内研修にスミッシング演習を追加します。
C. 会社全体に電子メールによる警告を発行します。
D. CEO に電話番号を変更してもらいます。
E. CEO の電話のフォレンジック調査を実施します。
F. モバイル デバイス管理を実装します。
Answer: B,C (メーッセージを残す**)**
この状況はスミッシングの一例です。スミッシングは、テキスト メッセージ (SMS) を使用して個人を誘導し、個人情報や機密情報をサイバー犯罪者に提供させるフィッシングの一種です。この状況に対する最善の対応は、年次の企業トレーニングにスミッシング演習を追加し、会社に一般的な電子メール警告を発行することです。スミッシング演習は、スミッシング攻撃を認識して回避する方法を従業員に教育し、意識を高めるのに役立ちます。電子メール警告は、従業員に不正なテキスト メッセージがあることを警告し、情報や金銭の要求の身元と正当性を確認するよう思い出させます。参考資料 = フィッシングとは | サイバーセキュリティ | CompTIA、フィッシング - SY0-601 CompTIA Security+: 1.1 - Professor Messer IT 認定トレーニング コース

最新問題**: 17**
ある企業がインフラストラクチャを再設計し、使用中の物理サーバーの数を減らしたいと考えています。この目標に最適なアーキテクチャは次のどれですか。
A. 仮想化
B. セグメンテーション
C. マイクロサービス
D. サーバーレス
Answer: (解答を表示する**)**

最新問題**: 18**
次のどれがクラウド環境における高可用性として分類されますか?

A. アクセスブローカー
B. クラウド HSM
C. WAF
D. ロードバランサー
Answer: D (メーッセージを残す)
クラウド環境では、高可用性は通常、ロード バランサの使用によって確保されます。ロード バランサは、ネットワークまたはアプリケーションのトラフィックを複数のサーバーに分散し、単一のサーバーが過負荷になることを防ぎ、1 台以上のサーバーに障害が発生してもサービスが利用可能であることを保証します。この設定により、アプリケーションの信頼性と可用性が向上します。
ロード バランサー: トラフィックを複数のサーバーまたはインスタンスに分散し、過負荷を防ぎ、継続的な可用性を確保することで、高可用性を実現します。
アクセス ブローカー: 通常、高可用性とは直接関係なく、リソースへの安全なアクセスを容易にするサービスを指します。
クラウド HSM (ハードウェア セキュリティ モジュール): クラウド内で安全なキー管理を提供しますが、特に高可用性を保証するものではありません。
WAF (Web アプリケーション ファイアウォール): HTTP トラフィックをフィルタリングおよび監視することで Web アプリケーションを保護しますが、主に高可用性の確保に重点を置いていません。

最新問題**: 19**
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
Answer: C (メーッセージを残す)
バッファ オーバーフローは、アプリケーションがメモリ バッファに保持できる以上のデータを書き込むと、隣接するメモリ位置が超過データによって上書きされる脆弱性です。レジスタは、一時的なデータや命令を保持する CPU 内の小さなストレージ領域です。攻撃者はバッファ オーバーフローを悪用して、シェルコードを指す悪意のあるアドレスでレジスタを上書きすることができます。シェルコードは、攻撃者がシステムを制御できるようにするコードです。これにより、攻撃者はアプリケーションの通常の実行フローをバイパスし、任意のコマンドを実行できます。
参考資料: CompTIA Security+ SY0-701 認定試験学習ガイド、第 2 章: 脅威、攻撃、脆弱性、セクション 2.3: アプリケーション攻撃、76 ページ 1; バッファ オーバーフロー - CompTIA Security+ SY0-
701 - 2.3 2

最新問題: **20**
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
Answer: (解答を表示する**)**
セキュリティ意識向上プログラムのトレーニング カリキュラム計画では、次の要素を考慮する必要があります。
組織が運営する業界に基づいた脅威ベクトル。これにより、従業員は組織が直面している特定のリスクと課題を理解し、サイバー攻撃から自分自身と組織を保護する方法を知ることができます。たとえば、ヘルスケア組織は、ランサムウェア、データ侵害、医療機器のハッキングなど、金融機関とは異なる脅威ベクトルに直面する可能性があります1。
トレーニング イベントの頻度と期間。これにより、従業員は学習した情報とスキルを維持し、セキュリティ環境の変化に対応できるようになります。トレーニング イベントは、主要な概念と行動を強化するのに十分な頻度で実施する必要がありますが、従業員の注意や関心を失わせるほど長すぎたり短すぎたりしてはなりません。たとえば、セキュリティ意識向上プログラムには、月刊ニュースレター、四半期ごとのウェビナー、年次ワークショップ、定期的なクイズなどが含まれます2。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、34 ページ; CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 2 章、55 ページ。

最新問題: **21**
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
Answer: A (メッセージを残す**)**
保存時の暗号化は、ノート PC などのデバイスに保存されているデータを、復号化キーまたはパスワードでのみアクセスできる読み取り不可能な形式に変換することで保護する戦略です。保存時の暗号化は、デバイスが物理的に侵害された場合でも、データへの不正アクセスを防止することで、盗難されたノート PC のデータ損失を防ぐことができます。保存時の暗号化は、データ保護を必要とするデータ プライバシー規制および標準に準拠するのにも役立ちます。マスキング、データ分類、およびアクセス許可の制限は、データ保護に役立つその他の戦略ですが、ノート PC に保存されているデータには十分ではないか、適用できな

い可能性があります。マスキングは、クレジットカード番号などの機密データ要素をランダムな文字または記号で隠す手法ですが、通常は転送中または使用中のデータに使用され、保存中のデータには使用されません。データ分類は、機密性とビジネスへの影響に基づいてデータにラベルを割り当てるプロセスですが、データ自体を保護するものではありません。アクセス許可の制限は、データにアクセス、変更、または削除できるユーザーを定義するルールですが、ノート PC が盗まれ、セキュリティ制御がバイパスされた場合、不正アクセスを防ぐことができない可能性があります。参考資料: CompTIA Security+ 学習ガイド:
試験 SY0-701、第 9 版、17-18 ページ、372-373

最新問題: **22**
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
Answer: (解答を表示する**)**
VPN は、パブリック ネットワークを介して 2 台以上のデバイス間に安全なトンネルを作成する仮想プライベート ネットワークです。VPN は、データの暗号化と認証を行うほか、デバイスの IP アドレスと場所を隠すことができます。ジャンプ サーバーは、ユーザーとターゲット サーバー (運用サーバーなど) の間の仲介役として機能するサーバーです。ジャンプ サーバーは、セキュリティとアクセス制御の追加レイヤー、およびログ機能と監査機能を提供できます。ファイアウォールは、定義済みのルールに基づいて不要なネットワーク トラフィックをフィルタリングしてブロックするデバイスまたはソフトウェアです。ファイアウォールは、内部ネットワークを外部の脅威から保護し、機密性の高いサービスとポートの露出を制限できます。セキュリティ アナリストは、運用ネットワークへのリモート デスクトップ アクセスのセキュリティを強化するために、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ことを推奨する必要があります。この方法では、リモート デスクトップ サービスはパブリック ネットワークに公開されず、VPN 資格情報を持つ承認済みユーザーのみがジャンプ サーバーにアクセスし、運用サーバーにアクセスできます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 8 章: セキュア プロトコルとサービス、382 ～ 383 ページ 1、第 9 章: ネットワーク セキュリティ、441 ～ 442 ページ 1

最新問題: **23**

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
Answer: D (メーッセージを残す**)**
FIM はファイル整合性監視の略で、ファイル、ディレクトリ、またはレジストリ キーの変更を検出してデータを保護する方法です。FIM を使用すると、セキュリティ管理者はデータに対する不正な変更や悪意のある変更を追跡したり、データの整合性とコンプライアンスを確認したりできます。また、FIM はデータに関連する潜在的な違反やインシデントを管理者に警告することもできます。

最新問題**: 24**
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
Answer: (解答を表示する**)**
暗号化とは、データを平文に戻すために必要な秘密鍵がなければ読み取れないようにデータを変換する方法です。暗号化は、データの不正アクセス、変更、盗難を防ぐため、保存中のデータを保護する最も一般的で効果的な方法の 1 つです。暗号化は、ブロック ストレージ、オブジェクト ストレージ、データベース、アーカイブなど、保存中のさまざまなタイプのデータに適用できます。ハッシュ化、トークン化、セグメンテーションは、保存中のデータを読み取り不可能にする方法ではなく、他の方法でデータを保護する方法です。
ハッシュは、入力からハッシュまたはダイジェストと呼ばれる固定長の出力を生成する一方向関数です。出力から入力を復元することはできません。ハッシュは、データの整合性と信頼性を検証するために使用されますが、データを暗号化するものではありません。トークン化は、機密データを、それ自体には意味や価値のないトークンと呼ばれる非機密の代替物に置き換えるプロセスです。トークン化は、機密データの露出とコンプライアンスの範囲を縮小するために使用されますが、データを暗号化するものではありません。セグメンテーションは、ネットワークまたはシステムをセグメントと呼ばれる、アクセスとセキュリティの異なるレベルのより小さな分離された単位に分割する手法です。セグメンテーションは、攻撃対象領域を制限し、侵害の影響を抑えるために使用されますが、保存されているデータを暗号化するものではありません。

最新問題**: 25**

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
Answer: A (メーッセージを残す**)**
アクティブ偵察は、ターゲットにパケットまたはリクエストを送信し、応答を分析する偵察の一種です。アクティブ偵察により、開いているポート、サービス、オペレーティング システム、脆弱性などの情報が明らかになることがあります。ただし、アクティブ偵察は、ターゲットまたはそのセキュリティ デバイス (ファイアウォールや侵入検知システムなど) によって検出される可能性も高くなります。ポート スキャンとサービス スキャンは、ターゲットを精査して特定の情報を探すため、アクティブ偵察手法の例です。参考資料 = CompTIA Security+ 認定試験の目標、ドメイン 1.1: シナリオが与えられた場合、適切な手法とツールを使用して偵察を実施します。CompTIA Security+ 学習ガイド (SY0-701)、第 2 章: 偵察と情報収集、47 ページ。CompTIA Security+ 認定試験 SY0-701 模擬試験 1、質問 1。

最新問題**: 26**
最高情報セキュリティ責任者 (CISO) は、経営陣へのレポートで、サービスとしてのランサムウェアの増加について明確に認識を高めたいと考えています。CISO のレポートに記載されている脅威アクターを最もよく表しているのは、次のうちどれですか。
A. 内部脅威
B. ハクティビスト
C. 国民国家
D. 組織犯罪
Answer: (解答を表示する**)**
説明
ランサムウェア ･アズ ･ア ･サービスは、ハッカーがランサムウェアのツールやサービスを他の犯罪者に販売または貸与し、攻撃を仕掛けて被害者から金銭をゆすり取るサイバー犯罪の一種です。これは、利益のために違法行為を行うために協力する犯罪者のグループである組織犯罪の典型的な例です。組織犯罪は、内部脅威、ハクティビスト、国家など、動機、方法、ターゲットが異なる可能性のある他のタイプの脅威アクターとは異なります。参考文献: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、17 ページ 1

最新問題**: 27**
大企業の最高情報セキュリティ責任者 (CISO) は、自社のセキュリティ ポリシーが外部規制当局によって課せられた要件とどのように比較されるかを理解したいと考えています。CISO は次のどれを使用する必要がありますか。

A. 侵入テスト
B. 内部監査
C. 証明
D. 外部検査
Answer: D (メーッセージを残す)
外部検査 (外部監査または外部レビューとも呼ばれます) は、最高情報セキュリティ責任者 (CISO) が会社のセキュリティ ポリシーを外部の規制要件と比較する方法について理解するための最適な方法です。外部検査は、法律、規制、業界標準に対する組織のコンプライアンスを評価する第三者機関によって実施されます。
* 侵入テストはコンプライアンスではなく脆弱性の特定に重点を置いています。
* 内部監査は内部統制を評価しますが、公平ではなく、規制要件に重点が置かれていません。
* 証明は正式な宣言であり、コンプライアンスの実際の評価は含まれません。

最新問題: **28**
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、次の点に気付きました。
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 のアカウントをブルートフォース攻撃しようとしています。
D. ドメインにランサムウェアが展開されました。
Answer: (解答を表示する)
ブルート フォースは、多数の可能な組み合わせを使用して、ユーザー アカウントのパスワードやその他の資格情報を推測しようとするタイプの攻撃です。攻撃者は自動化されたツールやスクリプトを使用してブルート フォース攻撃を実行し、アカウントへの不正アクセスを取得することができます。ドメイン アクティビティ ログには、ユーザー ismith が短期間に 10 回連続してログインに失敗したことが示されています。これは、ブルート フォース攻撃の強力な指標です。ログには、失敗したログインのソース IP アドレスが ismith の通常の IP アドレスと異なることも示されています。これは、攻撃者が別のデバイスまたは場所を使用して攻撃を開始していることを示しています。セキュリティ アナリストは、攻撃者の IP アドレスをブロックし、ismith のパスワードをリセットし、ismith にインシデントを通知するために、直ちに行動を起こす必要があります。参考資料 = 500 以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 1 章、14 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 1.1、2 ページ。脅威アクターと属性 - SY0-601 CompTIA Security+: 1.1

最新問題: **29**

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
Answer: (解答を表示する**)**
バッファ オーバーフローは、アプリケーションがメモリ バッファに保持できる以上のデータを書き込むと発生するソフトウェア脆弱性の一種で、超過したデータによって隣接するメモリ位置が上書きされます。これにより、クラッシュ、エラー、コード実行などの予期しない動作が発生する可能性があります。バッファ オーバーフローは、攻撃者が悪意のあるコードやコマンドをアプリケーションに挿入するために悪用される可能性があり、システムのセキュリティと機能が侵害される可能性があります。組織のインターネットに面した Web サイトは、攻撃者がバッファ オーバーフローを悪用したときに侵害されました。今後同様の攻撃から組織を保護するには、Web アプリケーション ファイアウォール (WAF) を導入する必要があります。WAF は、Web アプリケーションとインターネット間のトラフィックを監視およびフィルタリングするファイアウォールの一種です。WAF は、バッファ オーバーフロー、SQL インジェクション、クロスサイト スクリプティング (XSS) などの一般的な Web 攻撃を検出してブロックできます。また、WAF は、入力検証、出力エンコード、暗号化などのセキュリティ ポリシーとルールを適用することもできます。WAF は Web アプリケーションに保護レイヤーを提供し、攻撃者が脆弱性を悪用してデータを侵害するのを防ぎます。

最新問題: **30**
企業は、ネットワークを構築するときに認定ハードウェアを使用する必要があります。偽造ハードウェアの調達に伴うリスクに最もよく対処しているのは、次のどれですか。
A. サプライチェーンの徹底的な分析
B. 法的に強制力のある企業買収ポリシー
C. ベンダー契約およびSOWにおける監査権条項
D. すべてのサプライヤーとベンダーに対する徹底的な侵入テスト
Answer: (解答を表示する**)**
説明
偽造ハードウェアとは、OEM (Original Equipment Manufacturer) の許可なく製造または変更されたハードウェアのことです。ネットワークの品質、パフォーマンス、安全性、信頼性に重大なリスクをもたらす可能性があります12。偽造ハードウェアには、ネットワークのセキュリティとネットワークを流れるデータを危険にさらす可能性のある悪意のあるコンポーネントが含まれている場合もあります3。偽造ハードウェアの調達に関連するリスクに対処するには、企業はサプライ チェーン (ハードウェアの製造、流通、配送に関与するエンティティのネットワーク) を徹底的に分析する必要があります。サプライ チェーンを分析

することで、企業はハードウェアの出所、信頼性、整合性を確認し、偽造または改ざんされた製品の潜在的な出所を特定できます。サプライ チェーンの徹底的な分析には、次の手順が含まれます。
OEM および認定再販業者との信頼関係を確立する OEM または認定再販業者にハードウェアのドキュメントと証明書を要求する ラベル、シリアル番号、コンポーネントの不一致など、ハードウェアに改ざんの兆候がないか検査する ハードウェアの機能、パフォーマンス、セキュリティをテストする ハードウェアのライフサイクル全体を監視する追跡システムを実装する 疑わしいハードウェアや偽造ハードウェアを OEM および法執行機関に報告する 参照資料 = 1: 偽造および海賊版製品の特定 - Cisco、2: ハードウェア セキュリティとは? 定義、脅威、およびベスト プラクティス、3: 偽造ネットワーク機器にご注意ください - TechNewsWorld、: 偽造ハードウェア: 脅威とその回避方法

最新問題**: 31**
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
Answer: A (メーッセージを残す**)**
代替コントロールは、プライマリ コントロールでは解決できない脆弱性や弱点のリスクを軽減するために実装されるセキュリティ対策です。代替コントロールは脆弱性や弱点を防止または排除するものではありませんが、攻撃の可能性や影響を軽減できます。特定の内部 IP アドレスからの接続のみを許可するレガシー Linux システム上のホストベースのファイアウォールは、外部または許可されていないソースからの潜在的な脅威に対するシステムの露出を制限できるため、代替コントロールの一例です。ホストベースのファイアウォールは、一連のルールまたはポリシーに基づいて、単一のホスト上の受信および送信ネットワーク トラフィックを監視およびフィルタリングするソフトウェア アプリケーションです。レガシー Linux システムは、最新のセキュリティ更新やパッチと互換性がない可能性があり、攻撃者に悪用される可能性のある既知の脆弱性や弱点がある可能性のある、Linux オペレーティング システムの古いバージョンです。参考資料 = セキュリティ コントロール - SY0-601 CompTIA Security+: 5.1、セキュリティ コントロール - CompTIA Security+ SY0-501 - 5.7、500 以上の練習テスト問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 5 章、240 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 5.1、18 ページ。

最新問題: 32
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
Answer: B (メーッセージを残す)
アクセスの無効化は、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のユースケースです。アクセスの無効化は、ログイン認証情報、メール、VPN、クラウド サービスなどのユーザー アカウントのアクセス権を取り消すか、一時停止するプロセスです。アクセスを無効にすると、アカウントを侵害した可能性のある元従業員や攻撃者によるアカウントの不正使用や悪意のある使用を防ぐことができます。また、アクセスを無効にすると、攻撃対象領域が減り、データ侵害や漏洩のリスクも軽減されます。アクセスの無効化は、従業員の退職、辞職、異動などの定義済みイベントに基づいてアクションをトリガーできるスクリプト、ツール、ワークフローを使用して自動化できます。自動化により、手動介入や人的エラーに頼ることなく、アクセスをタイムリーかつ一貫性のある効率的な方法で無効にすることができます。

最新問題: 33
ある組織では、サーバーのハードウェアの問題を解決するために必要な時間を計算したいと考えています。
次のリスク管理プロセスのどれがこの例を説明していますか?
A. リカバリポイント目標
B. 平均故障間隔
C. 回復時間目標
D. 平均修復時間
Answer: D (メーッセージを残す)
平均修復時間 (MTTR) は、サーバーのハードウェアの問題を解決するのに必要な時間を表します。
MTTR は、リスク管理とメンテナンスにおける重要な指標であり、故障したコンポーネントまたはシステムを修復して動作状態に戻すのに必要な平均時間を測定します。
リカバリポイント目標 (RPO): 時間で測定されたデータ損失の最大許容量を定義します。これは、災害後にデータを復元する必要がある時点です。

平均故障間隔 (MTBF): システムまたはコンポーネントの故障間隔の平均時間を測定し、信頼性を示します。
復旧時間目標 (RTO): 災害や中断後にシステムを復旧するために許容される最大時間を定義します。
平均修復時間 (MTTR): 故障したコンポーネントまたはシステムを修復するのに必要な平均時間を測定します。

最新問題**: 34**
最近の侵害では、サービスデスクの従業員が、従業員を装って電話をかけてきた攻撃者に MFA バイパス コードを発行したため、従業員の資格情報が侵害されました。今後、この種のインシデントを防ぐには、次のどれを使用する必要がありますか。
A. ハードウェア トークン MFA
B. 生体認証
C. 本人確認
D. 最小権限
Answer: C (メッセージを残す**)**
従業員を装った攻撃者に MFA バイパス コードが発行されるのを防ぐには、身元証明を実装することが最も効果的です。身元証明では、アクセスを許可したり機密情報を提供したりする前に、個人の身元を確認します。
本人確認: MFA バイパスを要求している人物が本人であることを確認し、攻撃者が正当な従業員を装うソーシャル エンジニアリング攻撃を防止します。
ハードウェア トークン MFA: 認証のための追加要素を提供しますが、要求者の ID の確認には対応していません。
生体認証: 身体的特徴に基づいた強力な認証を提供しますが、MFA バイパス コードの発行プロセスとは関係ありません。
最小権限: ユーザーのアクセス権を、作業を実行するために必要な最小限に制限しますが、サービス デスクを標的としたソーシャル エンジニアリング攻撃を防ぐことはできません。

最新問題**: 35**
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は、IP アドレスが組織のネットワークにアクセスするの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どれですか。
A. アクセスリスト インバウンド 拒否 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
B. アクセスリスト インバウンド 拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
C. アクセスリスト インバウンド 許可 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
D. アクセスリスト インバウンド 許可 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
Answer: B (メッセージを残す**)**

ファイアウォール ルールは、パケットがファイアウォールを通過することを許可するか拒否するかを決定する一連の基準です。ファイアウォール ルールは、アクション、プロトコル、送信元アドレス、宛先アドレス、ポート番号などの複数の要素で構成されます。ファイアウォール ルールの構文は、ファイアウォールの種類とベンダーによって異なる場合がありますが、基本的なロジックは同じです。この質問では、セキュリティ アナリストは、IP アドレス 10.1.4.9 が組織のネットワークにアクセスするのをブロックする受信ファイアウォール ルールを作成しています。つまり、アクションは拒否、プロトコルは any (または IP の場合は ig)、送信元アドレスは 10.1.4.9 である必要があります。
/32 (単一の IP アドレスを意味します)、宛先アドレスは 0.0.0.0/0 (任意の IP アドレスを意味します)、ポート番号は任意である必要があります。したがって、正しいファイアウォール ルールは次のようになります。
アクセスリスト 受信拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
このルールは、送信元 IP アドレスが 10.1.4.9 であるすべてのパケットに一致し、それをドロップします。その他のオプションは、アクション、送信元アドレス、または宛先アドレスが間違っているため、正しくありません。たとえば、オプション A では送信元アドレスと宛先アドレスが逆になっているため、宛先 IP アドレスが 10.1.4.9 であるすべてのパケットがブロックされますが、これは本来の目的ではありません。オプション C ではアクションが間違っており、許可になっています。つまり、パケットがファイアウォールを通過できるようになりますが、これも本来の目的ではありません。オプション D には、送信元アドレスと宛先アドレスが逆になっているため、オプション A と同じ問題があります。
参考資料 = ファイアウォールルール - CompTIA Security+ SY0-401: 1.2、ファイアウォール - SY0-601 CompTIA Security+:
3.3、ファイアウォール - CompTIA Security+ SY0-501、ファイアウォール ルールの理解 - CompTIA Network+ N10-
005: 5.5、Windows ファイアウォールの構成 - CompTIA A+ 220-1102 - 1.6。

最新問題**: 36**
オンボーディング プロセス中に、従業員はイントラネット アカウントのパスワードを作成する必要があります。パスワードには、10 文字の英数字と特殊文字 2 文字を含める必要があります。パスワードが作成されると、会社はイントラネット プロファイルに基づいて、従業員に会社所有の他の Web サイトへのアクセスを許可します。
イントラネット アカウントを保護し、ユーザーのイントラネット アカウントに基づいて複数のサイトへのアクセスを許可するために、企業が使用するアクセス管理の概念は次のどれですか (2 つ選択)。
A. 連邦
B. 本人確認
C. パスワードの複雑さ
D. デフォルトのパスワードの変更
E. パスワードマネージャー

F. オープン認証
Answer: (解答を表示する**)**
説明
フェデレーションは、ユーザーが一度認証するだけで、異なるドメインや組織にまたがる複数のリソースやサービスにアクセスできるようにするアクセス管理の概念です。フェデレーションは、ユーザーの資格情報を保存し、それを公開せずに要求されたリソースやサービスに提供する信頼できるサードパーティに依存します。
パスワードの複雑さは、長さ、文字の種類、一意性など、特定の基準を満たすパスワードをユーザーに作成させるセキュリティ対策です。パスワードの複雑さにより、パスワードの解読や推測が困難になり、ブルートフォース攻撃、パスワード推測、クレデンシャルスタッフィングを防ぐことができます。参考文献: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、308 ～ 309 ページおよび
312-313 1

最新問題**: 37**
BYOD プログラムを導入する企業にとって、セキュリティ上の主な懸念事項は次のどれですか?
A. 寿命の終わり
B. バッファオーバーフロー
C. VMエスケープ
D. 脱獄
Answer: D (メーッセージを残す**)**
説明
ジェイルブレイクは、BYOD (Bring Your Own Device) プログラムを導入する企業にとって、セキュリティ上の主な懸念事項です。ジェイルブレイクとは、スマートフォンやタブレットなどのデバイスに対するメーカーまたはキャリアの制限を解除して、ルート アクセスを取得し、許可されていないソフトウェアやカスタム ソフトウェアをインストールするプロセスです。ジェイルブレイクにより、デバイスとそこに保存されているデータのセキュリティが侵害されるだけでなく、マルウェア、ウイルス、ハッキングの危険にさらされる可能性があります。また、ジェイルブレイクはデバイスの保証と利用規約に違反し、企業のセキュリティ ポリシーや標準に準拠しなくなる可能性があります。したがって、BYOD プログラムを導入する企業は、ジェイルブレイクを禁止し、デバイスのコンプライアンスと暗号化を実施する必要があります。参考資料 = 500 問以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、ページ
76. CompTIA Security+ SY0-701 試験目標、ドメイン 2.4、11 ページ。

最新問題**: 38**
ある企業は、侵入テストとソーシャル エンジニアリングを含む攻撃的なセキュリティ評価を実行するためにコンサルタントを雇いました。
次のどのチームがこの評価活動を実施しますか?

A. 白
B. 紫
C. 青
D. 赤
Answer: D (メーッセージを残す)
レッド チームは、侵入テストやソーシャル エンジニアリングを含む攻撃的なセキュリティ評価を実行するセキュリティ専門家のグループです。レッド チームは、実際の攻撃をシミュレートし、ターゲットの組織、システム、またはネットワークの脆弱性を悪用します。レッド チームの目的は、ターゲットのセキュリティ制御、ポリシー、および手順の有効性、およびスタッフとブルー チームの認識と対応をテストすることです。レッド チームは、外部コンサルタントとして雇用することも、組織内で内部的に形成することもできます。

最新問題**: 39**
ある企業が、社内ネットワークから発信される DNS トラフィックを制限しようとしています。発信 DNS 要求は、IP アドレス 10.50.10.25 を持つ 1 つのデバイスからのみ許可されます。次のファイアウォール ACL のどれがこの目的を達成しますか。
A. アクセスリスト アウトバウンド許可 0.0.0.0 0 0.0.0.0/0 ポート 53 アクセスリスト アウトバウンド拒否 10.50.10.25 32
0.0.0.0/0 ポート53
B. アクセスリスト アウトバウンド許可 0.0.0.0/0 10.50.10.25 32 ポート 53 アクセスリスト アウトバウンド拒否 0.0.0.0 0
0.0.0.0/0 ポート53
C. アクセスリスト アウトバウンド許可 0.0.0.0 0 0.0.0.0/0 ポート 53 アクセスリスト アウトバウンド拒否 0.0.0.0/0 10.50.10.25
32 ポート 53
D. アクセスリスト アウトバウンド 許可 10.50.10.25 32 0.0.0.0/0 ポート 53 アクセスリスト アウトバウンド 拒否
0.0.0.0.0.0.0.0/0 ポート53
Answer: (解答を表示する)
正解は D です。これは、IP アドレスが 10.50.10.25 のデバイスのみがポート 53 でアウトバウンド DNS 要求を送信できるようにし、他のすべてのデバイスがこれを拒否するためです。他のオプションは、すべてのデバイスがアウトバウンド DNS 要求を送信できるようにしている (A と C) か、どのデバイスもアウトバウンド DNS 要求を送信できない (B) ため、不正解です。参考資料 = ファイアウォール ACL と DNS の詳細については、次のリソースを参照してください。
* CompTIA Security+ SY0-701 認定試験学習ガイド、第 4 章: ネットワーク セキュリティ 1
* メッサー教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 3.2: ファイアウォール ルール 2
* 合計: CompTIA Security+ Cert (SY0-701) | Udemy、セクション 6: ネットワーク セキュリティ、講義 28:

ファイアウォールルール3

最新問題: **40**
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
Answer: D (メーッセージを残す**)**
ユーザー プロビジョニング スクリプトは、定義済みの一連の命令またはコマンドを使用してユーザー アカウントを作成、変更、または削除し、適切なアクセスまたは権限を割り当てる自動化手法です。ユーザー プロビジョニング スクリプトを使用すると、手動エラーが減り、一貫性とコンプライアンスが確保され、時間とリソースが節約されるため、アカウント作成が効率化されます。その他のオプションは、アカウント作成を効率化できる自動化手法ではありません。
ガードレール スクリプト: これは、システムまたはネットワーク上のセキュリティ ポリシーとルールを監視して適用するスクリプトです。ガードレール スクリプトは、セキュリティ設定の変更、制限されたリソースへのアクセス、不要なソフトウェアのインストールなど、不正または悪意のあるアクションを防止するのに役立ちます。チケット ワークフロー: これは、ユーザーまたは顧客から報告されたリクエスト、問題、またはインシデントを追跡して管理するプロセスです。チケット ワークフローは、コミュニケーション、コラボレーション、および問題の解決を改善するのに役立ちますが、アカウント作成プロセスを自動化するものではありません。エスカレーション スクリプト: これは、特定の条件またはしきい値に達したとき、またはそれを超過したときにアラートまたは通知をトリガーするスクリプトです。エスカレーション スクリプトは、セキュリティ違反、パフォーマンスの低下、またはサービスの停止などの重大な状況を関係者または当局に通知するのに役立ちます。

最新問題: **41**
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 ログを確認し、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。
次のどれが最も起こりそうですか?
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。
Answer: D (メーッセージを残す**)**
説明
ルートキットは、システム ファイルやプロセスを変更または置き換えて、その存在やアクティビティを隠すマルウェアの一種です。ルートキットは、Windows システムのコマンド ライン インタープリターである cmd.exe ファイルのハッシュを変更して、ウイルス対策ツールやファイル整合性監視ツールによる検出を回避できます。また、ルートキットは、感染したシステムへのリモート アクセスと制御を攻撃者に許可するほか、データの盗難、バックドアのインストール、他のシステムへの攻撃の開始などの悪意のあるアクションを実行することもできます。ルートキットは、OS を再起動したり再インストールしたりした後でも存続するため、削除が最も難しいマルウェアの 1 つです。参考資料 = CompTIA Security+ 学習ガイド (500 問以上の練習問題付き): 試験 SY0-701、第 9 版、第 4 章、ページ 147. CompTIA Security+ SY0-701 試験目標、ドメイン 1.2、9 ページ。

最新問題**: 42**
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
Answer: (解答を表示する**)**
説明
利用規定 (AUP) は、ユーザーが企業ネットワークやインターネットにアクセスして使用する方法を規定する一連の規則です。AUP は、企業がサイバー セキュリティの脅威にさらされるリスクを最小限に抑え、その他のリスクを制限するのに役立ちます。また、AUP は、ユーザーに禁止事項を通知する役割も果たし、企業をネットワークの悪用から保護します。通常、ユーザーはネットワークにアクセスする前に、規則を理解して同意していることを確認する必要があります1。
AUP は、潜在的なセキュリティ インシデントの発生を阻止または阻止することを目的としているため、予防的なセキュリティ管理タイプを最もよく表しています。予防管理はプロアクティブであり、起こり得る脅威と脆弱性を予測し、システムやデータが悪用されたり損害を受けたりしないように対策を講じます。予防管理は、物理的、技術的、または管理的な性質を持つ場合があります2。
予防管理の例としては、次のようなものがあります。
* 施設やデバイスへの不正な物理的アクセスを防ぐためのロック、フェンス、ガード
* ネットワークやシステムへの不正な論理アクセスを防ぐファイアウォール、ウイルス対策ソフトウェア、または暗号化
* ユーザーや従業員による不正または不適切な行動や行為を防止するポリシー、手順、またはトレーニング AUP は、ネットワークと IT リソースのセキュリティと適切な使用を確保

するためにユーザーが従う必要があるポリシーと手順を定義するため、管理上の予防制御の一例です。AUP は、次のようなネットワークまたはシステムのセキュリティ、パフォーマンス、または可用性を危険にさらす可能性のあるアクティビティにユーザーが関与するのを防止できます。
* 許可されていないソフトウェアや悪意のあるソフトウェアのダウンロードまたはインストール
* 許可や暗号化なしで機密情報や秘密情報にアクセスしたり共有したりすること
* ネットワークまたはシステムを個人的な目的、違法な目的、または非倫理的な目的で使用する
* セキュリティ制御やメカニズムを回避または無効化する
* セキュリティ保護されていないデバイスや承認されていないデバイスをネットワークに接続する
AUP を実施することで、企業はユーザーの行動または不作為によって引き起こされるセキュリティ侵害、データ損失、法的責任、または評判の失墜の可能性を防止または軽減できます3。
参考資料 = 1: 許容使用ポリシーの作成方法 - CoreTech、2: [セキュリティ制御の種類: 予防、検出、修正、補償]、3: 企業許容使用ポリシーが必要な理由 - CompTIA

最新問題**: 43**
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。
Answer: A (メーッセージを残す**)**
ビジネスメール詐欺 (BEC) 攻撃は、会社の資金や機密情報にアクセスできる従業員をターゲットにしたフィッシング攻撃の一種です。攻撃者は、役員、ベンダー、顧客などの信頼できる人物になりすまし、不正な支払い、電信送金、機密データを要求します。攻撃者は、緊急性、圧力、親密さなどのソーシャルエンジニアリング手法を使用して、被害者に要求に応じるよう説得することがよくあります12。
このシナリオでは、オプション A は、BEC 攻撃の可能性を示しています。従業員は、メールの表示フィールドに役員の名前が記載されたメールでギフト カードのリクエストを受け取ります。メールは役員から送信されたように見えますが、実際のメール アドレスは偽装または侵害されている可能性があります。攻撃者は、従業員や顧客に報いるなどのビジネス目的でギフト カードが必要であると主張し、従業員にギフト カードを購入してコードを

送信するように要求する可能性があります。これは、BEC 攻撃者が疑いを持たない被害者から金銭を盗むために使用する一般的な戦術です34。
オプション B は、悪意のあるソフトウェアがデバイス上のファイルを暗号化し、復号キーの身代金を要求するランサムウェア攻撃の可能性について説明しています。オプション C は、攻撃者が正当な権限を装って特権アカウントのログイン情報を取得しようとする資格情報収集攻撃の可能性について説明しています。
オプション D は、フィッシング攻撃の可能性を示しています。攻撃者は、企業のメールポータルを模倣した偽の Web サイトに被害者を誘導し、認証情報を取得しようとします。これらはすべてサイバー攻撃の一種ですが、BEC 攻撃の例ではありません。参考資料 = 1: ビジネス メール詐欺 - CompTIA Security+ SY0-701 - 2.2 2: CompTIA Security+ SY0-701 認定試験学習ガイド 3: ビジネスメール詐欺: 120 億ドルの詐欺 4: 合計: CompTIA Security+ 認定 (SY0-701) | Udemy

最新問題**: 44**
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は、IP アドレスが組織のネットワークにアクセスするの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どれですか。
A. アクセスリスト インバウンド 拒否 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
B. アクセスリスト インバウンド 拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
C. アクセスリスト インバウンド 許可 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
D. アクセスリスト インバウンド 許可 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
Answer: B (メーッセージを残す**)**
ファイアウォールルールは、パケットがファイアウォールを通過することを許可するか拒否するかを決定する一連の基準です。ファイアウォールルールは、アクション、プロトコル、送信元アドレス、宛先アドレス、ポート番号などのいくつかの要素で構成されます。ファイアウォールルールの構文は、ファイアウォールの種類とベンダーによって異なる場合がありますが、基本的なロジックは同じです。この質問では、セキュリティアナリストは、IPアドレス10.1.4.9が組織のネットワークにアクセスするのをブロックする受信ファイアウォールルールを作成しています。つまり、アクションは拒否、プロトコルは任意（IPの場合はig）、送信元アドレスは
10.1.4.9/32 (単一の IP アドレスを意味します)、宛先アドレスは 0.0.0.0/0 (任意の IP アドレスを意味します)、ポート番号は任意である必要があります。したがって、正しいファイアウォール ルールは次のようになります。
アクセスリスト 受信拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
このルールは、送信元 IP アドレスが 10.1.4.9 であるすべてのパケットと一致し、それをドロップします。

その他のオプションは、アクション、送信元アドレス、または宛先アドレスが間違っているため、正しくありません。たとえば、オプション A では送信元アドレスと宛先アドレスが逆になっているため、宛先 IP アドレスが 10.1.4.9 であるパケットはすべてブロックされますが、これは本来の目的ではありません。オプション C ではアクションが間違っており、許可になっています。つまり、パケットがファイアウォールを通過できるようになりますが、これも本来の目的ではありません。オプション D には、送信元アドレスと宛先アドレスが逆になっているため、オプション A と同じ問題があります。
参考資料 = ファイアウォールルール - CompTIA Security+ SY0-401: 1.2、ファイアウォール - SY0-601 CompTIA Security+:
3.3、ファイアウォール - CompTIA Security+ SY0-501、ファイアウォールルールの理解 - CompTIA Network+ N10-005:
5.5、Windows ファイアウォールの構成 - CompTIA A+ 220-1102 - 1.6。

最新問題**: 45**
従業員を異なる役割に割り当てることで不正行為を検出するために最も効果的なのは次のうちどれですか?
A. 最小権限
B. 強制休暇
C. 職務の分離
D. ジョブローテーション
Answer: D (メーッセージを残す**)**
ジョブローテーションは、組織内で従業員を定期的に異なる役割に割り当てることで不正行為を検出し防止するために組織で使用される戦略です。このアプローチにより、特定のプロセスまたは一連のタスクを長期間にわたって 1 人の従業員が独占的に管理することがなくなり、不正行為が見過ごされる可能性が減ります。役割をローテーションすることで、組織は機密機能に長期間アクセスしていた従業員によって隠されていた可能性のある不正行為や矛盾を発見できます。ジョブローテーションはクロストレーニングも促進し、組織全体の回復力と柔軟性を高めることができます。
参考文献
* CompTIA Security+ SY0-701 コース内容: ドメイン 05 セキュリティ プログラムの管理と監視。
* CompTIA Security+ SY0-601 学習ガイド: リスク管理とコンプライアンスの章。

最新問題**: 46**
ある企業は、SIEM システムを導入し、アナリストを任命して毎週ログを確認することを計画しています。
会社が設定している制御の種類は次のうちどれですか?
A. 修正
B. 予防的
C. 探偵

D. 抑止力
Answer: C (メーッセージを残す)
説明
検出制御は、システムまたはネットワーク内のイベントとアクティビティを監視および分析し、インシデントまたは違反が発生したときに警告または報告するタイプの制御です。SIEM (セキュリティ情報およびイベント管理) システムは、ファイアウォール、ルーター、サーバー、アプリケーションなどのさまざまなソースからログを収集、相関、分析し、セキュリティの状態とインシデントの集中ビューを提供するツールです。
毎週ログを確認するアナリストは、潜在的な脅威や侵害を示す異常、傾向、パターンを特定して調査することができます。検出制御は、企業がインシデントに迅速かつ効果的に対応し、セキュリティ体制と回復力を向上させるのに役立ちます。参考資料 = 500 問以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 1 章、23 ページ。CompTIA Security+ SY0-701 試験目標、ドメイン 4.3、ページ
14.

最新問題: **47**
エンジニアがネットワーク デバイスの廃止を推奨すべきケースは次のうちどれですか (2 つ選択)。
A. デバイスは実稼働環境からテスト環境に移動されました。
B. デバイスはクリアテキスト パスワードを使用するように構成されています。
C. デバイスは企業ネットワーク上の分離されたセグメントに移動されます。
D. デバイスが企業内の別の場所に移動されます。
E. デバイスの暗号化レベルが組織の標準を満たすことができません。
F. デバイスは承認された更新を受信できません。
Answer: E (メーッセージを残す)
デバイスが企業環境にセキュリティ リスクやコンプライアンス違反をもたらす場合、エンジニアはネットワーク デバイスの廃止を推奨する必要があります。暗号化標準に準拠できないデバイスや承認された更新を受信できないデバイスは、攻撃や侵害に対して脆弱であり、機密データを公開したり、ネットワークの整合性を損なったりする可能性があります。したがって、このようなデバイスはネットワークから削除し、より安全で更新されたデバイスに置き換える必要があります。

参考文献
* CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、セクション 2.2、671 ページ
* CompTIA Security+ 模擬試験: 試験 SY0-701、第 3 版、第 2 章、質問 16、512 ページ

最新問題: **48**
次のリスクのうち、HTTP ヘッダーによって軽減できるものはどれですか?
A. SQLi
B. XSS
C. DoS
D. SSL
Answer: B (メーッセージを残す**)**
HTTP ヘッダーを使用すると、クロスサイト スクリプティング (XSS) に関連するリスクを軽減できます。コンテンツ セキュリティ ポリシー (CSP) や X-XSS-Protection などのセキュリティ関連の HTTP ヘッダーを設定すると、Web ページのコンテキストで悪意のあるスクリプトが実行されないようにすることができます。XSS (クロスサイト スクリプティング): 攻撃者が他のユーザーが閲覧する Web ページに悪意のあるスクリプトを挿入できる脆弱性。CSP などの HTTP ヘッダーは、読み込みを許可する動的リソースを指定することにより、XSS 攻撃を防ぐのに役立ちます。
SQLi (SQL インジェクション): 通常は、HTTP ヘッダーではなく、パラメーター化されたクエリと入力検証を使用して軽減されます。
DoS (サービス拒否): HTTP ヘッダーではなく、ネットワークおよびアプリケーション レベルの防御によって軽減されます。
SSL (Secure Sockets Layer): 通信のセキュリティ保護を指し、HTTP ヘッダーによって直接緩和されるのではなく、SSL/TLS プロトコルを使用して実装されます。

最新問題: **49**
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
Answer: D (メーッセージを残す**)**
侵入防止システム (IPS) は、ネットワーク トラフィックを監視し、定義済みのルールまたはシグネチャに基づいて悪意のあるパケットをブロックまたは変更するセキュリティ デバイスです。IPS は、悪意のあるパケットがターゲット システムに到達する前に検出してドロップすることで、古いバージョンのブラウザーの既知の脆弱性を悪用する攻撃を防止

できます。IPS は、レート制限、暗号化、リダイレクトなどの他の機能も実行できます。参照: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 3 章: ネットワークのセキュリティ保護、132 ページ。

最新問題: **50**
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
Answer: (解答を表示する**)**
データ保持ポリシーは、データを保存する期間と、データを削除またはアーカイブする時期を定義する一連のルールです。管理者は、組織のデータ保持ポリシーに従って、法務およびコンプライアンス チームが顧客トランザクションに関する情報を適切な期間アーカイブできるように支援します。このポリシーは、組織が法的および規制上の要件に準拠し、ストレージ スペースを最適化し、データのプライバシーとセキュリティを保護するのに役立ちます。
参照
CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 3 章、セクション 3.4、ページ 1211 CompTIA Security+ 模擬試験: 試験 SY0-701、第 3 版、第 3 章、質問 15、ページ 832

最新問題: **51**
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
Answer: A (メーッセージを残す**)**
正解は A です。多要素認証 (MFA) は、ユーザーが知っている情報 (パスワードなど)、ユーザーが所有している情報 (トークンなど)、またはユーザー自身 (生体認証など) など、複数の要素を要求することでユーザーの ID を確認する方法です。MFA では、攻撃者がログインするために別の要素を提供する必要があるため、ユーザーのパスワードが侵害された場合でも不正アクセスを防止できます。その他の選択肢は、認証の弱さという攻撃の根本原因

に対処していないため、正しくありません。権限の割り当て (B) は、ユーザーの役割または ID に基づいてリソースへのアクセスを許可または拒否するプロセスです。
アクセス管理とは、誰が何にどのような条件でアクセスできるかを制御するプロセスです。パスワードの複雑さ (D) は、推測や解読が困難な強力なパスワードを使用する必要があることを意味しますが、攻撃者が盗んだパスワードを使用することを防ぐことはできません。

最新問題: **52**
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
Answer: (解答を表示する**)**
災害復旧計画 (DRP) は、システム障害、自然災害、その他の緊急事態が発生した場合に組織の通常の業務を回復することを目的とした一連のポリシーと手順です。DRP には通常、次の要素が含まれます。
組織の重要な資産とプロセスに対する潜在的な脅威と影響を特定するリスク評価。
最も重要な機能とデータの回復を優先するビジネス影響分析。
復旧チームの役割と責任、必要なリソースとツール、システムを復元するための手順を定義する復旧戦略。
DRP が定期的に更新され、検証されることを保証するテストおよびメンテナンス プラン。DRP は、災害からの復旧とダウンタイムおよびデータ損失の最小化のための明確で構造化されたフレームワークを提供するため、組織がシステム障害発生時に復元プロセスを適切に管理するために必要です。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 7 章: 回復力と回復、325 ページ。

最新問題: **53**
ある組織が、コストと利益を主な要件とし、RTO と RPO の値が約 2 日である新しいバックアップ データ センターを構築しています。このシナリオに最適なサイトは次のうちどれですか。
A. リアルタイムリカバリ
B. ホット
C. 冷たい
D. 暖かい
Answer: (解答を表示する**)**
コールド サイトは、IT 運用をサポートするために必要なインフラストラクチャを備えているものの、事前構成されたハードウェアやソフトウェアを備えていないタイプのバックアップ データ センターです。コールド サイトは、バックアップ データ センター タイプの

中で最も安価なオプションですが、目標復旧時間 (RTO) と目標復旧ポイント (RPO) の値も最も長くなります。コールド サイトは、コスト メリットが主な要件であり、RTO と RPO の値がそれほど厳しくないシナリオに適しています。コールド サイトでは、災害発生後に通常の運用を回復するのに最大 2 日以上かかる場合があります。

最新問題: **54**
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
Answer: D (メーッセージを残す**)**
予防的 - 許容使用ポリシーは、会社のリソースを使用するためのルールをユーザーに強制します。
例: 会社 A では、自宅勤務時に会社のサーバー内のファイルにアクセスするには、会社の VPN に接続する必要があると規定しています。これにより、安全でないネットワークからの接続を防止できます。

最新問題: **55**
組織では単一のオペレーティング システムのバリエーションが多すぎるため、システム イメージをユーザーにプッシュする前に配置を標準化する必要があります。組織が最初に実装する必要があるのは次のうちどれですか。
A. 標準的な命名規則
B. マッシュ
C. ネットワーク図
D. ベースライン構成
Answer: D (メーッセージを残す**)**
ベースライン構成は、システムまたはネットワークの構成設定を標準化するプロセスです。このシナリオでは、組織はオペレーティング システムの構成を標準化してから、ネットワーク全体に展開する必要があります。ベースライン構成を確立すると、すべてのシステムが組織のセキュリティ ポリシーと運用要件に準拠することが保証されます。
参考資料 = CompTIA Security+ SY0-701 学習教材、特にシステム強化と構成管理の分野。

最新問題: **56**
セキュリティ インシデントが発生した後、システム管理者は会社に NAC プラットフォームの購入を依頼します。システム管理者が保護しようとしている攻撃対象領域は次のどれですか。
A. ブルートゥース
B. 有線
C. NFC

D. SCADA
Answer: (解答を表示する**)**
NAC (ネットワーク アクセス コントロール) プラットフォームは、ネットワークにアクセスしようとするデバイスにセキュリティ ポリシーを適用するテクノロジです。NAC プラットフォームは、デバイスの ID、役割、コンプライアンスを確認し、定義済みのルールに基づいてアクセスを許可または拒否できます。NAC プラットフォームは有線ネットワークと無線ネットワークの両方を保護できますが、このシナリオでは、システム管理者は有線攻撃対象領域を保護しようとしています。これは、ネットワークへの物理的な接続を通じて悪用される可能性のある一連の脆弱性です12。

最新問題**: 57**
次のインシデント対応活動のうち、証拠が適切に渡されることを保証するものはどれですか?
A. 電子証拠開示
B. 保管の連鎖
C. 法的保留
D. 保存
Answer: (解答を表示する**)**
証拠管理の連鎖とは、インシデント対応中に収集された証拠の完全性を文書化して保存するプロセスです。証拠を扱った各人の詳細、各転送の日時、証拠が保管された場所を記録します。証拠管理の連鎖により、証拠が法的手続きで許容され、その出所まで追跡できることが保証されます。電子証拠開示、法的保留、および保存は関連する概念ですが、証拠が適切に扱われることを保証するものではありません。参照: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、487 ページ、NIST SP 800-61: 3.2. 証拠の収集と処理

最新問題**: 58**
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。
Answer:
Web サーバー ボットネット DDoS 保護を有効にする
ユーザーRAT ホストベースのIPSを実装する
データベースサーバーワーム デフォルトのアプリケーションパスワードを変更する
エグゼクティブキーロガー 脆弱なサービスを無効にする
アプリケーションバックドア プッシュ通知を使用して2FAを実装する

最新問題**: 59**

システム管理者は、クラウドベースの低コストのアプリケーション ホスティング ソリューションを探しています。
次のどれがこれらの要件を満たしていますか?
A. タイプ 1 hvpervisor
B. サーバーレスフレームワーク
C. SD-WAN
D. SDN
Answer: B (メーッセージを残す**)**

最新問題**: 60**
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
Answer: A (メーッセージを残す**)**
PCI DSS は、Payment Card Industry Data Security Standard (PCI DSS) の略で、カード所有者データを保存、処理、または送信する組織に対する一連のセキュリティ要件です。PCI DSS は、カード所有者データの機密性、整合性、可用性を保護し、詐欺、個人情報の盗難、およびデータ侵害を防止することを目的としています。PCI DSS
は、Visa、Mastercard、American Express、Discover、JCB などのペイメント カード ブランドによって施行されており、販売業者、アクワイアラー、発行者、プロセッサ、サービス プロバイダ、および支払いアプリケーションなど、ペイメント カード エコシステムに関係するすべてのエンティティに適用されます。
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、最も可能性が高いのは、銀行がペイメント カード ブランドから罰金を科されることです。内部 PCI DSS コンプライアンス評価は、銀行が PCI DSS 要件への準拠を評価するために実行する自己評価です。銀行は、内部評価の結果をペイメント カード ブランドまたはその指定代理店 (アクワイアラーや認定セキュリティ評価機関 (QSA) など) に提出する必要があります。内部評価で銀行が PCI DSS 要件に準拠していないことが判明した場合、ペイメント カード ブランドは PCI DSS 契約違反のペナルティとして銀行に罰金を科すことがあります。罰金の額と頻度は、非準拠の重大性と期間、侵害されたカード所有者データの数と種類、銀行の協力と改善のレベルによって異なります。罰金は月額数千ドルから数百万ドルに及ぶ可能性があり、非準拠が解決されない場合は時間の経過とともに増加する可能性があります。
その他のオプションは、大手銀行が内部 PCI DSS コンプライアンス評価に不合格になった場合に最も起こり得る結果ではないため、正しくありません。
B) 監査結果。監査結果は、QSA または認定スキャン ベンダー (ASV) によって実行される外部 PCI DSS コンプライアンス評価の結果です。大量のカード所有者データを処理するか、非準拠の履歴がある特定のエンティティには、外部評価が必要です。外部評価は、セ

キュリティ インシデントまたはペイメント カード ブランドからの要求によってトリガーされる場合もあります。監査結果により、銀行のセキュリティ管理のギャップと弱点が明らかになり、コンプライアンスを達成するための是正措置が推奨される場合があります。ただし、監査結果は、銀行自体によって実行される内部評価の結果ではありません。C. 制裁。制裁は、銀行が罰金を支払わないか、PCI DSS 要件に準拠しない場合に、ペイメント カード ブランドが銀行に対して取る措置です。制裁には、罰金の増額、銀行のペイメント カードの受け入れまたは処理の停止または終了、銀行の PCI DSS 認定の取り消しなどが含まれます。制裁は内部評価の直接的な結果ではなく、長期にわたるまたは繰り返される非準拠の結果として生じる可能性があります。D. 評判の失墜。評判の失墜とは、銀行が内部 PCI DSS 準拠評価に合格しなかった場合に、顧客、パートナー、規制当局、および一般の人々から銀行が被る可能性がある信用と信用の喪失です。評判の失墜は、銀行のブランド イメージ、顧客ロイヤルティ、市場シェア、および収益性に影響を及ぼす可能性があります。評判の失墜は内部評価の直接的な結果ではなく、非準拠が悪意のある行為者によって暴露または悪用された場合に銀行が直面する可能性のある潜在的なリスクです。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 8 章: ガバナンス、リスク、およびコンプライアンス、388 ページ。Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 8.2: コンプライアンスとコントロール、ビデオ: PCI DSS (5:12)。PCI セキュリティ標準協議会、PCI DSS クイック リファレンス ガイド、4 ページ。PCI セキュリティ標準協議会、PCI DSS FAQ、質問 8。PCI セキュリティ標準協議会、PCI DSS FAQ、質問 9。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 10。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 11。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 12。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 13。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 14。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 15。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 16。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問 17。[PCI セキュリティ標準協議会]、PCI DSS FAQ、質問18. [PCI セキュリティ標準協議会]、PCI DSS よくある質問、質問 19. [PCI セキュリティ標準協議会]、PCI DSS よくある質問、質問 20. [PCI セキュリティ標準協議会]、PCI DSS よくある質問、質問 21. [PCI セキュリティ標準協議会]、PCI DSS よくある質問、質問 22. [PCI セキュリティ標準協議会]、PCI DSS よくある質問、質問 23. [PCI セキュリティ標準協議会]、PCI DSS よくある質問、質問 24. [PCI セキュリティ標準協議会]、PCI DSS に関する FAQ、質問 25. [PCI セキュリティ標準協議会]、PCI DSS に関する FAQ、質問 26. [PCI セキュリティ標準協議会]、PCI DSS に関する FAQ、質問 27. [PCI セキュリティ標準協議会]、PCI DSS に関する FAQ、質問 28. [PCI セキュリティ標準協議会]、PCI DSS に関する FAQ、質問 29. [PCI セキュリティ標準協議会]、PCI DSS に関する FAQ、質問 30. [PCI セキュリティ標準協議会]

最新問題**: 61**
セキュリティ マネージャーは、さまざまな種類のセキュリティ インシデントに対応するために使用する新しいドキュメントを作成しました。
マネージャーが次に取るべきステップは次のどれですか?

A. 最大データ保持ポリシーを設定します。
B. ドキュメントをエアギャップネットワーク上に安全に保存します。
C. ドキュメントのデータ分類ポリシーを確認します。
D. チームで卓上演習を実施します。
Answer: D (メーッセージを残す**)**
机上演習は、セキュリティ インシデント対応計画の有効性をテストするシミュレートされたシナリオです。関連する関係者を集め、計画の手順を順に実行し、対処が必要なギャップや問題を特定します。机上演習は、セキュリティ マネージャーが作成したドキュメントを検証し、チームがさまざまな種類のセキュリティ インシデントに備えられるようにするための優れた方法です。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 6 章: リスク管理、2841 ページ。CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 6 章: リスク管理、2842 ページ。

最新問題: **62**
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
Answer: A (メーッセージを残す**)**
作業明細書 (SOW) は、プロジェクトまたはサービスの範囲、目的、成果物、タイムライン、およびコストを定義するドキュメントです。通常、作業を完了するために必要な時間数の見積もり、および関係者の役割と責任が含まれます。SOW は、クライアントとベンダーの両方が、期待される内容と作業の実行方法について明確な相互理解を持つようにするために、侵入テスト プロジェクトでよく使用されます。ビジネス パートナーシップ契約 (BPA)、サービス レベル契約 (SLA)、および秘密保持契約 (NDA) は、侵入テスト プロジェクトに関連する可能性のあるさまざまなタイプの契約ですが、これらには、作業を完了するために必要な時間数の見積もりは含まれていません。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、492 ページ、侵入テストの作業明細書で注目すべき点

最新問題: **63**
システム管理者は、多数のエンド ユーザーのアカウント作成時に時間を節約し、人為的エラーを防ぐスクリプトを作成しています。このタスクに適した使用例はどれですか。
A. 市販ソフトウェア
B. オーケストレーション
C. ベースライン
D. ポリシーの適用
Answer: B (メーッセージを残す**)**
オーケストレーションは、さまざまなシステムやアプリケーション間で複数のタスクを自動化するプロセスです。定義済みのワークフローやスクリプトを実行することで、時間を節約し、人的エラーを減らすことができます。この場合、システム管理者はオーケストレーションを使用して、手動で情報を入力し、権限を割り当てることなく、多数のエンドユーザーのアカウントを作成できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、457 ページ 1

最新問題: **64**
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 Web 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、開発者が Web サイトに掲載する必要があるのは次のうちどれですか。
A. ハッシュ
B. 証明書
C. アルゴリズム
D. 塩漬け
Answer: A (メーッセージを残す**)**
ダウンロードしたファイルの整合性を確認するには、ソフトウェア開発者はハッシュを Web サイトに掲載する必要があります。ハッシュとは、ファイルなどの入力データから生成される固定長の文字列または数値です。ユーザーがアプリケーション ファイルをダウンロードするときに、ダウンロードしたファイルから独自のハッシュを生成し、開発者が提供したハッシュと比較することができます。ハッシュが一致すれば、ダウンロード プロセス中にファイルが変更または破損していないことが確認できます。
ハッシュ: ダウンロードしたファイルが元のファイルと同一であることをユーザーが確認できるようにすることで、データの整合性を確保します。一般的なハッシュ アルゴリズムには、MD5、SHA-1、SHA-256 などがあります。
証明書とアルゴリズム: ファイルの整合性を検証することよりも、信頼性を確保し、通信を保護することに関連しています。
ソルト: ファイルの整合性を検証するためではなく、セキュリティの層を追加するためにパスワードをハッシュするために使用される手法です。

最新問題: **65**
将来の参照のためにオフサイトの場所にログを記録するようにデバイスを構成する方法を最もよく説明しているのはどれですか?
A. ログの集約
B. DLP
C. アーカイブ
D. 最高司令官
Answer: A (メッセージを残す**)**
将来の参照に備えてオフサイトの場所にログを記録するようにデバイスを構成することを、ログ集約と表現するのが最も適切です。ログ集約では、複数のソースからログを収集し、それらを中央の場所 (多くの場合はオフサイト) に保存して、ログが確実に保存され、将来分析できるようにします。
ログの集約: 複数のデバイスからのログ データを一元管理することで、分析が容易になり、ログを将来参照できるようになります。
DLP (データ損失防止): 不正なデータ転送を防止し、データのセキュリティを確保することに重点を置いています。
アーカイブ: 長期保存のためにデータを保存することを含みます。これはログ集約の一部である可能性がありますが、範囲はより広範囲です。
SCAP (Security Content Automation Protocol): 脆弱性管理とポリシーコンプライアンスを自動化する標準。

最新問題: **66**
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。
Answer: A (メッセージを残す**)**
説明
ビジネスメール詐欺 (BEC) 攻撃は、会社の資金や機密情報にアクセスできる従業員をターゲットにしたフィッシング攻撃の一種です。攻撃者は、役員、ベンダー、顧客などの信頼できる人物になりすまし、不正な支払い、電信送金、機密データを要求します。攻撃者は、緊急性、圧力、親密さなどのソーシャルエンジニアリング手法を使用して、被害者に要求に応じるよう説得することがよくあります12。

このシナリオでは、オプション A は、BEC 攻撃の可能性を示しています。従業員は、メールの表示フィールドに役員の名前が記載されたメールでギフト カードのリクエストを受け取ります。メールは役員から送信されたように見えますが、実際のメール アドレスは偽装または侵害されている可能性があります。攻撃者は、従業員や顧客に報いるなどのビジネス目的でギフト カードが必要であると主張し、従業員にギフト カードを購入してコードを送信するように要求する可能性があります。これは、BEC 攻撃者が疑いを持たない被害者から金銭を盗むために使用する一般的な戦術です34。
オプション B は、悪意のあるソフトウェアがデバイス上のファイルを暗号化し、復号キーと引き換えに身代金を要求するランサムウェア攻撃の可能性について説明しています。オプション C は、資格情報収集攻撃の可能性について説明しています。資格情報収集攻撃は、攻撃者が正当な権限を装って特権アカウントのログイン情報を取得しようとします。オプション D は、フィッシング攻撃の可能性について説明しています。攻撃者は、企業のメールポータルを模倣した偽の Web サイトに被害者を誘導し、資格情報を取得しようとします。これらはすべてサイバー攻撃の一種ですが、BEC 攻撃の例ではありません。参考資料 = 1: ビジネス メール詐欺 - CompTIA Security+ SY0-701 -
2.2 2: CompTIA Security+ SY0-701 認定試験学習ガイド 3: ビジネスメール詐欺: 120 億ドルの詐欺 4: 合計: CompTIA Security+ 認定 (SY0-701) | Udemy

最新問題**: 67**
ソフトウェア開発マネージャーは、会社が作成したコードの信頼性を確保したいと考えています。次のオプションのうち、最も適切なものはどれですか。
A. ユーザー入力フィールドの入力検証をテストする
B. 自社開発ソフトウェアのコード署名の実行
C. ソフトウェアの静的コード解析を実行する
D. 安全なCookieが使用されていることを確認する
Answer: B (メーッセージを残す**)**
コード署名は、企業が作成したコードの信頼性と整合性を暗号化を使用して検証する手法です。コード署名では、企業のみが所有する秘密キーを使用してコードにデジタル署名を適用します。デジタル署名は、信頼できる証明機関を通じて配布できる対応する公開キーを持つ人なら誰でも検証できます。コード署名により、コードへの不正な変更、改ざん、マルウェアの挿入を防ぐことができ、また、コードが正当なソースからのものであることをユーザーに保証できます。

最新問題**: 68**
ある企業が、社内ネットワークから発信される DNS トラフィックを制限しようとしています。発信 DNS 要求は、IP アドレス 10.50.10.25 を持つ 1 つのデバイスからのみ許可されます。次のファイアウォール ACL のどれがこの目的を達成しますか。
A. アクセスリスト アウトバウンド許可 0.0.0.0 0 0.0.0.0/0 ポート 53 アクセスリスト アウトバウンド拒否 10.50.10.25 32 0.0.0.0
/0 ポート 53

B. アクセスリスト アウトバウンド許可 0.0.0.0/0 10.50.10.25 32 ポート 53 アクセスリスト アウトバウンド拒否 0.0.0.0 0 0.0.0.0
/0 ポート 53
C. アクセスリスト アウトバウンド許可 0.0.0.0 0 0.0.0.0/0 ポート 53 アクセスリスト アウトバウンド拒否 0.0.0.0/0 10.50.10.25
32 ポート 53
D. アクセスリスト アウトバウンド許可 10.50.10.25 32 0.0.0.0/0 ポート 53 アクセスリスト アウトバウンド拒否 0.0.0.0.0.0.0.0
/0 ポート 53
Answer: D (メーッセージを残す)
正解は D です。これは、IP アドレスが 10.50.10.25 のデバイスのみがポート 53 でアウトバウンド DNS 要求を送信できるようにし、他のすべてのデバイスがこれを拒否するためです。他のオプションは、すべてのデバイスがアウトバウンド DNS 要求を送信できるようにしている (A と C) か、どのデバイスもアウトバウンド DNS 要求を送信できない (B) ため、不正解です。参考資料 = ファイアウォール ACL と DNS の詳細については、次のリソースを参照してください。
* CompTIA Security+ SY0-701 認定試験学習ガイド、第 4 章: ネットワーク セキュリティ 1
* メッサー教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 3.2: ファイアウォール ルール 2
* 合計: CompTIA Security+ Cert (SY0-701) | Udemy、セクション 6: ネットワーク セキュリティ、講義 28:
ファイアウォールルール3

最新問題**: 69**
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
Answer: D (メーッセージを残す)
このシナリオでは、攻撃者が侵害されたシステムのメモリから資格情報を取得し、クラッキングせずにそれを使用してネットワーク内を横方向に移動する様子が描かれています。この手法は「pass-the-hash」攻撃と呼ばれ、攻撃者はハッシュされた資格情報 (例: NTLM ハッシュ) を取得し、それを使用してプレーンテキストのパスワードを知らなくても他のシステムへの認証とアクセスを行います。これは、セキュリティ対策が脆弱な環境や古いプロトコルが使用されている環境でよく見られる攻撃方法です。
参考文献

* CompTIA Security+ SY0-701 コース内容: このコースでは、パスザハッシュなどの資格情報ベースの攻撃について説明し、その影響と資格情報ストアの保護の重要性を強調します。

最新問題: **70**
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. 塩漬け
Answer: D (メーッセージを残す**)**
ソルトとは、ハッシュ関数などの一方向データ変換アルゴリズムを適用する前に、パスワードやその他のデータにランダムなデータを追加するプロセスです。ソルトにより、入力データの複雑さとランダム性が増し、攻撃者が事前に計算されたテーブルやブルートフォース メソッドを使用して元のデータを推測したり解読したりすることが難しくなります。また、ソルトは、同一のパスワードから同一のハッシュ値が生成されるのを防ぐのにも役立ちます。ハッシュ値が生成されてしまうと、ハッシュ データにアクセスできる攻撃者にパスワードが漏れてしまう可能性があります。ソルトは、データベースに保存されているパスワードやネットワーク経由で送信されるパスワードを保護するためによく使用されます。

最新問題: **71**
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は、IP アドレスが組織のネットワークにアクセスするの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どれですか。
A. アクセスリスト インバウンド 拒否 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
B. アクセスリスト インバウンド 拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
C. アクセスリスト インバウンド 許可 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
D. アクセスリスト インバウンド 許可 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
Answer: B (メーッセージを残す**)**
ファイアウォールルールは、パケットがファイアウォールを通過することを許可するか拒否するかを決定する一連の基準です。ファイアウォールルールは、アクション、プロトコル、送信元アドレス、宛先アドレス、ポート番号などのいくつかの要素で構成されます。ファイアウォールルールの構文は、ファイアウォールの種類とベンダーによって異なる場合がありますが、基本的なロジックは同じです。この質問では、セキュリティアナリストは、IPアドレス10.1.4.9が組織のネットワークにアクセスするのをブロックする受信ファイ

アウォールルールを作成しています。つまり、アクションは拒否、プロトコルは任意（IPの場合はig）、送信元アドレスは
10.1.4.9/32 (単一の IP アドレスを意味します)、宛先アドレスは 0.0.0.0/0 (任意の IP アドレスを意味します)、ポート番号は任意である必要があります。したがって、正しいファイアウォール ルールは次のようになります。
アクセスリスト 受信拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
このルールは、送信元 IP アドレスが 10.1.4.9 であるすべてのパケットに一致し、それをドロップします。その他のオプションは、アクション、送信元アドレス、または宛先アドレスが間違っているため、正しくありません。たとえば、オプション A では送信元アドレスと宛先アドレスが逆になっているため、宛先 IP アドレスが 10.1.4.9 であるすべてのパケットがブロックされますが、これは本来の目的ではありません。オプション C ではアクションが間違っており、許可になっています。つまり、パケットがファイアウォールを通過できるようになりますが、これも本来の目的ではありません。オプション D には、送信元アドレスと宛先アドレスが逆になっているため、オプション A と同じ問題があります。
参考資料 = ファイアウォールルール - CompTIA Security+ SY0-401: 1.2、ファイアウォール - SY0-601 CompTIA Security+:
3.3、ファイアウォール - CompTIA Security+ SY0-501、ファイアウォール ルールの理解 - CompTIA Network+ N10-005: 5.5、Windows ファイアウォールの構成 - CompTIA A+ 220-1102 - 1.6。

最新問題**: 72**
運用サーバーに影響を与えずに潜在的な攻撃者の活動を特定するために使用できるのは次のうちどれですか?
A. ハニーポット
B. ビデオ監視
C. ゼロトラスト
D. ジオフェンシング
Answer: A (メーッセージを残す**)**
ハニーポットとは、実際の運用サーバーを模倣し、潜在的な攻撃者を引き付けるように設計されたシステムまたはネットワークです。ハニーポットを使用すると、実際の運用サーバーに影響を与えることなく、攻撃者の方法、テクニック、目的を特定できます。また、ハニーポットは、攻撃者の注意を実際のターゲットからそらし、時間とリソースを無駄にすることもできます12。
その他のオプションは、運用サーバーに影響を与えずに潜在的な攻撃者の活動を特定する効果的な方法ではありません。
ビデオ監視: これは、カメラとモニターを使用して特定のエリアでの活動を記録および観察する物理的なセキュリティ技術です。ビデオ監視は、物理的な侵入を阻止、検出、調査するのに役立ちますが、ネットワークまたはサーバーでの攻撃者の活動を直接特定することはできません3。

ゼロ トラスト: これは、デフォルトではどのユーザー、デバイス、またはネットワークも信頼できないと想定し、すべてのリクエストとトランザクションに対して厳格な検証と検証を要求するセキュリティ戦略です。ゼロ トラストは、セキュリティ体制を改善し、組織の攻撃対象領域を減らすのに役立ちますが、ネットワークまたはサーバー上での攻撃者の活動を直接特定するものではありません4。
ジオフェンシング: これは、地理的位置を基準としてデータやリソースへのアクセスを制限または許可するセキュリティ技術です。ジオフェンシングは、組織のデータ主権とコンプライアンスを保護するのに役立ちますが、ネットワークまたはサーバー上での攻撃者の活動を直接特定することはできません5。
参考資料 = 1: CompTIA Security+ SY0-701 認定試験学習ガイド、542 ページ: ハニーポットと欺瞞
- SY0-601 CompTIA Security+: 2.1、メッサー教授によるビデオ3: CompTIA Security+ SY0-701 認定試験学習ガイド、974 ページ: CompTIA Security+ SY0-701 認定試験学習ガイド、985 ページ:
CompTIA Security+ SY0-701 認定試験学習ガイド、99 ページ。

最新問題**: 73**
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。
Answer: C (メーッセージを残す**)**
SMS OTP (ワンタイム パスワード) 方式は、TOTP (時間ベースのワンタイム パスワード) に比べて傍受に対して脆弱です。これは、SMS メッセージは、SIM スワッピングや SMS フィッシングなどのさまざまな攻撃ベクトルを通じて傍受される可能性があるためです。一方、TOTP はデバイス上で直接コードを生成し、SMS などの通信チャネルに依存しないため、傍受される可能性が低くなります。
参考資料 = CompTIA Security+ SY0-701 学習教材、特に ID およびアクセス管理の分野。

最新問題**: 74**
監査後、管理者はすべてのユーザーがファイル サーバー上の機密データにアクセスできることを発見しました。管理者は、データへのアクセスを迅速に制限するために、次のどれを使用する必要がありますか。
A. グループ ポリシー

B. コンテンツフィルタリング
C. データ損失防止
D. アクセス制御リスト
Answer: D (メーッセージを残す**)**
アクセス制御リスト (ACL) は、ファイル サーバー上のどのリソースにどのユーザーまたはグループがアクセスできるかを指定するルールです。ユーザーの ID またはロールに基づいて権限を付与または拒否することで、機密データへのアクセスを制限することができます。この場合、管理者は ACL を使用してユーザーのアクセス権をすばやく変更し、ユーザーが表示を許可されていないデータにアクセスできないようにすることができます。

最新問題**: 75**
絶えず変化する環境に最も適しているのはどれでしょうか?
A. RTOS
B. コンテナ
C. 組み込みシステム
D. SCADA
Answer: B (メーッセージを残す**)**
コンテナは、アプリケーションを独自の依存関係、ライブラリ、および構成を持つ分離された環境で実行できるようにする仮想化の方法です。コンテナは軽量で、移植性があり、拡張性があり、展開と更新が容易であるため、常に変化する環境に最適です。また、コンテナはマイクロサービス アーキテクチャをサポートできるため、ソフトウェア機能をより迅速かつ頻繁に提供できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 10 章: モバイル デバイス セキュリティ、512 ページ 1

最新問題**: 76**
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るでしょうか。
（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
Answer: (解答を表示する**)**
スミッシングは、テキスト メッセージ (SMS) を使用して被害者を騙し、機密情報を漏らしたり、悪意のあるリンクをクリックさせたり、マルウェアをダウンロードさせたりするためのソーシャル エンジニアリング手法の一種です。スミッシング メッセージは、銀行、政府機関、サービス プロバイダーなどの正当なソースから送信されたように見えることが多

く、緊急または脅迫的な言葉を使用して受信者に行動を起こさせようとします12。このシナリオでは、給与部門からのテキスト メッセージであると主張するテキスト メッセージは、スミッシングの一例です。
なりすましは、権威のある人物、信頼できる人物、同僚など、別の人物になりすまして、ターゲットの信頼や協力を得るというソーシャル エンジニアリング手法の一種です。なりすましは、電話、メール、テキスト メッセージ、直接の訪問など、さまざまなチャネルを通じて実行され、被害者から情報、アクセス、または金銭を取得するために使用されます34。このシナリオでは、給与部門からのテキスト メッセージになりすましたものがなりすましの例です。
A: タイポスクワッティングは、人気のあるウェブサイトやよく知られているウェブサイトに似ているが、意図的にスペルミスや異なる拡張子を持つドメイン名を登録するサイバー攻撃の一種です。タイポスクワッティングは、ユーザーがウェブアドレスを入力する際に犯す一般的な間違いを悪用し、悪意のあるサイトや詐欺サイトにユーザーをリダイレクトして、情報を盗んだり、マルウェアをインストールしたり、広告を表示したりすることを目的としています56。タイポスクワッティングは、テキストメッセージや資格情報の検証とは関係ありません。
B: フィッシングは、ソーシャル エンジニアリング手法の一種で、詐欺メールを使用して受信者を騙し、機密情報を開示させたり、悪意のあるリンクをクリックさせたり、マルウェアをダウンロードさせたりします。フィッシング メールは、銀行、小売業者、サービス プロバイダーなどの正当な組織の外観や口調を模倣することが多く、欺瞞的または緊急の言葉を使用して受信者に行動を起こさせます78。フィッシングは、テキスト メッセージや資格情報の検証とは関係ありません。
D: ビッシングはソーシャル エンジニアリングの手法の一種で、音声通話を利用して被害者を騙し、パスワード、クレジットカード番号、銀行口座の詳細などの機密情報を漏らします。ビッシングの電話は、法執行機関、政府機関、テクニカル サポートなどの正当なソースから発信されたように見えることが多く、脅迫や偽りの約束を使って受信者に従わせようとします。ビッシングは、テキスト メッセージや認証情報の確認とは関係ありません。
E: 誤情報は、虚偽または誤解を招く情報を広めて、対象の信念、意見、または行動に影響を与えるソーシャル エンジニアリング手法の一種です。誤情報は、世論を操作したり、混乱を引き起こしたり、評判を傷つけたり、議題を推進したりするために使用される可能性があります。誤情報は、テキスト メッセージや資格情報の検証とは関係ありません。
参考資料 = 1: スミッシングとは? | 定義と例 | Kaspersky 2: スミッシング - Wikipedia 3: なりすまし攻撃とは何か、また、それに対してどのように防御するか? 4: なりすまし - Wikipedia 5: タイポスクワッティングとは? | 定義と例 | Kaspersky 6: タイポスクワッティング - Wikipedia 7: フィッシングとは? | 定義と例 | Kaspersky 8: フィッシング - Wikipedia 9: ヴィッシングとは? | 定義と例 | Kaspersky : ヴィッシング - Wikipedia : 誤情報とは? | 定義と例 | Britannica : 誤情報 - Wikipedia

最新問題: **77**
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
Answer: D (メーッセージを残す**)**
ホエーリングは、企業の重役、著名人、政治家などの著名人をターゲットにしたフィッシング攻撃の一種です。攻撃者は権威や影響力のある人物になりすまし、被害者を騙して金銭の送金、機密情報の漏洩、悪意のあるリンクのクリックなどのアクションを実行させようとします。ホエーリングは、CEO 詐欺やビジネス メール詐欺とも呼ばれます2。

最新問題: **78**
次の脆弱性のうち、製造元が承認したソフトウェア リポジトリの外部にソフトウェアをインストールすることに関連しているのはどれですか。
A. 脱獄
B. メモリインジェクション
C. リソースの再利用
D. サイドローディング
Answer: (解答を表示する**)**
サイドローディングとは、製造元が承認したソフトウェア リポジトリの外部にソフトウェアをインストールするプロセスです。
これにより、デバイスがマルウェア、スパイウェア、不正アクセスなどの潜在的な脆弱性にさらされる可能性があります。
サイドローディングは、製造元または組織によって強制されているセキュリティ制御とポリシーを回避することもできます。サイドローディングは、デバイスで利用できない、または許可されていないアプリケーションや機能にアクセスしたいユーザーによって行われることがよくあります。参考資料 = サイドローディング - CompTIA Security + ビデオトレーニング | インターフェイス技術トレーニング、Security+ (Plus) 認定 | CompTIA IT 認定、ロードバランサー - CompTIA Security+ SY0-501 - 2.1、CompTIA Security+ SY0-601 認定学習ガイド。

最新問題: **79**
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
Answer: (解答を表示する**)**
リスク レジスタは、プロジェクト、システム、または組織に関連するリスクを記録して追跡するドキュメントです。リスク レジスタには通常、リスクの説明、リスクの所有者、リスクの可能性、リスクの影響、リスク レベル、リスク対応戦略、リスクの状態などの情報が含まれます。リスク レジスタは、リスクの特定、評価、優先順位付け、監視、および制御、ならびに関連する利害関係者への伝達に役立ちます。リスク レジスタは、組織のリスク許容度としきい値 (リスクにさらされる許容レベルと、リスクをエスカレーションまたは軽減するための基準) を文書化するのに役立てることもできます。参照 = CompTIA Security+ 認定試験の目標、ドメイン 5.1: 組織のセキュリティに関連するポリシー、計画、および手順の重要性を説明する。CompTIA Security+ 学習ガイド (SY0-701)、第 5 章: ガバナンス、リスク、コンプライアンス、211 ページ。CompTIA Security+ 認定ガイド、第 2 章: リスク管理、33 ページ。CompTIA Security+ 認定試験 SY0-701 模擬試験 1、質問 4。

最新問題: **80**
次のベスト プラクティスのうち、可用性を確保し、ビジネスへの影響を最小限に抑えるために、管理者が運用システムに変更を加えるための一定期間を与えるものはどれですか。
A. 影響分析
B. 予定されたダウンタイム
C. バックアウト計画
D. 変更管理委員会
Answer: B (メーッセージを残す**)**
スケジュールされたダウンタイムとは、メンテナンス、更新、アップグレード、その他の変更のためにシステムまたはサービスが利用できない予定の期間です。スケジュールされたダウンタイムにより、管理者は、通常の業務を中断したり、システムまたはサービスの可用性に影響を与えたりすることなく、運用システムに変更を加えるための一定の期間を確保できます。また、スケジュールされたダウンタイムにより、管理者は、変更の予想される期間と影響についてユーザーと関係者に通知できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 12 章: セキュリティ運用と管理、579 ページ 1

最新問題: **81**
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
Answer: (解答を表示する**)**
アーキテクチャのセキュリティとは、ビジネスの目的と要件を満たす安全なインフラストラクチャを設計および実装するプロセスです。クラウド コンピューティングなどのオフプレミス ソリューションに移行する場合は、まずアーキテクチャのセキュリティを検討する必要があります。これは、データ セキュリティ、コンプライアンス、可用性、スケーラビリティ、パフォーマンスなど、移行に関連する潜在的なリスクと課題を特定して軽減するのに役立つためです。アーキテクチャのセキュリティは、ビジネスのセキュリティと運用のニーズを満たすことができる信頼できるクラウド サービス プロバイダーを評価して選択するプロセスであるクラウド プロバイダーのセキュリティとは異なります。アーキテクチャのセキュリティは、インフラストラクチャをクラウドに移行して維持するために必要な金額である実装コストとも異なります。アーキテクチャのセキュリティは、クラウド インフラストラクチャの移行と管理を担当する IT スタッフのスキルと知識のレベルであるエンジニアの能力とも異なります。

最新問題: **82**
レガシー アプリケーションがビジネス運営に不可欠であり、予防的制御がまだ実装されていない場合、企業はまず次のどのリスク管理戦略を採用すべきでしょうか。
A. 軽減
B. 受け入れる
C. 転送
D. 避ける
Answer: A (メーッセージを残す**)**
軽減は、リスクの発生可能性や影響を軽減するリスク管理戦略です。レガシー アプリケーションが業務運営に不可欠であり、予防的コントロールがまだ実装されていない場合、企業はまず軽減戦略を採用して、アプリケーションの既存の脆弱性とギャップに対処する必要があります。これには、アプリケーションへのパッチ、更新、または構成変更の適用、またはアプリケーションの周囲にセキュリティ コントロールのレイヤーの追加が含まれる場合があります。受け入れ、転送、回避もリスク管理戦略ですが、このシナリオでは最適なオプションではありません。受け入れとは、リスクを認識し、何もせずに結果を受け入れることです。転送とは、保険会社やベンダーなどのサード パーティにリスクを移すことです。回避とは、リスクの原因を取り除くかプロセスを変更することでリスクを排除することです。これらの戦略は、業務運営に不可欠であり、予防的コントロールが実装されていないレガシー アプリケーションでは実行可能または望ましくない可能性があります。参照: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、1221 ページレガシーシステムの移行と廃止のためのリスクベースのフレームワーク2

最新問題: **83**

セキュリティ管理者は、従業員のラップトップ上のデータを保護したいと考えています。セキュリティ管理者は次のどの暗号化手法を使用する必要がありますか?

A. パーティション

B. 非対称

C. ディスクがいっぱい

D. データベース

Answer: C (メーッセージを残す**)**

フルディスク暗号化 (FDE) は、オペレーティングシステム、アプリケーション、ファイルなど、ハードドライブ上のすべてのデータを暗号化する技術です。FDE は、ラップトップが紛失、盗難、または適切なサニタイズを行わずに廃棄された場合に、不正アクセスからデータを保護します。FDE では、ドライブのロックを解除してシステムを起動するために、ユーザーはパスワード、PIN、スマートカード、または生体認証要素を入力する必要があります。FDE は、BitLocker、FileVault、VeraCrypt などのソフトウェアソリューション、または自己暗号化ドライブ (SED) や Trusted Platform Modules (TPM) などのハードウェアソリューションを使用して実装できます。FDE は、機密データを保存するラップトップやその他のモバイルデバイスに推奨される暗号化技術です。

パーティション暗号化は、ハード ドライブ上の特定のパーティションまたはボリュームのみを暗号化し、ドライブの残りの部分は暗号化しない技術です。パーティション暗号化は、ドライブ全体を保護せず、暗号化されていない領域にデータの痕跡が残る可能性があるため、FDE よりも安全性が低くなります。パーティション暗号化は、ユーザーが暗号化されたパーティションを手動でマウントおよびマウント解除する必要があるため、FDE よりも使い勝手が悪くなります。

非対称暗号化は、公開キーと秘密キーのペアを使用してデータを暗号化および復号化する手法です。非対称暗号化は、保存データの暗号化ではなく、電子メール、Web、VPN などの通信のセキュリティ保護に主に使用されます。また、非対称暗号化は、FDE やパーティション暗号化で使用されるタイプの暗号化である対称暗号化よりも遅く、計算量が多くなります。

データベース暗号化は、テーブル、列、行、セルなど、データベースに保存されているデータを暗号化する手法です。データベース暗号化は、アプリケーション レベル、データベース レベル、またはファイル システム レベルで実行できます。データベース暗号化は、データベース管理者、ハッカー、またはマルウェアによる不正アクセスからデータを保護するのに便利ですが、データベースをホストするデバイスの物理的な盗難や紛失からデータを保護することはできません。

参考資料 = データ暗号化 - CompTIA Security+ SY0-401: 4.4、CompTIA Security+ チートシートと PDF | Zero To Mastery、CompTIA Security+ SY0-601 認定コース - Cybr、アプリケーション強化 - SY0-601 CompTIA Security+: 3.2。

最新問題: 84

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に接続された Web サイトが侵害されました。
将来同様の攻撃から組織を最も効果的に保護するために、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
Answer: B (メーッセージを残す**)**
バッファ オーバーフローは、アプリケーションがメモリ バッファに保持できる以上のデータを書き込むと発生するソフトウェア脆弱性の一種で、超過したデータによって隣接するメモリ位置が上書きされます。これにより、クラッシュ、エラー、コード実行などの予期しない動作が発生する可能性があります。バッファ オーバーフローは、攻撃者が悪意のあるコードやコマンドをアプリケーションに挿入するために悪用される可能性があり、システムのセキュリティと機能が侵害される可能性があります。組織のインターネットに面した Web サイトは、攻撃者がバッファ オーバーフローを悪用したときに侵害されました。今後同様の攻撃から組織を保護するには、Web アプリケーション ファイアウォール (WAF) を導入する必要があります。WAF は、Web アプリケーションとインターネット間のトラフィックを監視およびフィルタリングするファイアウォールの一種です。WAF は、バッファ オーバーフロー、SQL インジェクション、クロスサイト スクリプティング (XSS) などの一般的な Web 攻撃を検出してブロックできます。また、WAF は、入力検証、出力エンコード、暗号化などのセキュリティ ポリシーとルールを適用することもできます。WAF は、Web アプリケーションに保護レイヤーを提供し、攻撃者が脆弱性を悪用してデータを侵害するのを防ぎます。参考資料 = バッファ オーバーフロー - CompTIA Security+ SY0-701 - 2.3、Web アプリケーション ファイアウォール - CompTIA Security+ SY0-701 - 2.4、[500 以上の練習テスト問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版]

最新問題**: 85**
セキュリティ アナリストがアプリケーション サーバーを調査しているときに、サーバー上のソフトウェアが異常な動作をしていることを発見しました。このソフトウェアは通常、バッチ ジョブをローカルで実行し、トラフィックを生成しませんが、プロセスがランダムな高ポートを介して送信トラフィックを生成しています。このソフトウェアで悪用された可能性のある脆弱性は次のどれですか。
A. メモリインジェクション
B. 競合状態
C. サイドローディング
D. SQLインジェクション
Answer: (解答を表示する**)**

メモリ インジェクションの脆弱性により、ソフトウェア プログラム内で不正なコードやコマンドが実行され、ランダムな高ポート経由で送信トラフィックが生成されるなどの異常な動作が発生します。この問題は、ソフトウェアが入力を適切に検証またはエンコードしていないために発生することが多く、攻撃者が悪意のあるコードを挿入するために悪用される可能性があります。
参考: CompTIA Security+ SY0-701 コース コンテンツと公式 CompTIA 学習リソース。

最新問題: **86**
ある企業では、廃棄したシステムをリサイクルに送る前に、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す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
Answer: B (メーッセージを残す**)**
説明
サニタイズとは、ストレージ デバイスまたはシステムを廃棄または再利用する前に、機密データを削除するプロセスです。サニタイズは、データをランダム パターンまたはゼロで上書きして回復不能にするソフトウェア ツールまたはハードウェア デバイスを使用して実行できます。サニタイズは、ストレージ デバイスを物理的に損傷して使用不能にする破壊とは異なります。また、サニタイズは、ネットワーク リソースまたはデバイスを識別する列挙や、資産とその場所を追跡するインベントリとも異なります。廃棄されたシステムをリサイクルに送る前にハード ドライブを安全に消去するというポリシーは、リサイクルされたデバイスから機密データを取得できないようにするため、サニタイズの一例です。参考資料 = 安全なデータ破壊 - SY0-601 CompTIA Security+: 2.7、ビデオ 1:00、CompTIA Security+ SY0-701 認定学習ガイド、387 ページ。

最新問題: **87**
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
Answer: (解答を表示する**)**
VPN アプライアンスのローカル管理者アカウントのデフォルト パスワードを変更することは、リモート管理インターフェイスへの予期しないログインを防止できる基本的なセキュリティ対策です。デフォルト パスワードは推測しやすいか公開されていることが多

く、攻撃者はそれを使用してデバイスやシステムに不正にアクセスできます。デフォルト パスワードを強力で一意のパスワードに変更すると、ブルート フォース攻撃や資格情報の盗難のリスクが軽減されます。最小限の権限の使用、個別のユーザー ID の割り当て、ログの頻繁な確認もセキュリティ対策として有効ですが、予期しないログインを防止するには、デフォルト パスワードの変更ほど効果的ではありません。参考資料: CompTIA Security + 学習ガイド: 試験 SY0-701、第 9 版、116 ページ、ローカル管理者アカウント - セキュリティ リスクとベスト プラクティス (パート 1)

最新問題: **88**
ユーザーに証明書が提示されたときに、証明書を検証するために使用されるのは次のどれですか?
A. OCSP
B. CSR
C. カナダ
D. CRC
Answer: A (メーッセージを残す**)**
OCSP は、Online Certificate Status Protocol の略です。これは、アプリケーションが証明書の失効ステータスをリアルタイムで確認できるようにするプロトコルです。これは、失効した証明書のデータベースを管理するサーバーである OCSP レスポンダーにクエリを送信することで機能します。OCSP レスポンダーは、証明書が有効か、失効しているか、不明かを示す応答を返します。
OCSP は、証明書失効リスト (CRL) をダウンロードして解析するよりも高速かつ効率的です。CRL は、証明機関 (CA) によって発行されたすべての失効した証明書のシリアル番号を含む大きなファイルです。

最新問題: **89**
ある会社のベンダーがアナリストに BIOS アップデートを推奨するセキュリティ情報を送信しました。パッチによって対処される脆弱性の種類は次のどれですか。
A. 仮想化
B. ファームウェア
C. アプリケーション
D. オペレーティング システム
Answer: B (メーッセージを残す**)**
ファームウェアは、BIOS、ルーター、プリンター、カメラなどのハードウェア デバイスに組み込まれているソフトウェアの一種です。ファームウェアはデバイスの基本的な機能と操作を制御し、アップデートやパッチ適用によってバグを修正したり、パフォーマンスを改善したり、セキュリティを強化したりすることができます。ファームウェアの脆弱性とは、ファームウェア コードの欠陥または弱点のことで、攻撃者がこれを悪用すると不正アクセスや設定の変更、デバイスやネットワークへの損害を引き起こす可能性があります。BIOS アップデートは、コンピューターの基本入出力システム (オペレーティング システムの起

動とハードウェアとソフトウェア間の通信の管理を担う) のファームウェアの脆弱性に対処するパッチです。その他のオプションは脆弱性の種類ではなく、ソフトウェアまたはテクノロジのカテゴリです。

最新問題: **90**
数人の従業員が、最高経営責任者 (CEO) を名乗る人物から詐欺のテキスト メッセージを受け取りました。メッセージには次のように書かれていました。
「私は今、空港にいて、メールにアクセスできません。従業員表彰賞用のギフト カードを購入していただく必要があります。ギフト カードを次のメール アドレスに送ってください。」
この状況に対する最適な対応は次のうちどれですか。(2 つ選択してください)。
A. 現在の従業員表彰ギフトカードをキャンセルします。
B. 毎年の社内研修にスミッシング演習を追加します。
C. 会社全体に電子メールによる警告を発行します。
D. CEO に電話番号を変更してもらいます。
E. CEO の電話のフォレンジック調査を実施します。
F. モバイル デバイス管理を実装します。
Answer: B,C (メーッセージを残す)
説明
この状況はスミッシングの一例です。スミッシングは、テキスト メッセージ (SMS) を使用して個人を誘導し、個人情報や機密情報をサイバー犯罪者に提供させるフィッシングの一種です。この状況に対する最善の対応は、年次の企業トレーニングにスミッシング演習を追加し、会社に一般的な電子メール警告を発行することです。スミッシング演習は、スミッシング攻撃を認識して回避する方法を従業員に教育し、意識を高めるのに役立ちます。電子メール警告は、従業員に不正なテキスト メッセージがあることを警告し、情報や金銭の要求の身元と正当性を確認するよう思い出させます。参考資料 = フィッシングとは | サイバーセキュリティ | CompTIA、フィッシング - SY0-601 CompTIA Security+: 1.1 - Professor Messer IT 認定トレーニング コース

最新問題: **91**
次の契約タイプのうち、ベンダーが応答する必要がある時間枠を定義するのはどれですか?
A. 種をまく
B. SLA
C. モア
D. 覚書
Answer: (解答を表示する)
説明
サービス レベル契約 (SLA) は、サービス プロバイダーと顧客の間の期待と責任を定義する契約の一種です。通常、サービスの品質、可用性、パフォーマンス メトリック、およびプロバイダーがサービス要求、インシデント、苦情に対応する必要がある時間枠が含まれま

す。SLA は、顧客が希望するレベルのサービスを受けられるようにし、プロバイダーが合意された基準を満たす責任を負うようにするのに役立ちます。
参考文献:
Security+ (Plus) 認定 | CompTIA IT 認定、 試験について」の箇条書き 3:
「ガバナンス、リスク、コンプライアンスの原則を含む、適用される規制とポリシーを認識して運用します。」CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 1 章、14 ページ: 「サービス レベル契約 (SLA) は、サービス プロバイダーと顧客の間で締結される契約であり、サービス プロバイダーに期待されるサービスのレベルを指定します。」

最新問題: **92**
内部者が企業の開発プロセスに悪意のあるコードを持ち込むのを防ぐには、次のどの方法が最適ですか?
A. 脆弱性のコードスキャン
B. オープンソースコンポーネントの使用
C. 品質保証テスト
D. ピアレビューと承認
Answer: (解答を表示する**)**
ピア レビューと承認とは、コードを展開またはリリースする前に、他の開発者や専門家にコードをレビューしてもらうことです。ピア レビューと承認は、開発プロセスにおける悪意のあるコード、エラー、バグ、脆弱性、品質の低さを検出して防止するのに役立ちます。また、ピア レビューと承認により、コーディング標準、ベスト プラクティス、コンプライアンス要件を強制することもできます。ピア レビューと承認は、手動で行うことも、コード分析、コード レビュー、コード署名などのツールを利用して行うこともできます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 11 章: セキュア アプリケーション開発、543 ページ 2

最新問題: **93**
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
Answer: A (メーッセージを残す)
ホストベースのファイアウォールは、個々のエンドポイントで実行され、一連のルールに基づいて受信および送信ネットワーク トラフィックをフィルタリングするソフトウェア アプリケーションです。ホストベースのファイアウォールは、送信元、送信先、ポート、プロトコル、またはアプリケーションに基づいてトラフィックをブロックまたは許可することで、内部エンドポイント間の疑わしい接続によってもたらされる脅威を軽減するのに役立ちます。ホストベースのファイアウォールは、SQL インジェクション、クロスサイト スクリプティング、セッション ハイジャックなどの一般的な Web ベースの攻撃から Web アプリケーションを保護するファイアウォールの一種である Web アプリケーション ファイアウォールとは異なります。また、ホストベースのファイアウォールは、ファイル、フォルダー、プリンター、ルーターなどのネットワーク リソースへのアクセスを制御するルールのリストであるアクセス制御リストとも異なります。ホストベースのファイアウォールは、エンドポイントでの実行が許可されているアプリケーションのリストであるアプリケーション許可リストとも異なり、許可されていないアプリケーションや悪意のあるアプリケーションの実行を防ぎます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、254 ページ

最新問題**: 94**
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. 暗号化=オフ\
B. http://
C. www.*.com
D. :443
Answer: B (メーッセージを残す)
Web フィルターは、定義済みのルールやポリシーに基づいて Web トラフィックを監視、ブロック、または許可できるデバイスまたはソフトウェアです。Web フィルタリングの一般的な方法の 1 つは、URL をスキャンして文字列を検索し、一致する文字列が見つかった場合にアクセスを拒否することです。たとえば、Web フィルターは、URL に 「ギャンブル」、「ポルノ」、または 「マルウェア」という単語が含まれる Web サイトへのアクセスをブロックできます。URL は、Web リソースの場所とプロトコルを識別するユニフォーム リソース ロケーターです。URL は通常、protocol://domain:port/path?query#fragment というコンポーネントで構成されます。プロトコルは、HTTP、HTTPS、FTP、SMTP など、Web リソー

スへのアクセスに使用される通信方法を指定します。ドメインは、www.google.com や www.bing.com など、Web リソースをホストする Web サーバーの名前です。ポートは、Web サーバーで実行されている特定のサービスまたはアプリケーションを識別するオプションの番号で、HTTP の場合は 80、HTTPS の場合は 443 です。パスは、/index.html や /images/logo.png などの Web リソースの特定のフォルダーまたはファイル名です。クエリは、?q=security や ?lang=en などの Web リソースの追加情報またはパラメーターを含むオプションの文字列です。フラグメントは、#introduction や #summary などの Web リソースの特定の部分またはセクションを識別するオプションの文字列です。
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、アナリストは暗号化されていない Web トラフィックのプロトコル (HTTP) に一致する検索文字列を使用する必要があります。HTTP はハイパーテキスト転送プロトコルの略で、Web サーバーと Web ブラウザー間でデータを転送するための標準プロトコルです。ただし、HTTP ではデータの暗号化やセキュリティが提供されないため、Web トラフィックを傍受した人は誰でもデータを読み取ったり変更したりできます。したがって、暗号化されていない Web サイトは、盗聴、改ざん、またはスプーフィング攻撃に対して脆弱です。暗号化されていない Web サイトにアクセスするには、通常、URL は http:// で始まり、その後にドメイン名とオプションでポート番号が続きます。たとえば、http://www.example.com または http://www.example.com:80 です。URL で文字列 http:// をスキャンすることにより、Web フィルターは暗号化されていない Web サイトを識別してブロックできます。
その他のオプションは、暗号化されていない Web トラフィックのプロトコルと一致しないため、正しくありません。Encryption=off は、Web リソースの暗号化ステータスを示すクエリ文字列として考えられますが、標準または必須のパラメータではありません。Https:// は暗号化された Web トラフィックのプロトコルであり、データの暗号化とセキュリティを提供するために HTTPS (Hypertext Transfer Protocol Secure) を使用します。Www.*.com は、www で始まり .com で終わる任意の Web サイトに一致するドメイン名として考えられますが、プロトコルは指定しません。:443 は、暗号化された Web トラフィックのプロトコルである HTTPS のポート番号です。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 2 章: ネットワークのセキュリティ保護、69 ページ。Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 2.1: ネットワーク デバイスとテクノロジ、ビデオ: Web フィルター (5:16)。

最新問題**: 95**
レガシー アプリケーションがビジネス運営に不可欠であり、予防的制御がまだ実装されていない場合、企業はまず次のどのリスク管理戦略を採用すべきでしょうか。
A. 軽減
B. 受け入れる
C. 転送
D. 避ける
Answer: A (メーッセージを残す**)**

軽減とは、リスクの発生可能性または影響を軽減するリスク管理戦略です。
レガシー アプリケーションが業務運営に不可欠であり、予防的制御がまだ実装されていない場合、企業はまず軽減戦略を採用して、アプリケーションの既存の脆弱性とギャップに対処する必要があります。これには、アプリケーションへのパッチ、更新、または構成変更の適用、またはアプリケーションの周囲にセキュリティ制御のレイヤーの追加が含まれる場合があります。受け入れ、転送、回避もリスク管理戦略ですが、このシナリオでは最適なオプションではありません。受け入れとは、リスクを認識し、何もせずに結果を受け入れることです。転送とは、保険会社やベンダーなどのサードパーティにリスクを移すことです。回避とは、リスクの原因を取り除くかプロセスを変更することでリスクを排除することです。これらの戦略は、業務運営に不可欠であり、予防的制御が実装されていないレガシー アプリケーションでは実行可能または望ましくない場合があります。

最新問題: **96**
セキュリティ アナリストは、従業員の会社のラップトップから送信される悪意のあるネットワーク トラフィックの可能性に関する SIEM のアラートを確認しています。セキュリティ アナリストは、調査を続けるには、マシンで実行されている実行可能ファイルに関する追加データが必要であると判断しました。アナリストは、次のログのうちどれをデータソースとして使用する必要がありますか。
A. エンドポイント
B. IPS/IDS
C. アプリケーション
D. ネットワーク
Answer: A (メーッセージを残す**)**

最新問題: **97**
長期にわたる停電が企業の環境に与える影響を最も軽減できるのはどれでしょうか?
A. ホットサイト
B. UPS
C. スナップショット
D. 飛翔
Answer: B (メーッセージを残す**)**
UPS (無停電電源装置) は、長時間の停電が企業の環境に与える影響を軽減する可能性が高いでしょう。UPS はバックアップ電源を提供し、短時間の停電時にシステムが継続して稼働するようにし、秩序立ったシャットダウンを実行したり、発電機などの長期的な電源ソリューションに切り替えたりするのに十分な時間を確保します。
ホット サイト: プライマリ サイトが使用できなくなった場合に使用できる、完全に機能するオフサイト データ センター。短期間の停電を軽減するよりも、災害復旧に適しています。
UPS: 即時のバックアップ電源を提供し、停電時のデータ損失やハードウェアの損傷を防ぎます。

スナップショット: 停電の緩和ではなく、データのバックアップと回復に使用されます。
SOAR (セキュリティ オーケストレーション、自動化、および対応): 停電緩和とは関係のないセキュリティ操作を自動化するプラットフォーム。

最新問題**: 98**
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。
この決定を下す際に、会社が最も使用した分析要素は次のどれですか?
A. 次回
B. RTO
C. ARO
D. MTBF
Answer: (解答を表示する**)**
ARO (年間発生率) は、特定の年に発生するイベントの頻度または可能性を測定する分析要素です。ARO は、イベントの潜在的な損失または影響を予測するのに役立つため、リスク評価および管理でよく使用されます。企業は ARO を使用して、イベントの年間損失予測 (ALE) を計算できます。これは、ARO と単一損失予測 (SLE) の積です。ALE は、イベントの年間予想コストを表し、セキュリティ制御の実装または保険契約の購入コストと比較するために使用できます。
同社は、サイバー保険契約からランサムウェア攻撃の補償を削除する決定を下す際に、おそらく ARO を使用しました。同社は、過去のデータ、業界の傾向、または脅威インテリジェンスに基づいてランサムウェア攻撃の ARO を推定し、ARO が低いか無視できるほど小さいことを発見した可能性があります。また、同社はランサムウェア攻撃の ALE を計算し、ALE が保険契約のコストよりも低いことを発見した可能性があります。したがって、同社はリスクが許容可能または管理可能であると判断し、ランサムウェア攻撃の補償を削除して年間サイバー保険契約のコストを削減することを決定しました。
IMTTR (インシデント管理チームのトレーニングと準備)、RTO (目標復旧時間)、および MTBF (平均故障間隔) は、企業がサイバー保険契約からランサムウェア攻撃の補償を削除する決定を下す際に使用した可能性が最も高い分析要素ではありません。IMTTR は、セキュリティ インシデントに効果的に対応できるようにインシデント管理チームを準備およびトレーニングするプロセスです。IMTTR は、イベントの頻度や影響を測定するものではなく、チームの能力と準備状況を測定するものです。RTO は、中断後にシステムまたはサービスを復元するための最大許容時間を定義する指標です。RTO は、イベントの頻度や影響を測定するものではなく、システムまたはサービスの可用性と継続性を測定するものです。MTBF は、システムまたはコンポーネントの故障間隔の平均時間を測定する指標です。
MTBF は、イベントの頻度や影響を測定するものではなく、システムまたはコンポーネントの信頼性とパフォーマンスを測定します。

参考資料 = CompTIA Security+ SY0-701 認定学習ガイド、97 ～ 98 ページ、Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、ビデオ 5.2 - リスク管理、0:00 ～ 3:00。

最新問題**: 99**
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
Answer: B (メーッセージを残す**)**
サイバー保険は、データ侵害、ランサムウェア、サービス拒否、フィッシング、マルウェアなどのサイバー攻撃によって生じる金銭的損失や負債をカバーする保険の一種です。サイバー保険は、企業がデータの復元、システムの修復、身代金の支払い、顧客への補償、法的措置にかかる費用を回収するのに役立ちます。サイバー保険は、企業がリスク レジスターに記載されている項目に対処するために使用できる戦略の 1 つです。リスク レジスターは、特定されたリスク、その確率、影響、およびプロジェクトまたは組織に対する軽減戦略を記録する文書です。一般的な 4 つのリスク軽減戦略は次のとおりです。
受け入れ: 企業はリスクを認識し、リスクを軽減または排除するための措置を講じることなく、結果を受け入れることを決定します。この戦略は通常、リスクが低い場合、またはリスク軽減のコストが高すぎる場合に選択されます。
移転: 企業はリスクを保険会社、ベンダー、パートナーなどの第三者に移転します。この戦略は通常、リスクが高い場合、または企業にリスクに対処するためのリソースや専門知識が不足している場合に選択されます。
軽減: 企業は、リスクの発生可能性または影響を軽減するための制御または対策を実施します。この戦略は通常、リスクが中程度の場合、または軽減コストが妥当な場合に選択されます。
回避: 企業は、プロジェクトまたは組織の範囲、計画、設計を変更することでリスクを排除します。この戦略は通常、リスクが許容できない場合、またはリスク軽減のコストが高すぎる場合に選択されます。
サイバー保険を購入することで、企業はリスクを保険会社に移転し、サイバー攻撃が発生した場合の金銭的損失と責任を保険会社が補償することになります。
したがって、正解は B. 転送です。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 8 章: ガバナンス、リスク、コンプライアンス、377 ページ。Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 8.1: リスク管理、ビデオ: リスク軽減戦略 (5:37)。

最新問題**: 100**

ソフトウェア開発マネージャーは、会社が作成したコードの信頼性を確保したいと考えています。次のオプションのうち、最も適切なものはどれですか。
A. ユーザー入力フィールドの入力検証をテストする
B. 自社開発ソフトウェアのコード署名の実行
C. ソフトウェアの静的コード解析を実行する
D. 安全なCookieが使用されていることを確認する
Answer: (解答を表示する**)**
説明
コード署名は、企業が作成したコードの信頼性と整合性を暗号化を使用して検証する手法です。コード署名では、企業のみが所有する秘密鍵を使用してコードにデジタル署名を適用します。デジタル署名は、信頼できる証明機関を通じて配布できる対応する公開鍵を持つ人なら誰でも検証できます。コード署名により、コードへの不正な変更、改ざん、マルウェアの挿入を防ぐことができ、コードが正当なソースからのものであることをユーザーに保証することもできます。参考資料 = 500 以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、74 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 3.2、11 ページ。アプリケーション セキュリティ - SY0-601 CompTIA Security+: 3.2

最新問題**: 101**
評価を実行した後、アナリストは結果のリスク評価を提供したいと考えています。評価を計算する際に考慮すべき概念は次のうちどれですか。
A. 所有者としきい値
B. 影響と可能性
C. 食欲と寛容
D. 確率と露出係数
Answer: B (メーッセージを残す**)**
リスク評価を計算する場合、影響と可能性の概念が最も考慮される可能性が高くなります。リスク評価には通常、脅威の潜在的な影響 (脅威が現実化した場合の結果の重大さ) と脅威が発生する可能性 (脅威が発生する可能性がどの程度あるか) の評価が含まれます。
影響: 特定の脅威が脆弱性を悪用した場合の結果の重大度を測定します。金銭的損失、評判の失墜、業務の中断などの要因を考慮します。
可能性: 脅威が脆弱性を悪用する可能性を測定します。これは、履歴データ、現在の脅威の状況、専門家の判断に基づいて算出されます。

最新問題**: 102**
ある企業が機密ストレージアレイを廃棄することになり、廃棄作業を完了するために外部ベンダーを雇います。
企業がベンダーに要求すべき事項は次のうちどれですか?
A. 認定
B. 在庫リスト

C. 分類
D. 所有権の証明
Answer: A (メーッセージを残す**)**
企業は、ストレージ アレイが安全に、また企業のポリシーと基準に従って廃棄されたことを確認する証明書をベンダーに要求する必要があります。証明書は、機密データを破棄し、不正アクセスや復旧を防ぐためにベンダーが適切な手順と方法に従ったことを証明します。証明書には、廃棄の日付、時間、場所、方法、および関係者の名前と署名などの詳細も含まれる場合があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 3 章、1441 ページ

最新問題**: 103**
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
Answer: (解答を表示する**)**
説明
ダッシュボードは、セキュリティ イベントやインシデントに関連する主要なパフォーマンス指標、メトリック、傾向を視覚的に表示するグラフィカル ユーザー インターフェイスです。ダッシュボードを使用すると、取締役会は、特定の期間に組織に影響を与えたインシデントの数と影響、およびセキュリティ制御とプロセスのステータスと有効性を把握できます。また、ダッシュボードを使用すると、取締役会は特定の詳細をドリルダウンしたり、さまざまな基準でデータをフィルター処理したりすることもできます12。
パケット キャプチャは、デバイスまたはネットワーク セグメントを通過するネットワーク トラフィックをキャプチャして分析する方法です。パケット キャプチャでは、各パケットの送信元、送信先、プロトコル、およびコンテンツに関する詳細な情報を提供できますが、取締役会にインシデントの概要を提示するには適していません13。
脆弱性スキャンは、攻撃者に悪用される可能性のあるシステムまたはネットワークの弱点と露出を特定して評価するプロセスです。脆弱性スキャンは、組織がリスクの優先順位付けと修復を行い、セキュリティ体制を改善するのに役立ちますが、四半期に発生したインシデントの数を報告する適切な方法ではありません14。
メタデータは、他のデータの形式、起源、構造、コンテキストなどを説明するデータです。メタデータは、データの特性とプロパティに関する有用な情報を提供できますが、取締役会にインシデントの影響と頻度を伝えるための有意義な方法ではありません。参考資料 = 1: CompTIA Security+ SY0-701 認定学習ガイド、37 ページ22: SIEM ダッシュボード -

SY0-601 CompTIA Security+: 4.3、メッサー教授によるビデオ3: CompTIA Security+ SY0-701 認定学習ガイド、34 ページ64:
CompTIA Security+ SY0-701 認定試験学習ガイド、362 ページ。: CompTIA Security+ SY0-701 認定試験学習ガイド、97 ページ。

最新問題: **104**
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
Answer: D (メーッセージを残す)
説明
内部脅威とは、組織のデータやシステムへのアクセスを許可された従業員、請負業者、ビジネス パートナーなど、組織内部から発生するセキュリティ リスクです。内部脅威は、機密データの盗難、漏洩、破壊などの悪意のあるものや、フィッシングやソーシャル エンジニアリングの被害に遭うなどの意図的でないものがあります。内部脅威は、組織の評判、財務、運営、法令遵守に重大な損害を与える可能性があります。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する行為は、組織のセキュリティ ポリシーに違反し、データの機密性と整合性を損なうため、悪意のある内部脅威の一例です。参考資料 = 内部脅威 - CompTIA Security+ SY0-701: 3.2、ビデオの 0:00、CompTIA Security+ SY0-701 認定試験学習ガイド、133 ページ。

最新問題: **105**
脆弱性の重大性を定量的に測定するために使用されるのは次のどれですか?
A. CVE
B. CVSS
C. CIA
D. CERT
Answer: B (メーッセージを残す)
CVSS は Common Vulnerability Scoring System の略で、脆弱性の重大度とリスクを評価して伝達するための標準化された方法を提供するフレームワークです。CVSS は、一連の指標と数式を使用して 0 から 10 までの数値スコアを計算します。スコアが高いほど、重大度が高くなります。CVSS は、組織が修復作業に優先順位を付け、さまざまなシステムやベンダー間で脆弱性を比較するのに役立ちます。その他のオプションは、脆弱性の重大度を測定するために使用されるのではなく、脆弱性を特定、分類、または報告するために使用されます。参考: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、39 ページ

最新問題: **106**
オンボーディング プロセス中に、従業員はイントラネット アカウントのパスワードを作成する必要があります。パスワードには、10 文字の英数字と特殊文字 2 文字を含める必要があります。パスワードが作成されると、会社はイントラネット プロファイルに基づいて、従業員に会社所有の他の Web サイトへのアクセスを許可します。
イントラネット アカウントを保護し、ユーザーのイントラネット アカウントに基づいて複数のサイトへのアクセスを許可するために、企業が使用するアクセス管理の概念は次のどれですか (2 つ選択)。
A. 連邦
B. 本人確認
C. パスワードの複雑さ
D. デフォルトのパスワードの変更
E. パスワードマネージャー
F. オープン認証
Answer: A,C (メーッセージを残す)
フェデレーションは、ユーザーが一度認証するだけで、異なるドメインや組織にまたがる複数のリソースやサービスにアクセスできるようにするアクセス管理の概念です。フェデレーションは、ユーザーの資格情報を保存し、それを公開せずに要求されたリソースやサービスに提供する信頼できるサードパーティに依存します。
パスワードの複雑さは、長さ、文字の種類、一意性など、特定の基準を満たすパスワードをユーザーに作成させるセキュリティ対策です。パスワードの複雑さにより、パスワードの解読や推測が困難になり、ブルートフォース攻撃、パスワード推測、クレデンシャルスタッフィングを防ぐことができます。参考文献: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、308 ～ 309 ページおよび
312-313 1

最新問題: **107**
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。
不正なデバイスの接続が許可される可能性が最も高い方法はどれですか?
A. ユーザーが個人のデバイスを使用して MAC クローン攻撃を実行しました。
B. DMCP障害により誤ったIPアドレスが配布されました
C. 管理者がテストのためにセキュリティ制御をバイパスしました。
D. DNS ハイジャックにより、攻撃者はキャプティブ ポータルのトラフィックを傍受できます。
Answer: A (メーッセージを残す**)**
不正なデバイスがネットワークに接続できる可能性が最も高い方法は、MAC クローン攻撃です。この攻撃では、個人のデバイスが承認されたデバイスの MAC アドレスをコピーし、ネットワーク アクセスに既知のハードウェア アドレスを使用する 802.1X アクセス制御を回避します。監査レポートで一致する MAC アドレスは、この手法が不正なネットワーク アクセスを取得するために使用されたことを示しています。
参考文献
* CompTIA Security+ SY0-701 コース内容: ドメイン 03 セキュリティ アーキテクチャ。
* CompTIA Security+ SY0-601 学習ガイド: ネットワーク セキュリティと MAC アドレス スプーフィングの章。

最新問題**: 108**
セキュリティ マネージャーは、さまざまな種類のセキュリティ インシデントに対応するために使用する新しいドキュメントを作成しました。マネージャーが次に取るべきステップは次のどれですか。
A. 最大データ保持ポリシーを設定します。
B. ドキュメントをエアギャップネットワーク上に安全に保存します。
C. ドキュメントのデータ分類ポリシーを確認します。
D. チームで卓上演習を実施します。
Answer: (解答を表示する**)**
机上演習は、セキュリティ インシデント対応計画の有効性をテストするシミュレートされたシナリオです。関連する関係者を集め、計画の手順を順に実行し、対処が必要なギャップや問題を特定します。机上演習は、セキュリティ マネージャーが作成したドキュメントを検証し、チームがさまざまな種類のセキュリティ インシデントに備えられるようにするための優れた方法です。

最新問題**: 109**
次のチームのうち、組織の重要なシステムを保護するために、攻撃的テスト手法と防御的テスト手法の両方を組み合わせているのはどれですか?
A. 赤
B. 青
C. 紫

D. 黄色
Answer: (解答を表示する**)**
パープルは、攻撃的テスト手法と防御的テスト手法の両方を組み合わせて組織の重要なシステムを保護するチームです。パープルは独立したチームではなく、レッド チームとブルー チームの共同作業です。レッド チームは、攻撃をシミュレートして組織のシステムの脆弱性を悪用する攻撃チームです。ブルー チームは、組織のシステムを監視および保護する防御チームです。パープル チームは、ブルー チームの防御戦術と制御を、レッド チームによって発見された脅威と脆弱性と統合して 1 つのナラティブにまとめ、組織の全体的なセキュリティ体制を改善することで、レッド チームとブルー チームの有効性を確保し、最大化するために存在します。レッド、ブルー、イエローは、セキュリティ テストに関与する他の種類のチームですが、攻撃的手法と防御的手法の両方を組み合わせていません。イエロー チームは、ブルー チームがセキュリティ テストで使用するソフトウェア ソリューション、スクリプト、およびその他のプログラムを作成するチームです。参考文献: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、1331 ページ侵入テスト: レッド チーム、ブルーチーム、パープルチームを理解する3

最新問題**: 110**
技術者が、SaaS プロバイダーによって導入およびサポートされている新しいシステム用にファイアウォールのポートを開いています。次のどれが新しいシステムのリスクですか?
A. デフォルトの資格情報
B. セグメント化されていないネットワーク
C. サプライチェーンベンダー
D. 脆弱なソフトウェア
Answer: C (メーッセージを残す**)**
サプライ チェーン ベンダーは、SaaS プロバイダーなど、組織に商品やサービスを提供するサード パーティ エンティティです。サプライ チェーン ベンダーのセキュリティ プラクティスが不十分であったり、違反や侵害があったりして、システムやそのデータの機密性、整合性、可用性に影響を及ぼす可能性がある場合、そのベンダーは新しいシステムにリスクをもたらす可能性があります。組織は、このリスクを軽減するために、デュー デリジェンスを実行し、ベンダーとサービス レベル契約を締結する必要があります。その他のオプションは、SaaS プロバイダーを使用するシナリオに固有のものではなく、どのシステムにも当てはまる一般的なリスクです。

最新問題**: 111**
ある企業は、従業員がモバイル デバイスのオペレーティング システムを変更できないという条項を AUP に追加しています。組織が対処しようとしている脆弱性は次のどれですか。
A. クロスサイトスクリプティング
B. バッファオーバーフロー
C. 脱獄
D. サイドローディング

Answer: C (メーッセージを残す)
ジェイルブレイクとは、iPhone や iPad などのモバイル デバイスにメーカーやキャリアが課している制限を解除するプロセスです。ジェイルブレイクにより、ユーザーは不正なアプリケーションをインストールしたり、システム設定を変更したり、ルート権限にアクセスしたりできるようになります。ただし、ジェイルブレイクにより、デバイスはマルウェア、スパイウェア、不正アクセス、データ損失、保証の無効化などの潜在的なセキュリティ リスクにさらされることになります。したがって、組織は、これらの脆弱性を防ぎ、企業のデータとネットワークを保護するために、従業員によるモバイル デバイスのジェイルブレイクを禁止する場合があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 10 章: モバイル デバイス セキュリティ、507 ページ 2

最新問題**: 112**
ある企業が、社内ネットワークから発信される DNS トラフィックを制限しようとしています。発信 DNS 要求は、IP アドレス 10.50.10.25 を持つ 1 つのデバイスからのみ許可されます。次のファイアウォール ACL のどれがこの目的を達成しますか。
A. アクセスリスト 送信許可 0.0.0.0/0 0.0.0.0/0 ポート 53
アクセスリスト アウトバウンド拒否 10.50.10.25/32 0.0.0.0/0 ポート 53
B. アクセスリスト送信許可 0.0.0.0/0 10.50.10.25/32 ポート53
アクセスリスト アウトバウンド拒否 0.0.0.0/0 0.0.0.0/0 ポート 53
C. アクセスリスト 送信許可 0.0.0.0/0 0.0.0.0/0 ポート 53
アクセスリスト アウトバウンド拒否 0.0.0.0/0 10.50.10.25/32 ポート 53
D. アクセスリストの送信許可 10.50.10.25/32 0.0.0.0/0 ポート 53
アクセスリスト アウトバウンド拒否 0.0.0.0/0 0.0.0.0/0 ポート 53
Answer: D (メーッセージを残す)
ファイアウォール ACL (アクセス制御リスト) は、ファイアウォールによって許可または拒否されるトラフィックを決定する一連のルールです。ルールは、一致するものが見つかるまで上から下へ順番に処理されます。ファイアウォール ACL ルールの構文は次のとおりです。
アクセス リスト <方向> <アクション> <送信元アドレス> <宛先アドレス> <プロトコル> <ポート> 内部ネットワークから発信される送信 DNS トラフィックを制限するには、ファイアウォール ACL で、IP アドレス 10.50.10.25 を持つデバイスのみがポート 53 の任意の宛先に DNS 要求を送信できるようにし、ポート 53 の他のすべての送信トラフィックを拒否する必要があります。正しいファイアウォール ACL は次のとおりです。
アクセス リスト アウトバウンド 許可 10.50.10.25/32 0.0.0.0/0 ポート 53 アクセス リスト アウトバウンド 拒否 0.0.0.0/0 0.0.0.0/0 ポート 53 最初のルールは、送信元アドレス 10.50.10.25/32 (単一ホスト) からポート 53 (DNS) 上の任意の宛先アドレス (0.0.0.0/0) へのアウトバウンド トラフィックを許可します。2 番目のルールは、ポート 532 上のその他すべてのアウトバウンド トラフィックを拒否します。
参考資料: CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 4 章、175 ページ。

最新問題: **113**
セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに従うべき事項は次のどれですか。
A. 災害復旧計画
B. インシデント対応手順
C. 事業継続計画
D. 変更管理手順
Answer: D (メーッセージを残す**)**
説明
変更管理手順とは、セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに従わなければならない一連の手順とガイドラインです。ファイアウォールは、定義済みのルールまたはポリシーに基づいてネットワーク トラフィックをフィルタリング、ブロック、または許可できるデバイスまたはソフトウェアです。ファイアウォール ルールとは、ファイアウォールがパケットまたは接続に適用する基準とアクションを定義するステートメントです。たとえば、ファイアウォール ルールは、送信元と宛先の IP アドレス、ポート、プロトコル、またはアプリケーションに基づいてトラフィックを許可または拒否できます。新しいファイアウォール ルール セットを設定することは、ネットワークのセキュリティ、パフォーマンス、および機能に影響を与える可能性のある変更の一種です。したがって、変更が管理された一貫した方法で計画、テスト、承認、実装、文書化、およびレビューされるようにするには、変更管理手順が必要です。変更管理手順には通常、次の要素が含まれます。
変更の目的、範囲、影響、利点、および変更の所有者、実装者、承認者の役割と責任を説明する変更要求。
変更の実現可能性、リスク、コスト、依存性、および代替案と緊急時対応計画を評価する変更評価。
変更ポリシーによって定義された基準としきい値に基づいて、変更を実装段階に進めることを承認する変更承認。
計画とスケジュールに従って変更を実行し、変更の結果と成果を検証する変更実装。
変更の詳細とステータス、および学んだ教訓とベスト プラクティスを記録する変更ドキュメント。
変更のパフォーマンスと有効性を監視および測定し、対処または改善する必要がある問題やギャップを特定する変更レビュー。
変更管理手順は、セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに遵守することが重要であり、次の目的の達成に役立ちます。
ファイアウォール ルールがセキュリティ ポリシーと標準に準拠し、脆弱性や競合が発生しないようにすることで、ネットワークのセキュリティ体制とコンプライアンスを強化します。

ファイアウォール ルールが展開前にテストおよび検証され、ネットワーク サービスまたはアプリケーションの可用性や機能に影響を与えないようにすることで、ネットワークの中断とダウンタイムを最小限に抑えます。
ファイアウォール ルールがネットワーク ユーザーと関係者の変化するニーズと要求に応じて最適化および更新され、パフォーマンスや互換性の問題が発生しないようにすることで、ネットワークの効率と品質を向上させます。
ファイアウォール ルールが文書化され、定期的にレビューされ、関係当局や関係者によって追跡および監査可能であることを保証することで、ネットワークの説明責任と透明性を高めます。
その他のオプションは、新しいファイアウォール ルールのセットを設定するプロセスに関連していないため、正しくありません。災害復旧計画は、システム障害、自然災害、またはその他の緊急事態が発生した場合に、組織の通常の運用を回復することを目的とした一連のポリシーと手順です。インシデント対応手順は、サイバー攻撃、データ侵害、マルウェア感染などのセキュリティ インシデントの封じ込め、分析、根絶、および回復を目的とした一連の手順とガイドラインです。事業継続計画は、パンデミック、停電、市民の暴動などの混乱を引き起こすイベントの発生中および発生後に、組織の重要な機能と業務を維持することを目的とした一連の戦略とアクションです。参考文献 = CompTIA Security+ 学習ガイド (SY0-701)、第 7 章: 回復力と回復、325 ページ。Messer 教授の CompTIA SY0-701 Security + トレーニング コース、セクション 1.3: セキュリティ運用、ビデオ: 変更管理 (5:45)。

最新問題**: 114**
ソフトウェア開発マネージャーは、会社が作成したコードの信頼性を確保したいと考えています。次のオプションのうち、最も適切なものはどれですか。
A. ユーザー入力フィールドの入力検証をテストする
B. 自社開発ソフトウェアのコード署名の実行
C. ソフトウェアの静的コード解析を実行する
D. 安全なCookieが使用されていることを確認する
Answer: (解答を表示する**)**
コード署名は、企業が作成したコードの信頼性と整合性を暗号化を使用して検証する手法です。コード署名では、企業のみが所有する秘密鍵を使用してコードにデジタル署名を適用します。デジタル署名は、信頼できる証明機関を通じて配布できる対応する公開鍵を持つ人なら誰でも検証できます。コード署名により、コードへの不正な変更、改ざん、マルウェアの挿入を防止できるほか、コードが正当なソースからのものであることをユーザーに保証できます。参考資料 = 500 問以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、74 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 3.2、11 ページ。アプリケーション セキュリティ - SY0-601 CompTIA Security+: 3.2

最新問題**: 115**

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
G. 誤情報は、虚偽または誤解を招く情報を広めて、対象の信念、意見、または行動に影響を与えるソーシャル エンジニアリング手法の一種です。誤情報は、世論を操作したり、混乱を引き起こしたり、評判を傷つけたり、議題を推進したりするために使用される可能性があります。誤情報は、テキスト メッセージや資格情報の検証とは関係ありません。
Answer: B,E (メーッセージを残す**)**
参照 = 1: スミッシングとは? | 定義と例 | Kaspersky 2: スミッシング - Wikipedia 3: なりすまし攻撃: なりすまし攻撃とは何か、また、それに対してどのように防御するか? 4: なりすまし - Wikipedia 5: タイポスクワッティングとは? | 定義と例 | Kaspersky 6: タイポスクワッティング - Wikipedia 7: フィッシングとは? | 定義と例 | Kaspersky 8: フィッシング - Wikipedia 9: ヴィッシングとは? | 定義と例 | Kaspersky : ヴィッシング - Wikipedia : 誤情報とは? | 定義と例 | Britannica : 誤情報 - Wikipedia 説明:
スミッシングは、テキスト メッセージ (SMS) を使用して被害者を騙し、機密情報を漏らしたり、悪意のあるリンクをクリックさせたり、マルウェアをダウンロードさせたりするためのソーシャル エンジニアリング手法の一種です。スミッシング メッセージは、銀行、政府機関、サービス プロバイダーなどの正当なソースから送信されたように見えることが多く、緊急または脅迫的な言葉を使用して受信者に行動を起こさせようとします12。このシナリオでは、給与部門からのテキスト メッセージであると主張するテキスト メッセージは、スミッシングの一例です。
なりすましは、権威のある人物、信頼できる人物、同僚など、別の人物になりすましてターゲットの信頼や協力を得るというソーシャル エンジニアリング手法の一種です。なりすましは、電話、メール、テキスト メッセージ、直接の訪問など、さまざまなチャネルを通じて実行され、被害者から情報、アクセス、または金銭を取得するために使用されます34。このシナリオでは、給与部門からのテキスト メッセージになりすましたものがなりすましの例です。
A) タイポスクワッティングは、人気のあるウェブサイトやよく知られているウェブサイトに似ているが、意図的にスペルミスや異なる拡張子を持つドメイン名を登録するサイバー攻撃の一種です。タイポスクワッティングは、ユーザーがウェブアドレスを入力する際に犯す一般的な間違いを悪用し、悪意のあるサイトや詐欺サイトにリダイレクトして、情報を盗んだり、マルウェアをインストールしたり、広告を表示したりすることを目的としています56。タイポスクワッティングは、テキストメッセージや資格情報の検証とは関係ありません。

B) フィッシングは、詐欺メールを使用して受信者を騙し、機密情報を開示させたり、悪意のあるリンクをクリックさせたり、マルウェアをダウンロードさせたりするためのソーシャルエンジニアリング手法の一種です。フィッシングメールは、銀行、小売業者、サービスプロバイダーなどの正当な組織の外観や口調を模倣することが多く、欺瞞的または緊急の言葉を使用して受信者に行動を起こさせます78。フィッシングは、テキストメッセージや資格情報の検証とは関係ありません。
D) ビッシングは、音声通話を利用して被害者を騙し、パスワード、クレジットカード番号、銀行口座の詳細などの機密情報を漏らすソーシャルエンジニアリング手法の一種です。ビッシングの電話は、法執行機関、政府機関、テクニカルサポートなどの正当なソースから発信されたように見えることが多く、脅迫や偽りの約束を使って受信者に従わせようとします9。ビッシングは、テキストメッセージや認証情報の確認とは関係ありません。

最新問題**: 116**
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
Answer: (解答を表示する**)**
アクセスの無効化は、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する自動化ユースケースです。アクセスの無効化は、ログイン資格情報、電子メール、VPN、クラウド サービスなどのユーザー アカウントのアクセス権を取り消したり、一時停止したりするプロセスです。
アクセスを無効にすると、アカウントを侵害した可能性のある元従業員や攻撃者によるアカウントの不正使用や悪意のある使用を防ぐことができます。また、アクセスを無効にすると、攻撃対象領域が減り、データ侵害や漏洩のリスクも軽減されます。アクセスの無効化は、従業員の解雇、辞職、異動などの定義済みイベントに基づいてアクションをトリガーできるスクリプト、ツール、またはワークフローを使用して自動化できます。
自動化により、手動による介入や人為的エラーに頼ることなく、アクセスをタイムリーかつ一貫して効率的に無効化できます。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 5 章: アイデンティティとアクセス管理、2131 ページ。CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 5 章:
アイデンティティとアクセス管理、2132 ページ。

最新問題**: 117**
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。
Answer: A (メーッセージを残す**)**
コード署名を検証することは、ソフトウェアが改ざんされていないこと、検証済みのソースから提供されたものであることを確認するため、ソフトウェアの信頼性を確認する最良の方法です。コード署名はソフトウェア ベンダーによって適用されるデジタル署名であり、これを検証することでソフトウェアの整合性と提供元が確認されます。参考資料: CompTIA Security+ SY0-701 コース コンテンツと公式 CompTIA 学習リソース。

最新問題**: 118**
ホットスポットに関する質問
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。
説明書
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て、どのホストが感染の原因となったかを判断し、残りの各ホストがクリーンか感染しているかを特定します。
いつでもシミュレーションの初期状態に戻したい場合は、「すべてリセット」ボタンをクリックしてください。
Answer:

最新問題**: 119**
データが変更されていないことを確認するために実行されるアルゴリズムは次のどれですか?
A. ハッシュ
B. コードチェック
C. 暗号化
D. チェックサム
Answer: A (メーッセージを残す**)**
ハッシュは、入力データから固定サイズの文字列を生成することでデータの整合性を検証するために使用されるアルゴリズムです。入力データの 1 ビットでも変更されるとハッシュ値が変わるため、ユーザーはデータの変更を検出できます。SHA-256 や MD5 などのハッシュ アルゴリズムは、データが変更されていないことを確認するためによく使用されます。
参考文献:
* CompTIA Security+ SY0-701 コース内容: ドメイン 6: 暗号化と PKI。データの整合性を検証する際のハッシュの役割について説明します。

最新問題: **120**
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、次の点に気付きました。
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 のアカウントをブルートフォース攻撃しようとしています。
D. ドメインにランサムウェアが展開されました。
Answer: C (メーッセージを残す)
ブルート フォースは、多数の可能な組み合わせを使用して、ユーザー アカウントのパスワードやその他の資格情報を推測しようとするタイプの攻撃です。攻撃者は自動化されたツールまたはスクリプトを使用してブルート フォース攻撃を実行し、アカウントへの不正アクセスを取得することができます。ドメイン アクティビティ ログには、ユーザー ismith が短期間に 10 回連続してログインに失敗したことが示されています。これは、ブルートフォース攻撃の強力な指標です。ログには、失敗したログインのソース IP アドレスが ismith の通常の IP アドレスと異なることも示されています。これは、攻撃者が別のデバイスまたは場所を使用して攻撃を開始していることを示唆しています。セキュリティ アナリストは、攻撃者の IP アドレスをブロックし、ismith のパスワードをリセットし、ismith にインシデントを通知するために、直ちに行動を起こす必要があります。参考資料 = 500 以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 1 章、14 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 1.1、2 ページ。脅威アクターと属性 - SY0-601 CompTIA Security+: 1.1

最新問題: **121**
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
Answer: (解答を表示する)
説明
部分的に既知の環境は、IP アドレス、オペレーティング システム、デバイスの種類など、ターゲットに関する一部の情報をテスト担当者が持っているタイプの侵入テストです。これにより、テスト担当者は特定の脆弱性に焦点を当て、テストの範囲を縮小できます。部分的に既知の環境は、グレー ボックス テストとも呼ばれます1。
参考資料: CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 10 章、543 ページ。

最新問題: **122**
従業員が、支払いウェブサイトからの電子メールで連絡先情報の更新を求めるリンクをクリックしました。従業員はログイン情報を入力しましたが、「ページが見つかりません」というエラー メッセージが表示されました。
次のどのタイプのソーシャル エンジニアリング攻撃が発生しましたか?
A. ブランドのなりすまし
B. プリテキスティング
C. タイプミススクワッティング
D. フィッシング
Answer: D (メーッセージを残す**)**
フィッシングはソーシャル エンジニアリング攻撃の一種で、支払い Web サイト、銀行、その他の信頼できる組織などの正当なソースから送信されたように見える不正なメールを送信します。フィッシングの目的は、受信者を騙して悪意のあるリンクをクリックさせたり、悪意のある添付ファイルを開かせたり、ログイン認証情報、個人データ、財務情報などの機密情報を提供させたりすることです。このシナリオでは、従業員は支払い Web サイトから連絡先情報の更新を求めるメールを受け取りました。メールには、本物の Web サイトの外観を模倣した偽の Web サイトに従業員を誘導するリンクが含まれていました。
従業員はログイン情報を入力しましたが、「ページが見つかりません」というエラー メッセージが表示されました。これは、従業員がフィッシング攻撃の被害者となり、攻撃者が支払い Web サイトの従業員の資格情報を入手した可能性があることを示しています。参考資料 = その他のソーシャル エンジニアリング攻撃 - CompTIA Security+ SY0-701 - 2.2、CompTIA Security+: ソーシャル エンジニアリング手法とその他の攻撃... - NICCS、[500 以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版]

最新問題: **123**
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べきものは次のどれですか。
A. ジャンプサーバー
B. 半径
C. HSM
D. ロードバランサー

Answer: A (メーッセージを残す)
説明
ジャンプ サーバーは、ユーザーのワークステーションとリモート ネットワーク セグメント間の仲介役として機能するデバイスまたは仮想マシンです。ジャンプ サーバーを使用すると、データベース サーバーなど、ユーザーのワークステーションから直接アクセスできないサーバーまたはデバイスに安全にアクセスすることができます。ジャンプ サーバーは、リモート接続の監査ログやアクセス制御も提供できます。ジャンプ サーバーは、ジャンプ ボックスまたはジャンプ ホストとも呼ばれます12。
RADIUS は、ネットワーク アクセスの認証、承認、アカウンティングを行うプロトコルです。RADIUS は、リモート サーバーにアクセスするためのデバイスや方法ではなく、ネットワーク アクセスを要求するユーザーまたはデバイスの ID と権限を確認する方法です34。
HSM はハードウェア セキュリティ モジュールの略で、暗号キーの安全な保管と生成を提供する物理デバイスです。HSM は、デジタル署名、暗号化、認証などの機密データとアプリケーションを保護するために使用されます。HSM はリモート サーバーにアクセスするために使用されず、サーバー上にあるデータとアプリケーションのセキュリティを強化するために使用されます5。
ロード バランサは、可用性、パフォーマンス、容量などの基準に基づいて、ネットワーク トラフィックを複数のサーバーまたはデバイスに分散するデバイスまたはソフトウェアです。ロード バランサを使用すると、Web サーバー、アプリケーション サーバー、データベース サーバーなどのネットワーク サービスのスケーラビリティ、信頼性、効率性を向上させることができます。ロード バランサは、リモート サーバーにアクセスするために使用されるのではなく、リモート サーバーで実行されるサービスの配信を最適化するために使用されます。参考資料 = ジャンプ ホストを使用してリモート サーバーにアクセスする方法 ジャンプ サーバー RADIUS リモート認証ダイヤルイン ユーザー サービス (RADIUS) ハードウェア セキュリティ モジュール (HSM)
【HSMとは？】
[負荷分散 ロンピューティング)]
[ロードバランシングとは?]

最新問題: **124**
ある企業が機密ストレージ アレイを廃棄し、廃棄を完了するために外部ベンダーを雇います。企業がベンダーに要求する必要があるのは次のうちどれですか。
A. 認定
B. 在庫リスト
C. 分類
D. 所有権の証明
Answer: A (メーッセージを残す)
企業は、ストレージ アレイが安全に、また企業のポリシーと基準に従って廃棄されたことを確認する証明書をベンダーに要求する必要があります。証明書は、機密データを破棄し、

不正アクセスや回復を防ぐためにベンダーが適切な手順と方法に従ったことを証明します。証明書には、廃棄の日付、時間、場所、方法、および関係者の名前と署名などの詳細も含まれる場合があります。

最新問題: **125**
ある会社では、パブリック ネットワーク上で Web サービスが停止しています。サービスは稼働していますが、アクセスできません。ネットワーク ログには、ネットワーク トラフィックの急激な増加が示されており、これが停止の原因となっています。組織が経験している攻撃は次のどれですか。
A. バッファオーバーフロー
B. DDoS
C. ARP ポイズニング
D. ブルートフォース
Answer: (解答を表示する**)**

最新問題: **126**
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に同じ番号を割り当てています
Answer: B (メーッセージを残す**)**
訓練生が会社の電話番号を使用して迷惑電話をかけ、ログで番号が偽装されていないことが確認された場合、SIP (セッション開始プロトコル) サーバーのセキュリティ設定が弱い可能性があります。これにより、会社の電話サービスへの不正アクセスや悪用が可能になり、権限のない個人による悪用につながる可能性があります。
参考資料 = CompTIA Security+ SY0-701 学習教材、特に SIP セキュリティと一般的な脆弱性について。

最新問題: **127**
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
Answer: A (メーッセージを残す**)**
正解は A です。多要素認証 (MFA) は、ユーザーが知っている情報 (パスワードなど)、ユーザーが所有している情報 (トークンなど)、またはユーザー自身 (生体認証など) など、複数の要素を要求することでユーザーの ID を確認する方法です。MFA では、攻撃者がログインするために別の要素を提供する必要があるため、ユーザーのパスワードが侵害された場合でも不正アクセスを防止できます。その他の選択肢は、認証の弱さという攻撃の根本原因に対処していないため、正しくありません。権限の割り当て (B) は、ユーザーの役割または ID に基づいてリソースへのアクセスを許可または拒否するプロセスです。
アクセス管理とは、誰が何にどのような条件でアクセスできるかを制御するプロセスです。パスワードの複雑さ (D) は、推測や解読が困難な強力なパスワードを使用する必要があることを意味しますが、攻撃者が盗んだパスワードを使用することを防ぐことはできません。参考資料 = 多要素認証やその他のセキュリティ概念の詳細については、次のリソースを参照してください。
CompTIA Security+ SY0-701 認定学習ガイド、第 1 章: 一般的なセキュリティ概念1
Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 1.2: セキュリティ概念2 多要素認証 - SY0-601 CompTIA Security+: 2.43 合計: CompTIA Security+ 認定 (SY0-701) | Udemy、セクション 3: アイデンティティとアクセス管理、講義 15: 多要素認証4 CompTIA Security+ 認定 SY0-601: 総合コース [ビデオ]、第 3 章: アイデンティティとアカウント管理、セクション 2: 多要素認証の有効化5

最新問題**: 128**
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
Answer: B (メーッセージを残す**)**
転送中のデータとは、ネットワークや無線などを通じて、ある場所から別の場所へ移動するデータのことです。転送中のデータは、悪意のある人物による傍受、変更、盗難の危険にさらされています。VPN (仮想プライベート ネットワーク) は、2 つのエンドポイント間に安全なトンネルを作成し、そこを通過するデータを暗号化することで、転送中のデータを保護するテクノロジです。

最新問題**: 129**
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。
Answer: D (メーッセージを残す**)**
メタデータは、フォーマット、出所、作成日、作成者、その他の属性など、他のデータを説明するデータです。他の種類のファイルと同様に、ビデオ ファイルには、フォレンジック分析に役立つ情報を提供できるメタデータを含めることができます。たとえば、メタデータから、カメラのモデル、場所、日時、ビデオ ファイルの作成または編集に使用されたソフトウェアを明らかにできます。ファイルのメタデータを照会するために、セキュリティ アナリストは、MediaInfo、ffprobe、hexdump などのさまざまなツールを使用して、ビデオ ファイルからメタデータを抽出して表示できます。ファイルのメタデータを照会することで、セキュリティ アナリストは、作成日とファイルの作成者、およびその他の関連情報の両方を特定できる可能性が高くなります。ファイルの SHA-256 ハッシュの取得、エンドポイント ログの確認、ファイルの内容に対する hexdump の使用などのアクションも考えられますが、質問に答えるには最適な方法ではありません。ファイルの SHA-256 ハッシュは、ファイルの整合性や一意性を検証するために使用できる暗号化値ですが、ファイルの作成日や作成者に関する情報は明らかにしません。エンドポイント ログを確認すると、ファイルの出所やアクティビティに関する手がかりが得られますが、特にログが改ざんされていたり不完全だったりする場合は、信頼性や正確性に欠ける可能性があります。ファイルの内容に hexdump を使用すると、ファイルの生のバイナリ データを表示できますが、特にファイルが大きい場合や暗号化されている場合は、16 進出力からメタデータを解釈するのは簡単ではないか不可能です。

最新問題**: 130**
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
Answer: (解答を表示する**)**
説明
正解は A です。多要素認証 (MFA) は、ユーザーが知っている情報 (パスワードなど)、ユーザーが所有している情報 (トークンなど)、ユーザーがどのような人物であるか (生体認証など) など、複数の要素を要求することでユーザーの ID を確認する方法です。MFA では、攻撃者がログインするために別の要素を提供する必要があるため、ユーザーのパスワードが

侵害された場合でも不正アクセスを防止できます。その他の選択肢は、認証の弱さという攻撃の根本的な原因に対処していないため、正しくありません。
権限の割り当て (B) は、ユーザーの役割または ID に基づいてリソースへのアクセスを許可または拒否するプロセスです。アクセス管理は、誰が何にどのような条件でアクセスできるかを制御するプロセスです。パスワードの複雑さ (D) は、推測や解読が困難な強力なパスワードを使用する必要があることを意味しますが、攻撃者が盗んだパスワードを使用することを防ぐことはできません。参考資料 = 多要素認証やその他のセキュリティの概念の詳細については、次のリソースを参照してください。
CompTIA Security+ SY0-701 認定学習ガイド、第 1 章: 一般的なセキュリティ概念1
Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 1.2: セキュリティ概念2 多要素認証 - SY0-601 CompTIA Security+: 2.43 合計: CompTIA Security+ 認定 (SY0-701) | Udemy、セクション 3: アイデンティティとアクセス管理、講義 15: 多要素認証4 CompTIA Security+ 認定 SY0-601: 総合コース [ビデオ]、第 3 章: アイデンティティとアカウント管理、セクション 2: 多要素認証の有効化5

最新問題**: 131**
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
Answer: (解答を表示する**)**
説明
レガシー サーバーは、セキュリティ リスクや互換性の問題を引き起こす可能性のある、古いまたはサポートされていないソフトウェアまたはハードウェアを実行しているサーバーです。重要なビジネス アプリケーションは、会計、給与計算、在庫管理など、ビジネスの運用と継続に不可欠なアプリケーションです。重要なビジネス アプリケーションを実行しているレガシー サーバーは、交換やアップグレードが難しい場合がありますが、セキュリティ保護されていないままにしたり、潜在的な脅威にさらされたりしないようにする必要があります。
重要なビジネス アプリケーションを実行しているレガシー サーバーを管理する最善の方法の 1 つは、それを強化することです。強化とは、攻撃対象領域と脆弱性を減らすために、システムにセキュリティ対策と構成を適用するプロセスです。レガシー サーバーの強化には、次のような手順が含まれます。
オペレーティング システムとアプリケーションにパッチとアップデートを適用する (利用可能な場合) 不要なサービス、機能、またはアカウントを削除または無効化する ファイアウォール ルールとネットワーク アクセス制御リストを構成して、受信トラフィックと送信トラフィックを制限する データの転送と保存の暗号化と認証を有効にする 異常なアクティビティや悪意のあるアクティビティを検出して対応するためのロギング ツールと監

視ツールを実装する システムとアプリケーションの定期的なバックアップとテストを実行する レガシー サーバーを強化すると、重要なビジネス アプリケーションを不正アクセス、変更、または中断から保護しながら、その機能と可用性を維持できます。ただし、レガシー サーバーの強化は永続的なソリューションではなく、古いシステムやサポートされていないシステムによってもたらされるすべてのセキュリティの問題と課題に対処するには不十分な場合があります。したがって、レガシー サーバーの最終的な廃止またはより安全で最新のプラットフォームへの移行をできるだけ早く計画することをお勧めします。
参考資料: CompTIA Security+ SY0-701 認定試験学習ガイド、第 3 章: アーキテクチャと設計、セクション 3.2: セキュア システム設計、133 ページ 1; CompTIA Security+ 認定試験の目的、ドメイン
3: アーキテクチャと設計、目標 3.2: 安全なシステム設計の重要性を説明する、サブ目標: レガシーシステム 2

最新問題**: 132**
システム管理者は、多数のエンド ユーザーのアカウント作成時に時間を節約し、人為的エラーを防ぐスクリプトを作成しています。このタスクに適した使用例はどれですか。
A. 市販ソフトウェア
B. オーケストレーション
C. ベースライン
D. ポリシーの適用
Answer: B (メーッセージを残す**)**
説明
オーケストレーションは、さまざまなシステムやアプリケーション間で複数のタスクを自動化するプロセスです。定義済みのワークフローやスクリプトを実行することで、時間を節約し、人的エラーを減らすことができます。この場合、システム管理者はオーケストレーションを使用して、手動で情報を入力し、権限を割り当てることなく、多数のエンドユーザーのアカウントを作成できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、457 ページ 1

最新問題**: 133**
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 -スクリプト telnet暗号化
港湾サービス理由
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
セキュリティアナリストは、報告されたこの脆弱性について、次のどれを結論付けるでしょうか?
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。
Answer: A (メーッセージを残す**)**
誤検知とは、実際には脆弱性や問題がないのに、脆弱性や問題があると示す結果のことです。この場合、脆弱性スキャン レポートには、ポート 23 の Telnet サービスが開いており、安全でないネットワーク プロトコルを使用していることが示されています。ただし、セキュリティ アナリストは、nmap と、Telnet 暗号化サポートを確認するスクリプトを使用してテストを実行します。結果は、Telnet サーバーが暗号化をサポートしていることを示しています。つまり、クライアントとサーバー間で送信されるデータは盗聴から保護できます。したがって、報告された脆弱性は誤検知であり、サーバーの実際のセキュリティ状態を反映していません。セキュリティ アナリストは、Telnet サーバーとクライアントの暗号化設定を確認し、適切に構成されていることを確認する必要があります3。参考資料: 3: Telnet プロトコル - Telnet を暗号化できますか?

最新問題**: 134**
セキュリティ アナリストは、従業員の会社のラップトップから送信される悪意のあるネットワーク トラフィックの可能性に関する SIEM のアラートを確認しています。セキュリティ アナリストは、調査を続けるには、マシンで実行されている実行可能ファイルに関する追加データが必要であると判断しました。アナリストは、次のログのうちどれをデータソースとして使用する必要がありますか。
A. アプリケーション
B. IPS/IDS
C. ネットワーク
D. エンドポイント
Answer: (解答を表示する**)**
エンドポイント ログは、ラップトップ、デスクトップ、タブレット、スマートフォンなどのエンド ユーザー デバイスで発生するアクティビティとイベントに関する情報を含むファイルです。エンドポイント ログは、デバイスで実行されているプロセス、確立されたネットワーク接続、アクセスまたは変更されたファイル、実行されたユーザー アクション、インストールまたは更新されたアプリケーションなど、セキュリティ アナリストにとって貴重なデータを提供できます。エンドポイント ログには、デバイスで実行されている実行可能ファイルの詳細 (実行可能ファイルの名前、パス、サイズ、ハッシュ、署名、アクセス許可など) も記録されます。

アプリケーション ログは、エラー、警告、トランザクション、パフォーマンス メトリックなど、ソフトウェア アプリケーション内で発生するイベントに関する情報を含むファイルです。アプリケーション ログは、開発者や管理者が問題のトラブルシューティング、パフォーマンスの最適化、ユーザーの動作の監視を行うのに役立ちます。ただし、デバイスで実行されている実行可能ファイル (特に悪意のあるファイルや不明なファイル) に関する十分な情報がアプリケーション ログに含まれない場合があります。
IPS/IDS ログは、侵入防止システム (IPS) または侵入検知システム (IDS) によって監視および分析されるネットワーク トラフィックに関する情報を含むファイルです。IPS/IDS ログは、セキュリティ アナリストがエクスプロイトの試み、サービス拒否 (DoS) 攻撃、悪意のあるスキャンなどの潜在的な攻撃を特定してブロックするのに役立ちます。ただし、IPS/IDS ログでは、デバイスで実行されている実行可能ファイルに関する十分な情報が提供されない場合があります。特に、実行可能ファイルが暗号化、難読化されている場合や、正当なプロトコルを使用している場合はそうです。
ネットワーク ログは、IP アドレス、ポート、プロトコル、パケット、バイトなど、デバイス間で発生するネットワーク アクティビティと通信に関する情報を含むファイルです。ネットワーク ログは、セキュリティ アナリストがネットワーク トポロジ、トラフィック パターン、帯域幅の使用状況を把握するのに役立ちます。ただし、デバイスで実行されている実行可能ファイル (特に、ファイルが隠されていたり、偽装されていたり、プロキシ サーバーを使用していたりする場合) に関する十分な情報がネットワーク ログから得られない場合があります。
したがって、マシン上で実行されている実行可能ファイルに関する追加情報のデータ ソースとして使用するのに最適なログ タイプはエンドポイント ログです。エンドポイント ログは、実行可能ファイルとその動作に関する最も関連性の高い詳細なデータを提供できるためです。
参考資料 = https://www.crowdstrike.com/cybersecurity-101/observability/application-log/ https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

最新問題: **135**
セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに従うべき事項は次のどれですか。
A. 災害復旧計画
B. インシデント対応手順
C. 事業継続計画
D. 変更管理手順
Answer: (解答を表示する**)**
変更管理手順とは、セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに従わなければならない一連の手順とガイドラインです。ファイアウォールは、定義済みのルールまたはポリシーに基づいてネットワーク トラフィックをフィルタリング、ブロック、または許可できるデバイスまたはソフトウェアです。ファイアウォール ルールとは、ファイアウォールがパケットまたは接続に適用する基準とアクションを定義するス

テートメントです。たとえば、ファイアウォール ルールは、送信元と宛先の IP アドレス、ポート、プロトコル、またはアプリケーションに基づいてトラフィックを許可または拒否できます。新しいファイアウォール ルール セットを設定することは、ネットワークのセキュリティ、パフォーマンス、および機能に影響を与える可能性のある変更の一種です。したがって、変更が管理された一貫した方法で計画、テスト、承認、実装、文書化、およびレビューされるようにするには、変更管理手順が必要です。変更管理手順には通常、次の要素が含まれます。
* 変更の目的、範囲、影響、利点、および変更の所有者、実装者、承認者の役割と責任を説明する変更要求。
* 変更の実現可能性、リスク、コスト、依存性、および代替案と緊急時対応計画を評価する変更評価。
* 変更ポリシーで定義された基準としきい値に基づいて、変更を実装段階に進めることを承認する変更承認。
* 計画とスケジュールに従って変更を実行し、変更の結果と成果を検証する変更実装。
* 変更の詳細とステータス、学んだ教訓、ベスト プラクティスを記録した変更ドキュメント。
* 変更のパフォーマンスと有効性を監視および測定し、対処または改善が必要な問題やギャップを特定する変更レビュー。
変更管理手順は、セキュリティ管理者が新しいファイアウォール ルール セットを設定するときに遵守することが重要であり、次の目的の達成に役立ちます。
* ファイアウォール ルールがセキュリティ ポリシーと標準に準拠し、脆弱性や競合が発生しないようにすることで、ネットワークのセキュリティ体制とコンプライアンスを強化します。
* ファイアウォール ルールが展開前にテストおよび検証され、ネットワーク サービスまたはアプリケーションの可用性や機能に影響を与えないようにすることで、ネットワークの中断とダウンタイムを最小限に抑えます。
* ファイアウォール ルールがネットワーク ユーザーと関係者の変化するニーズと要求に応じて最適化および更新され、パフォーマンスや互換性の問題が発生しないようにすることで、ネットワークの効率と品質を向上させます。
* ファイアウォール ルールが文書化され、定期的にレビューされ、関係当局や関係者によって追跡および監査可能であることを保証することで、ネットワークの説明責任と透明性を高めます。
その他のオプションは、新しいファイアウォール ルールのセットを設定するプロセスに関連していないため、正しくありません。災害復旧計画は、システム障害、自然災害、その他の緊急事態が発生した場合に組織の通常の運用を回復することを目的とした一連のポリシーと手順です。インシデント対応手順は、サイバー攻撃、データ侵害、マルウェア感染などのセキュリティ インシデントの封じ込め、分析、根絶、および回復を目的とした一連の手順とガイドラインです。事業継続計画は、パンデミック、停電、市民の暴動などの混乱を引き起こすイベントの発生中および発生後に組織の重要な機能と運用を維持することを目的とし

た一連の戦略とアクションです。参考文献 = CompTIA Security+ 学習ガイド (SY0-701)、第 7 章: 回復力と回復、325 ページ。メッサー教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 1.3: セキュリティ運用、ビデオ: 変更管理 (5:45)。

最新問題: **136**
ある組織は、不要なサービスを無効にし、ビジネスクリティカルなレガシー システムの前にファイアウォールを配置しました。
組織が取った行動を最もよく表しているのはどれですか?
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
Answer: D (メーッセージを残す**)**
代替制御は、主要な制御が実行不可能、費用対効果が低い、またはリスクを軽減するのに十分でない場合に実装される代替セキュリティ対策です。この場合、組織は、不要なサービスを無効にし、その前にファイアウォールを配置することで、潜在的な攻撃からレガシー システムを保護するために代替制御を使用しました。これにより、攻撃対象領域と悪用される可能性が減りました。
参考文献:
公式 CompTIA Security+ 学習ガイド (SY0-701)、29 ページ
セキュリティコントロール - CompTIA Security+ SY0-701 - 1.1 1

最新問題: **137**
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
Answer: (解答を表示する**)**

ファームウェアは、ルーター、プリンター、BIOS チップなどのハードウェア デバイスに組み込まれているソフトウェアの一種です。ファームウェアはデバイスの基本的な機能と操作を制御し、製造元またはユーザーが更新または変更できます。ファームウェア バージョンはハードウェア固有の脆弱性であり、古くなっていたり、破損していたり、改ざんされていたりすると、デバイスがセキュリティ リスクにさらされる可能性があります。攻撃者はファームウェアの脆弱性を悪用して、不正アクセス、デバイス設定の変更、マルウェアのインストール、デバイスまたはネットワークへの損害を引き起こす可能性があります。したがって、ファームウェアを最新の状態に保ち、その整合性と信頼性を確認することが重要です。参考資料 = CompTIA Security+ 学習ガイド (500 問以上の模擬試験問題付き): 試験 SY0-701、第 9 版、第 2 章、67 ページ。CompTIA Security+ SY0-701 試験目標、ドメイン 2.1、10 ページ。

最新問題: **138**
セキュリティ管理者は、従業員のラップトップ上のデータを保護したいと考えています。セキュリティ管理者は次のどの暗号化手法を使用する必要がありますか?
A. パーティション
B. 非対称
C. ディスクがいっぱい
D. データベース
Answer: C (メーッセージを残す**)**
フルディスク暗号化 (FDE) は、オペレーティングシステム、アプリケーション、ファイルなど、ハードドライブ上のすべてのデータを暗号化する技術です。FDE は、ラップトップが紛失、盗難、または適切なサニタイズを行わずに廃棄された場合に、不正アクセスからデータを保護します。FDE では、ドライブのロックを解除してシステムを起動するために、ユーザーはパスワード、PIN、スマートカード、または生体認証要素を入力する必要があります。FDE は、BitLocker、FileVault、VeraCrypt などのソフトウェアソリューション、または自己暗号化ドライブ (SED) や Trusted Platform Modules (TPM) などのハードウェアソリューションを使用して実装できます。FDE は、機密データを保存するラップトップやその他のモバイルデバイスに推奨される暗号化技術です。
パーティション暗号化は、ハード ドライブ上の特定のパーティションまたはボリュームのみを暗号化し、ドライブの残りの部分は暗号化しない技術です。パーティション暗号化は、ドライブ全体を保護せず、暗号化されていない領域にデータの痕跡が残る可能性があるため、FDE よりも安全性が低くなります。パーティション暗号化は、ユーザーが暗号化されたパーティションを手動でマウントおよびマウント解除する必要があるため、FDE よりも使い勝手が悪くなります。
非対称暗号化は、公開キーと秘密キーのペアを使用してデータを暗号化および復号化する手法です。非対称暗号化は、保存データの暗号化ではなく、電子メール、Web、VPN などの通信のセキュリティ保護に主に使用されます。また、非対称暗号化は、FDE やパーティショ

ン暗号化で使用されるタイプの暗号化である対称暗号化よりも遅く、計算量が多くなります。
データベース暗号化は、テーブル、列、行、セルなど、データベースに保存されているデータを暗号化する手法です。データベース暗号化は、アプリケーション レベル、データベース レベル、またはファイル システム レベルで実行できます。
データベースの暗号化は、データベース管理者、ハッカー、またはマルウェアによる不正アクセスからデータを保護するのに便利ですが、データベースをホストするデバイスの物理的な盗難や紛失からデータを保護することはできません。
参考資料 = データ暗号化 - CompTIA Security+ SY0-401: 4.4、CompTIA Security+ チートシートと PDF | Zero To Mastery、CompTIA Security+ SY0-601 認定コース - Cybr、アプリケーション強化 - SY0-601 CompTIA Security+: 3.2。

最新問題**: 139**
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
Answer: (解答を表示する**)**
暗号化とは、データを平文に戻すために必要な秘密鍵がなければ読み取れないようにデータを変換する方法です。暗号化は、データの不正アクセス、変更、盗難を防ぐため、保存中のデータを保護する最も一般的で効果的な方法の 1 つです。暗号化は、ブロック ストレージ、オブジェクト ストレージ、データベース、アーカイブなど、さまざまな種類の保存データに適用できます。ハッシュ、トークン化、セグメンテーションは、保存中のデータを読み取り不可能にする方法ではなく、他の方法でデータを保護する方法です。ハッシュは、入力からハッシュまたはダイジェストと呼ばれる固定長の出力を生成する一方向関数であり、出力から入力を復元することはできません。ハッシュは、データの整合性と信頼性を検証するために使用されますが、データを暗号化するものではありません。トークン化は、機密データを、それ自体では意味や価値のないトークンと呼ばれる非機密の代替物に置き換えるプロセスです。トークン化は、機密データの露出とコンプライアンスの範囲を縮小するために使用されますが、暗号化するものではありません。セグメンテーションとは、ネットワークまたはシステムをセグメントと呼ばれる、アクセスとセキュリティのレベルが異なる小さな独立した単位に分割する手法です。セグメンテーションは、攻撃対象を制限し、侵害の影響を抑えるために使用されますが、保存されているデータを暗号化するものではありません。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、ページ 77-781; 保存データの保護 - セキュリティの柱3

最新問題**: 140**

セキュリティ アナリストがアプリケーション サーバーを調査しているときに、サーバー上のソフトウェアが異常な動作をしていることを発見しました。このソフトウェアは通常、バッチ ジョブをローカルで実行し、トラフィックを生成しませんが、プロセスがランダムな高ポートを介して送信トラフィックを生成しています。このソフトウェアで悪用された可能性のある脆弱性は次のどれですか。
A. メモリインジェクション
B. 競合状態
C. サイドローディング
D. SQLインジェクション
Answer: (解答を表示する**)**
メモリ インジェクションの脆弱性により、ソフトウェア プログラム内で不正なコードやコマンドが実行され、ランダムな高ポート経由で送信トラフィックが生成されるなどの異常な動作が発生します。この問題は、ソフトウェアが入力を適切に検証またはエンコードしていないために発生することが多く、攻撃者が悪意のあるコードを挿入するために悪用される可能性があります。

最新問題**: 141**
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
Answer: A (メーッセージを残す**)**
要塞ホストは、攻撃に耐え、内部リソースへの安全なアクセスを提供するように設計された特殊用途のサーバーです。要塞ホストは通常、ネットワークのエッジに配置され、内部ネットワークへのゲートウェイまたはプロキシとして機能します。要塞ホストは、SSH や HTTP などの特定の種類のトラフィックのみを許可し、他のすべてのトラフィックをブロックするように構成できます。要塞ホストは、ファイアウォール、侵入検知システム、ウイルス対策プログラムなどのセキュリティ ソフトウェアを実行して、着信トラフィックと発信トラフィックを監視およびフィルタリングすることもできます。要塞ホストは、強力な認証と暗号化を要求し、監査目的ですべてのアクティビティをログに記録することで、内部リソースへの管理アクセスを提供できます12。
要塞ホストは、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、単一の制御ポイントと防御ポイントを提供するため、与えられたオプションの中で最も安全な方法です。要塞ホストは、内部ネットワークをインターネットやその他の信頼できないネットワークへの直接的な露出から分離し、攻撃対象領域と侵害のリスクを軽減することもできます3。

境界ネットワークを展開することは正しい答えではありません。境界ネットワークは、内部ネットワークを外部ネットワークから分離するネットワーク セグメントだからです。境界ネットワークは通常、インターネットからアクセスする必要がある Web サーバー、電子メール サーバー、DNS サーバーなどの公開サービスをホストします。境界ネットワークは内部リソースへの管理アクセスを提供するのではなく、不正アクセスから保護します。境界ネットワークは、ネットワーク管理とセキュリティの複雑さとコストを増大させる可能性もあります4。
WAF をインストールすることは正解ではありません。WAF は、HTTP トラフィックを監視、フィルタリング、ブロックすることで、一般的な Web ベースの攻撃から Web アプリケーションを保護するセキュリティ ツールだからです。WAF は、クロスサイト スクリプティング、SQL インジェクション、ファイル インクルードなどの攻撃を防ぐことができます。WAF は内部リソースへの管理アクセスを提供するのではなく、Web アプリケーションの脆弱性から内部リソースを保護します。また、WAF はアプリケーション層でのみ動作し、他の種類の攻撃や脅威から保護しないため、ネットワーク セキュリティの包括的なソリューションではありません5。
シングル サインオンを利用するのは正解ではありません。シングル サインオンは、ユーザーが 1 つのユーザー名とパスワードで複数のサイト、サービス、またはアプリケーションにアクセスできる認証方法だからです。シングル サインオンを使用すると、ユーザーのサインイン プロセスが簡素化され、覚えて管理しなければならないパスワードの数を減らすことができます。シングル サインオンでは、内部リソースへの管理アクセスは提供されませんが、ユーザーが使用を許可されているさまざまなリソースへのアクセスが可能になります。また、ユーザーの資格情報が侵害された場合やシングル サインオン プロバイダーが侵害された場合、シングル サインオンによってセキュリティ リスクが生じる可能性があります6。参考文献 = 1: 要塞ホスト - Wikipedia、2: SSH 要塞ホストを保護するための 14 のベスト プラクティス - goteleport.com、3: ネットワーク セキュリティにおける要塞ホストの重要性、4: ネットワーク境界とは何ですか? | Cloudflare、5: WAF とは何ですか? | Web アプリケーション ファイアウォールの説明、6: [シングル サインオン (SSO) とは何ですか? - WhatIs.com の定義]

最新問題**: 142**
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
Answer: A (メーッセージを残す**)**

最新問題**: 143**

次のどれがメッセージを個人に帰属させることを可能にしますか?
A. 適応型アイデンティティ
B. 否認防止
C. 認証
D. アクセスログ
Answer: B (メーッセージを残す**)**
否認防止とは、メッセージまたは文書が特定の人物によって送信または署名されたことを証明し、その人物が送信または署名を否定できないようにする機能です。否認防止は、ハッシュやデジタル署名などの暗号化技術を使用して、メッセージまたは文書の信頼性と整合性を検証することで実現できます。否認防止は、メッセージまたは文書の発信元と内容の証拠を提供できるため、法律、財務、または契約上の目的に役立ちます。

最新問題**: 144**
セキュリティ アナリストは、従業員の会社のラップトップから送信される悪意のあるネットワーク トラフィックの可能性に関する SIEM のアラートを確認しています。セキュリティ アナリストは、調査を続けるには、マシンで実行されている実行可能ファイルに関する追加データが必要であると判断しました。アナリストは、次のログのうちどれをデータソースとして使用する必要がありますか。
A. アプリケーション
B. IPS/IDS
C. ネットワーク
D. エンドポイント
Answer: D (メーッセージを残す**)**
エンドポイント ログは、ラップトップ、デスクトップ、タブレット、スマートフォンなどのエンド ユーザー デバイスで発生するアクティビティとイベントに関する情報を含むファイルです。エンドポイント ログは、デバイスで実行されているプロセス、確立されたネットワーク接続、アクセスまたは変更されたファイル、実行されたユーザー アクション、インストールまたは更新されたアプリケーションなど、セキュリティ アナリストにとって貴重なデータを提供できます。エンドポイント ログには、デバイスで実行されている実行可能ファイルの詳細 (実行可能ファイルの名前、パス、サイズ、ハッシュ、署名、アクセス許可など) も記録されます。
アプリケーション ログは、エラー、警告、トランザクション、パフォーマンス メトリックなど、ソフトウェア アプリケーション内で発生するイベントに関する情報を含むファイルです。アプリケーション ログは、開発者や管理者が問題のトラブルシューティング、パフォーマンスの最適化、ユーザーの動作の監視を行うのに役立ちます。ただし、デバイスで実行されている実行可能ファイル (特に悪意のあるファイルや不明なファイル) に関する十分な情報がアプリケーション ログに含まれない場合があります。
IPS/IDS ログは、侵入防止システム (IPS) または侵入検知システム (IDS) によって監視および分析されるネットワーク トラフィックに関する情報を含むファイルです。IPS/IDS ログは、セキュリティ アナリストがエクスプロイトの試み、サービス拒否 (DoS) 攻撃、悪意の

あるスキャンなどの潜在的な攻撃を特定してブロックするのに役立ちます。ただし、IPS/IDS ログでは、デバイスで実行されている実行可能ファイルに関する十分な情報が提供されない場合があります。特に、実行可能ファイルが暗号化、難読化されている場合や、正当なプロトコルを使用している場合はそうです。
ネットワーク ログは、IP アドレス、ポート、プロトコル、パケット、バイトなど、デバイス間で発生するネットワーク アクティビティと通信に関する情報を含むファイルです。ネットワーク ログは、セキュリティ アナリストがネットワーク トポロジ、トラフィック パターン、帯域幅の使用状況を把握するのに役立ちます。ただし、デバイスで実行されている実行可能ファイル (特に、ファイルが隠されていたり、偽装されていたり、プロキシ サーバーを使用していたりする場合) に関する十分な情報がネットワーク ログから得られない場合があります。
したがって、マシン上で実行されている実行可能ファイルに関する追加情報のデータ ソースとして使用するのに最適なログ タイプはエンドポイント ログです。エンドポイント ログは、実行可能ファイルとその動作に関する最も関連性の高い詳細なデータを提供できるためです。
参照 = https://www.crowdstrike.com/cybersecurity-101/observability/application-log/ https://owasp.org/www-project-proactive-controls/v3/en/c9-security-logging

最新問題**: 145**
セキュリティ管理者は、従業員のラップトップ上のデータを保護したいと考えています。セキュリティ管理者は次のどの暗号化手法を使用する必要がありますか?
A. パーティション
B. 非対称
C. ディスクがいっぱい
D. データベース
Answer: C (メーッセージを残す**)**
説明
フルディスク暗号化 (FDE) は、オペレーティングシステム、アプリケーション、ファイルなど、ハードドライブ上のすべてのデータを暗号化する技術です。FDE は、ラップトップが紛失、盗難、または適切なサニタイズを行わずに廃棄された場合に、不正アクセスからデータを保護します。FDE では、ドライブのロックを解除してシステムを起動するために、ユーザーはパスワード、PIN、スマートカード、または生体認証要素を入力する必要があります。FDE は、BitLocker、FileVault、VeraCrypt などのソフトウェアソリューション、または自己暗号化ドライブ (SED) や Trusted Platform Modules (TPM) などのハードウェアソリューションを使用して実装できます。FDE は、機密データを保存するラップトップやその他のモバイルデバイスに推奨される暗号化技術です。
パーティション暗号化は、ハード ドライブ上の特定のパーティションまたはボリュームのみを暗号化し、ドライブの残りの部分は暗号化しない技術です。パーティション暗号化は、ドライブ全体を保護せず、暗号化されていない領域にデータの痕跡が残る可能性があるため、FDE よりも安全性が低くなります。パーティション暗号化は、ユーザーが暗号化された

パーティションを手動でマウントおよびマウント解除する必要があるため、FDE よりも使い勝手が悪くなります。
非対称暗号化は、公開キーと秘密キーのペアを使用してデータを暗号化および復号化する手法です。非対称暗号化は、保存データの暗号化ではなく、電子メール、Web、VPN などの通信のセキュリティ保護に主に使用されます。また、非対称暗号化は、FDE やパーティション暗号化で使用されるタイプの暗号化である対称暗号化よりも遅く、計算量が多くなります。
データベース暗号化は、テーブル、列、行、セルなど、データベースに保存されているデータを暗号化する手法です。データベース暗号化は、アプリケーション レベル、データベース レベル、またはファイル システム レベルで実行できます。
データベースの暗号化は、データベース管理者、ハッカー、またはマルウェアによる不正アクセスからデータを保護するのに便利ですが、データベースをホストするデバイスの物理的な盗難や紛失からデータを保護することはできません。
参考資料 = データ暗号化 - CompTIA Security+ SY0-401: 4.4、CompTIA Security+ チートシートと PDF | Zero To Mastery、CompTIA Security+ SY0-601 認定コース - Cybr、アプリケーション強化 - SY0-601 CompTIA Security+: 3.2。

最新問題**: 146**
管理者が単一サーバーのセキュリティ ログを確認したところ、次のことが分かりました。このログ ファイルに記録されたアクションを最もよく表すのは次のどれですか。
A. ブルートフォース攻撃
B. 権限昇格
C. パスワード監査に失敗しました
D. ユーザーがパスワードを忘れた
Answer: (解答を表示する**)**
ブルート フォース攻撃は、正しいパスワードまたはキーが見つかるまで、すべての可能なパスワードまたはキーの組み合わせを体系的に試す攻撃の一種です。ログ ファイルには、短時間に複数の失敗したログイン試行が記録されます。これはブルート フォース攻撃の特徴です。
攻撃者はサーバーの管理者アカウントのパスワードを推測しようとしています。ログファイルには、失敗したログオン試行を示すイベントID 4625とステータスコードも表示されます。
0xC000006A は、ユーザー名は正しいがパスワードが間違っていることを意味します。これらは、ブルート フォース攻撃が行われていることを示す侵害の兆候 (IoC) です。

最新問題**: 147**
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
Answer: A (メーッセージを残す**)**
準備は、インシデント対応プロセスにおいて、セキュリティ アナリストが役割と責任、およびインシデントを処理するためのポリシーと手順を確認する段階です。準備には、インシデントに対応するために必要なツール、リソース、および連絡先の収集と維持も含まれます。準備により、セキュリティ アナリストは、インシデントが発生したときに準備を整えて積極的に対応できるようになり、インシデントの影響と期間を短縮できます。
セキュリティ アナリストが準備フェーズで実行するアクティビティの一部は次のとおりです。
インシデント マネージャー、インシデント コーディネーター、技術リーダー、コミュニケーション リーダー、法務顧問などのインシデント対応チーム メンバーの役割と責任を定義します。
インシデント対応計画を確立し、インシデントに対応するための目的、範囲、権限、手順、およびエスカレーションと報告のメカニズムを概説します。
インシデントの種類とカテゴリ、重大度レベル、通知および報告の要件、関係者の役割と責任を定義するインシデント対応ポリシーを開発します。
インシデント対応プレイブックを作成します。このプレイブックには、サービス拒否、ランサムウェア、フィッシング、データ侵害などの特定の種類のインシデントを処理するためのステップバイステップのガイダンスとチェックリストが記載されています。
ネットワークおよびホストベースのスキャナー、マルウェア分析ツール、フォレンジック ツール、バックアップおよびリカバリ ツール、コミュニケーションおよびコラボレーション ツールなどのインシデント対応ツールを取得してテストします。
インシデント対応チーム、インシデント対応場所、証拠保管場所、外部サポートなどのインシデント対応リソースを特定し、保護します。
社内外の利害関係者、法執行機関、規制機関、メディアなどのインシデント対応連絡先を構築および維持します。
参照：
CompTIA Security+ SY0-701 認定試験学習ガイド、第 6 章: アーキテクチャと設計、セクション 6.4: セキュア システム設計、p. 279-280 CompTIA Security+ SY0-701 認定試験の目標、ドメイン 3: アーキテクチャと設計、目標 3.5: シナリオに基づいて、セキュア ネットワーク アーキテクチャの概念を実装する、サブ目標: インシデント対応、p. 16

最新問題**: 148**
セキュリティ アナリストと管理チームは、最近のフィッシング キャンペーンの組織パフォーマンスを確認しています。ユーザーのクリックスルー率が許容リスクしきい値を超えたため、管理チームはユーザーがフィッシング メッセージ内のリンクをクリックしたと

きの影響を軽減したいと考えています。アナリストは次のうちどれを行う必要がありますか。
A. 一般的なフィッシング行為に対する認識を高めるために、オフィスのあちこちにポスターを貼ります。
B. フィッシングメールが配信されないようにメールセキュリティフィルターを実装する
C. ダウンロードしたプログラムの自動実行をブロックするように EDR ポリシーを更新します。
D. ユーザーがフィッシング攻撃の兆候を認識できるように、追加のトレーニングを作成します。
Answer: (解答を表示する**)**
エンドポイント検出および対応 (EDR) システムは、コンピューター、ラップトップ、モバイル デバイス、サーバーなどのエンドポイントのアクティビティと動作を監視および分析するセキュリティ ツールです。EDR システムは、マルウェア、ランサムウェア、フィッシング、高度な持続的脅威 (APT) など、さまざまな種類の脅威を検出し、防止し、対応することができます。EDR システムの機能の 1 つは、ダウンロードされたプログラムの自動実行をブロックすることです。これにより、ユーザーがフィッシング メッセージ内のリンクをクリックしたときに、エンドポイントで悪意のあるコードが実行されることを防ぐことができます。これにより、フィッシング攻撃の影響を軽減し、エンドポイントを侵害から保護できます。ダウンロードされたプログラムの自動実行をブロックするように EDR ポリシーを更新することは、ユーザーの認識や動作に関係なく、フィッシングのリスクを軽減できる技術的な制御です。したがって、これは与えられたオプションの中で最適な答えです。
その他のオプションは、EDR ポリシーの更新ほど効果的ではありません。管理上または物理的な制御に依存しているため、フィッシング攻撃を防止または阻止するには不十分な場合があります。一般的なフィッシング活動に関する認識を高めるためにオフィスのあちこちにポスターを貼ることは、ユーザーのフィッシングに関する知識を高める物理的な制御ですが、ユーザーの行動を変えたり、フィッシング メッセージ内のリンクをクリックするのを防いだりすることはできない可能性があります。フィッシング メールの配信を防ぐメール セキュリティ フィルターを実装することは、フィッシングにさらされる可能性を減らす管理上の制御ですが、特にフィルターをバイパスするように作成されたフィッシング メールの場合は、すべてのフィッシング メールをブロックできない可能性があります。
ユーザーがフィッシングの試みの兆候を認識できるようにするための追加のトレーニングを作成することは、ユーザーのフィッシング検出スキルを向上させる管理上の制御ですが、メールを受信するときに常に警戒したり用心深くなったりするとは限りません。
したがって、これらのオプションはこの質問に対する最適な回答ではありません。参考資料 = エンドポイント検出および応答 - CompTIA Security+ SY0-701 - 2.2、ビデオ 5:30、CompTIA Security+ SY0-701 認定学習ガイド、163 ページ。

最新問題**: 149**

セキュリティ アナリストは、業務時間外の短時間に、内部システムがインターネット上のシステムに大量の異常な DNS クエリを送信しているという警告を受け取ります。次のどれが最も発生していると考えられますか。
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。
Answer: B (メーッセージを残す**)**
データ流出は、攻撃者が DNS クエリと応答を介して機密データを送信することで、ターゲット システムまたはネットワークから機密データを盗むために使用する手法です。この方法は、攻撃者がターゲット環境での検出を継続的に回避しようとする、高度で持続的な脅威 (APT) 攻撃でよく使用されます。営業時間外の短時間にインターネット上のシステムに対して大量の異常な DNS クエリが送信されることは、データ流出の強力な指標です。ワーム、ロジック ボム、およびランサムウェアは、コマンド アンド コントロール サーバーと通信したり、悪意のあるアクションを実行したりするために DNS クエリを使用することはありません。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、487 ページ、DNS データ流出の概要、今回は現実ではなかった DNS 流出攻撃の特定

最新問題**: 150**
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
Answer: C (メーッセージを残す**)**
水飲み場型攻撃は、ユーザーグループが頻繁にアクセスする Web サイトに感染することで、そのユーザーグループを標的とするサイバー攻撃の一種です。攻撃者は脆弱性を悪用して、組織のネットワークに悪意のあるペイロードを送り込みます。この攻撃は、ユーザーのコンピューターを感染させ、接続されている企業ネットワークにアクセスすることを目的としています。攻撃者は、特定の組織または人口統計のメンバーに人気があることがわかっている Web サイトをターゲットにします。この攻撃は、通常、データを盗んだり、ユーザーのデバイスにマルウェアをインストールしたりしようとするフィッシング攻撃やスピアフィッシング攻撃とは異なります1 このシナリオでは、侵害された業界ブログは、攻撃者が会社のネットワーク全体にマルウェアを拡散するために使用した水飲み場です。攻撃者がこのブログを選んだのは、会社の従業員がそのコンテンツに興味を持ち、頻繁にアクセスしていることを知っていたためと考えられます。攻撃者は、ブログに悪意のあるコードを挿入したか、マルウェアをホストする偽の Web サイトに訪問者をリダイレクトした可能

性があります。その後、マルウェアは従業員のコンピューターに感染し、ネットワークに広がりました。
参照
1: ウォーターホール型攻撃: 段階、例、リスク要因、防御策...

最新問題: **151**
ある会社のエンドユーザーから、外部の Web サイトにアクセスできないという報告がありました。アナリストは、DNS サーバーのパフォーマンス データを調べたところ、CPU、ディスク、メモリの使用量は最小限であるものの、ネットワーク インターフェイスが受信トラフィックであふれていることを発見しました。ネットワーク ログには、このサーバーに送信された DNS クエリの数がわずかしか表示されていません。セキュリティ アナリストが見ている状況を最もよく表しているのは、次のどれですか。
A. 同時セッションの使用
B. セキュアDNS暗号化のダウングレード
C. パス上のリソース消費
D. 反射型サービス拒否
Answer: (解答を表示する**)**
リフレクション型サービス拒否 (RDoS) 攻撃は、偽装された送信元 IP アドレスを使用してサードパーティ サーバーにリクエストを送信し、サードパーティ サーバーが被害者サーバーに応答を送信する DDoS 攻撃の一種です。攻撃者は、リクエストと応答のサイズの違いを利用して、被害者サーバーに送信されるトラフィックの量を増やすことができます。また、攻撃者は被害者の IP アドレスを送信元として使用することで、自分の身元を隠します。RDoS 攻撃は、偽造された DNS クエリを送信して大きな DNS 応答を生成することで、DNS サーバーをターゲットにすることができます。これにより、DNS サーバーのネットワーク インターフェイスがフラッディングし、エンド ユーザーからの正当なリクエストを処理できなくなります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、215 ～ 216 ページ 1

最新問題: **152**
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. 塩漬け
Answer: (解答を表示する**)**
説明
ソルティングとは、ハッシュ関数などの一方向データ変換アルゴリズムを適用する前に、パスワードやその他のデータにランダムなデータを追加するプロセスです。ソルティングにより、入力データの複雑さとランダム性が増し、攻撃者が事前に計算されたテーブルやブルート フォース方式を使用して元のデータを推測したり解読したりすることが難しくなります。また、ソルティングは、同一のパスワードが同一のハッシュ値を生成するのを防ぐのにも役立ちます。同一のハッシュ値が生成されてしまうと、ハッシュ データにアクセスできる攻撃者にパスワードが漏れてしまう可能性があります。ソルティングは、データベースに保存されているパスワードやネットワーク経由で送信されるパスワードを保護するためによく使用されます。参考資料 = パスワードの技術概要 暗号化、ハッシュ、ソルティング - 違いは何ですか?
ソルト（暗号化）

最新問題: **153**
ある企業は、セキュリティ運用を主導するために、社外からセキュリティ マネージャーを雇いました。この新しい役割において、セキュリティ マネージャーが最初に実行する必要があるアクションは次のうちどれですか。
A. セキュリティ ベースラインを確立します。
B. セキュリティ ポリシーを確認します。
C. セキュリティベンチマークを採用します。
D. ユーザー ID の再検証を実行します。
Answer: B (メーッセージを残す**)**
セキュリティ マネージャーを組織外から雇用してセキュリティ運用を指揮させる場合、最初に行うべきことは既存のセキュリティ ポリシーを確認することです。現在のセキュリティ ポリシーを理解することで、強み、弱み、改善が必要な領域を特定するための基盤が得られ、セキュリティ プログラムが組織の目標や規制要件に合致していることが保証されます。
セキュリティ ポリシーを確認する: 既存のセキュリティ フレームワークを包括的に理解し、新しいマネージャーがギャップや強化すべき領域を特定できるようにします。
セキュリティ ベースラインを確立する: 重要ですが、既存のポリシーとプラクティスを十分に理解した上で行う必要があります。
セキュリティ ベンチマークを採用する: 標準を設定するのに役立ちますが、現在のポリシーを確認することが前提条件となります。

ユーザー ID の再検証を実行します。ユーザー アクセスが適切であることを確認するために重要ですが、全体的なセキュリティ操作を理解するための最初のステップではありません。

最新問題: **154**
エンジニアがネットワーク デバイスの廃止を推奨すべきケースは次のうちどれですか (2 つ選択)。
A. デバイスは実稼働環境からテスト環境に移動されました。
B. デバイスはクリアテキスト パスワードを使用するように構成されています。
C. デバイスは企業ネットワーク上の分離されたセグメントに移動されます。
D. デバイスが企業内の別の場所に移動されます。
E. デバイスの暗号化レベルが組織の標準を満たすことができません。
F. デバイスは承認された更新を受信できません。
Answer: E (メッセージを残す**)**
デバイスが企業環境にセキュリティ リスクやコンプライアンス違反をもたらす場合、エンジニアはネットワーク デバイスの廃止を推奨する必要があります。暗号化標準に準拠できないデバイスや承認された更新を受信できないデバイスは、攻撃や侵害に対して脆弱であり、機密データを公開したり、ネットワークの整合性を損なったりする可能性があります。したがって、このようなデバイスはネットワークから削除し、より安全で更新されたデバイスに置き換える必要があります。
参考文献
CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、セクション 2.2、671 ページ CompTIA Security+ 模擬試験: 試験 SY0-701、第 3 版、第 2 章、質問 16、512 ページ

最新問題: **155**
セキュリティ インシデントの発生中、セキュリティ運用チームは悪意のある IP アドレス 10.1.4.9 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。セキュリティ アナリストは、この IP アドレスが組織のネットワークにアクセスするのをブロックする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どれですか。
A. アクセスリスト インバウンド 拒否 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
B. アクセスリスト インバウンド 拒否 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
C. アクセスリスト インバウンド 許可 ig 送信元 0.0.0.0/0 宛先 10.1.4.9/32
D. アクセスリスト インバウンド 許可 ig 送信元 10.1.4.9/32 宛先 0.0.0.0/0
Answer: A (メッセージを残す**)**

最新問題: **156**
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. 拡張認証
B. 回復の容易さ

C. 応答性
D. 攻撃対象領域
E. 物理的な分離
F. パッチを当てる機能
Answer: B,D (メーッセージを残す**)**

最新問題**: 157**
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
Answer: A (メーッセージを残す**)**
説明
クラウド ホスティング プロバイダーがデータ センターを新しい海外の場所に拡張する前に最初に考慮すべきことは、現地のデータ保護規制です。データ保護規制とは、個人情報や機密データが国境を越えて収集、保存、処理、転送される方法を規定する法律または標準です。国や地域によってデータ保護規制は異なります。たとえば、欧州連合の一般データ保護規則 (GDPR)、カナダの個人情報保護および電子文書法 (PIPEDA)、米国のカリフォルニア州消費者プライバシー法 (CCPA) などです。クラウド ホスティング プロバイダーは、事業を展開したり顧客にサービスを提供したりする国や地域の現地のデータ保護規制に準拠する必要があります。準拠しない場合は、法的処罰、罰金、または評判の低下に直面する可能性があります。
したがって、クラウド ホスティング プロバイダーは、データ センターを拡張する前に、新しい海外拠点の現地データ保護規制を調査して理解する必要があります。参考資料 = 500 問以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 7 章、269 ページ。CompTIA Security+ SY0-701 試験目標、ドメイン 5.1、14 ページ。

最新問題**: 158**
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
Answer: (解答を表示する**)**

説明
高可用性ネットワークは、ダウンタイムを最小限に抑え、重要なサービスとアプリケーションの継続的な運用を保証するように設計されたネットワークです。この目標を達成するには、高可用性ネットワークでは、回復の容易さと攻撃対象領域という 2 つの重要な要素を考慮する必要があります。
回復の容易さは、障害、中断、または災害が発生した後に、ネットワークが通常の機能を迅速に回復できる能力を指します。高可用性ネットワークには、単一障害点によってネットワークが完全に停止することがないように、冗長性、フェイルオーバー、バックアップ、および復元などのメカニズムが必要です。また、高可用性ネットワークには、インシデント対応、災害復旧、およびビジネス継続性に関する手順とポリシーも必要であり、ネットワークの問題が組織の運用と評判に与える影響を最小限に抑えます。
攻撃対象領域とは、ネットワークが潜在的な脅威や脆弱性にさらされている状態を指します。高可用性ネットワークには、暗号化、認証、承認、ファイアウォール、侵入検知と防止、パッチ管理などの対策を講じて、不正アクセス、データ侵害、マルウェア、サービス拒否攻撃、その他のサイバー攻撃からネットワークを保護する必要があります。また、高可用性ネットワークには、リスク評価、脅威インテリジェンス、脆弱性スキャン、侵入テストなどのプロセスとツールも備え、ネットワーク セキュリティの弱点やギャップを特定して軽減する必要があります。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 4 章: アーキテクチャと設計、164 ～ 1651 ページ。CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 4 章:
建築とデザイン、164-1652ページ。

最新問題**: 159**
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
Answer: (解答を表示する**)**
水飲み場型攻撃は、ユーザーグループが頻繁にアクセスする Web サイトに感染することで、そのユーザーグループを標的とするサイバー攻撃の一種です。攻撃者は脆弱性を悪用して、組織のネットワークに悪意のあるペイロードを送り込みます。この攻撃は、ユーザーのコンピューターを感染させ、接続されている企業ネットワークにアクセスすることを目的としています。攻撃者は、特定の組織または人口統計のメンバーに人気があることがわかっている Web サイトをターゲットにします。この攻撃は、通常、データを盗んだり、ユーザーのデバイスにマルウェアをインストールしたりしようとするフィッシング攻撃やスピアフィッシング攻撃とは異なります1 このシナリオでは、侵害された業界ブログは、攻撃者

が会社のネットワーク全体にマルウェアを拡散するために使用した水飲み場です。攻撃者がこのブログを選んだのは、会社の従業員がそのコンテンツに興味を持ち、頻繁にアクセスしていることを知っていたためと考えられます。攻撃者は、ブログに悪意のあるコードを挿入したか、マルウェアをホストする偽の Web サイトに訪問者をリダイレクトした可能性があります。その後、マルウェアは従業員のコンピューターに感染し、ネットワークに広がりました。
参考資料 1: ウォーターホール型攻撃: 段階、例、リスク要因、防御策...

最新問題: **160**
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
Answer: (解答を表示する**)**
ホストベースのファイアウォールは、個々のエンドポイントで実行され、一連のルールに基づいて受信および送信ネットワーク トラフィックをフィルタリングするソフトウェア アプリケーションです。ホストベースのファイアウォールは、送信元、送信先、ポート、プロトコル、またはアプリケーションに基づいてトラフィックをブロックまたは許可することで、内部エンドポイント間の疑わしい接続によってもたらされる脅威を軽減するのに役立ちます。ホストベースのファイアウォールは、SQL インジェクション、クロスサイト スクリプティング、セッション ハイジャックなどの一般的な Web ベースの攻撃から Web アプリケーションを保護するファイアウォールの一種である Web アプリケーション ファイアウォールとは異なります。また、ホストベースのファイアウォールは、ファイル、フォルダー、プリンター、ルーターなどのネットワーク リソースへのアクセスを制御するルールのリストであるアクセス制御リストとも異なります。ホストベースのファイアウォールは、エンドポイントでの実行が許可されているアプリケーションのリストであるアプリケーション許可リストとも異なり、許可されていないアプリケーションや悪意のあるアプリケーションの実行を防ぎます。

最新問題: **161**
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
Answer: D (メーッセージを残す**)**
ハニーポットは、脆弱な資産をシミュレートして潜在的な攻撃者を引き寄せ、検出するために設定されたセキュリティ メカニズムです。企業の資産のように見え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、企業は偵察を行う攻撃者の行動を観察および分析できます。このアプローチにより、企業はアラートを受信し、潜在的な脅威に関する情報を収集できます。
参考資料 = CompTIA Security+ SY0-701 学習教材、特にハニーポットなどの脅威検出技術に関するもの。

最新問題**: 162**
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
Answer: A (メーッセージを残す**)**
エンゲージメント ルールは、侵入テストなどの情報セキュリティ テストの実行に関する詳細なガイドラインと制約です。テストの範囲、目的、方法、境界、およびテスト担当者とクライアントの役割と責任を定義します。エンゲージメント ルールは、テストが合法的、倫理的、専門的な方法で実施され、結果が正確で信頼できるものであることを保証するのに役立ちます。エンゲージメント ルールには通常、次の要素が含まれます。
テストの種類と範囲 (ブラック ボックス、ホワイト ボックス、グレー ボックスなど)、および対象のシステム、ネットワーク、アプリケーション、データ。
テスト中に問題、インシデント、または緊急事態を報告するためのクライアントの連絡先の詳細と通信チャネル。
テスト チームの資格情報と、使用できる承認済みのツールとテクニック。
テスト中に取得されたデータの保存、転送、破棄方法など、機密データの取り扱いと暗号化の要件。
ステータス会議とレポートのスケジュール、形式、受信者、およびテスト結果の機密保持契約と非開示契約。
テストのタイムラインと期間、および運用時間とテスト期間。
不必要な損害、混乱、情報の漏洩を避けるなど、テスターに期待される専門的かつ倫理的な行動。
サプライ チェーン分析、監査権条項、デュー デリジェンスは、サード パーティの侵入テスターによるテストの条件とは関係ありません。サプライ チェーン分析は、ビジネス ネットワーク内のサプライヤーとパートナーのセキュリティとリスクの状況を評価するプロセスです。監査権条項は、契約の条項であり、一方の当事者にもう一方の当事者を監査して契約条件への準拠を確認する権利を与えます。

デューデリジェンスとは、潜在的なベンダーまたはパートナーが組織にもたらすサイバーリスクを特定し、対処するプロセスです。
参考資料 =https://www.yeahhub.com/every-penetration-tester-you-should-know-about-this-rules-of-engageme
https://bing.com/search?q=rules+of+engagement+penetration+testing

最新問題: **163**
ある顧客がセキュリティ会社に、プロジェクトの概要、コスト、完了までの期間を記載した文書を提供するよう依頼しました。次の文書のうち、会社が顧客に提供すべきものはどれですか。
A. MSA
B. SLA
C. BPA
D. 種をまく
Answer: (解答を表示する**)**
ISOW は、セキュリティ会社が顧客にサービスを提供するプロジェクト、コスト、完了までの期間を概説した文書です。ISOW は Information Security Operations Work (情報セキュリティ運用作業) の略で、セキュリティ プロジェクトの範囲、成果物、マイルストーン、支払い条件を指定する契約の一種です。ISOW は通常、目的と結果が明確かつ定義されている 1 回限りまたは短期のプロジェクトに使用されます。
たとえば、ISOW は、セキュリティ評価、侵入テスト、セキュリティ監査、セキュリティ トレーニングに使用できます。
その他の選択肢は、セキュリティ会社が顧客にサービスを提供するプロジェクト、コスト、および完了までの期間を概説した文書ではないため、正しくありません。MSA はマスター サービス契約であり、セキュリティ会社と顧客との長期的または継続的な関係の一般的な条件を確立する契約の一種です。MSA は個々のプロジェクトの詳細を指定するのではなく、個別の作業明細書 (SOW) によって管理される将来のプロジェクトのフレームワークを設定します。SLA はサービス レベル契約であり、セキュリティ会社が顧客に提供するセキュリティ サービスの品質とパフォーマンスの基準を定義する契約の一種です。SLA には通常、サービス レベルを測定して保証するための指標、目標、責任、および罰則が含まれます。BPA はビジネス パートナーシップ契約であり、顧客に共同サービスを提供するために協力する 2 社以上のセキュリティ会社間の戦略的提携の役割と期待を確立する契約の一種です。BPA では通常、パートナーシップの目的、利点、リスク、および義務がカバーされます。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 8 章: ガバナンス、リスク、コンプライアンス、387 ページ。Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、セクション 8.2:
コンプライアンスとコントロール、ビデオ: 契約と合意 (5:12)。

最新問題: **164**

セキュリティ オペレーション センターは、疑わしい IP アドレスに関するイベントを調査しています。セキュリティ アナリストが次のイベント ログを確認すると、同じ IP アドレスから認証するときに、ユーザー アカウントの大部分でログイン試行の失敗が発生していることが分かりました。
発生した攻撃を最もよく表しているのは次のどれですか?
A. スプレー
B. ブルートフォース
C. 辞書
D. レインボーテーブル
Answer: (解答を表示する**)**
パスワード スプレーは、攻撃者が多数のアカウントに対して少数のよく使用されるパスワードを試すタイプの攻撃です。同じ IP アドレスからの多数のユーザー アカウントへのログイン試行が失敗したことを示すイベント ログは、攻撃者が一般的なパスワードを推測してアクセスを取得しようとしているパスワード スプレー攻撃を示しています。
参考資料 = CompTIA Security+ SY0-701 学習教材、特に ID およびアクセス管理の領域と、パスワード スプレーなどの一般的な攻撃ベクトル。

最新問題**: 165**
ある組織は最近、セキュリティ ポリシーを更新し、次のステートメントを追加しました。
正規表現は、Web アプリケーションのフォームによって設定された変数から $、|、;、&、`、? などの特殊文字を削除するためにソース コードに含まれています。
組織がポリシーにこの追加を行うことで採用したセキュリティ手法を最もよく説明しているのは、次のうちどれですか。
A. 埋め込まれたキーを識別する
B. コードのデバッグ
C. 入力検証
D. 静的コード分析
Answer: C (メーッセージを残す**)**
入力検証は、アプリケーションで処理する前に、ユーザー入力に悪意のあるデータや予期しないデータが含まれていないかチェックするセキュリティ手法です。入力検証により、アプリケーション コードの脆弱性を悪用するインジェクション、クロスサイト スクリプティング、バッファ オーバーフロー、コマンド実行などのさまざまなタイプの攻撃を防ぐことができます。入力検証は、ホワイトリスト、ブラックリスト、フィルタリング、サニタイズ、エスケープ、エンコードなどの方法を使用して、クライアント側とサーバー側の両方で実行できます。組織は、Web アプリケーションのフォームで設定された変数から特殊文字を削除する正規表現をソース コードに含めることで、セキュリティ手法として入力検証を採用しました。正規表現は、特定の文字または文字列のセットに一致するパターンであり、不要な入力や有害な入力を除外するために使用できます。$、|、;、&、`、? などの特殊文字は、攻撃者がアプリケーションにコマンドやスクリプトを挿入して、損害やデータの盗難

を引き起こすために使用できます。これらの文字を入力から削除することで、組織はそのような攻撃のリスクを軽減できます。
埋め込みキーの識別、コード デバッグ、静的コード分析は、ポリシーにこの追加を行うことで組織が採用したセキュリティ手法ではありません。埋め込みキーの識別は、ソース コードからハードコードされたキーや資格情報を見つけて削除するプロセスです。これらは、公開されたり侵害されたりするとセキュリティ リスクを引き起こす可能性があります。
コード デバッグは、アプリケーションの機能やパフォーマンスに影響を与える可能性のあるソース コード内のエラーやバグを見つけて修正するプロセスです。静的コード分析は、ソース コードを実行せずに分析し、脆弱性、欠陥、コーディング標準違反を特定するプロセスです。これらの手法は、入力から特殊文字を削除する正規表現の使用とは関係ありません。
参考資料 = CompTIA Security+ SY0-701 認定学習ガイド、375 ～ 376 ページ、Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、ビデオ 4.1 - 脆弱性スキャン、8:00 ～ 9:08、アプリケーション セキュリティ - SY0-601 CompTIA Security+: 3.2、0:00 ～ 2:00。

最新問題: **166**
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
Answer: A (メーッセージを残す**)**
クラウド ホスティング プロバイダーがデータ センターを新しい海外の場所に拡張する前に最初に考慮すべきことは、現地のデータ保護規制です。データ保護規制とは、個人データや機密データがどのように収集、保存、処理され、国境を越えて転送されるかを規定する法律または標準です。
国や地域によってデータ保護規制が異なる場合があります。たとえば、欧州連合の一般データ保護規則 (GDPR)、カナダの個人情報保護および電子文書法 (PIPEDA)、米国のカリフォルニア州消費者プライバシー法 (CCPA) などです。
クラウド ホスティング プロバイダーは、事業を展開したり顧客にサービスを提供したりする国や地域の現地のデータ保護規制に準拠する必要があります。準拠しない場合、法的処罰、罰金、または評判の失墜に直面する可能性があります。
したがって、クラウド ホスティング プロバイダーは、データ センターを拡張する前に、新しい国際的な場所の現地のデータ保護規制を調査して理解する必要があります。参考資料 = 500 以上の練習テスト問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 7 章、269 ページ。

CompTIA Security+ SY0-701 試験目標、ドメイン 5.1、14 ページ。

最新問題: **167**
セキュリティアナリストが次のログを確認しています:
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
Answer: (解答を表示する**)**
パスワード スプレーは、複数のアカウントで共通のパスワードを試して一致するものを探すブルート フォース攻撃の一種です。これは、アカウント ロックアウト プロトコルを回避できる大規模な試行錯誤のアプローチです。これにより、ハッカーは個人または企業のアカウントや情報にアクセスできます。これは標的型攻撃ではなく、辞書や一般的なパスワードや脆弱なパスワードのリストを使用する大規模な攻撃戦術です12。
ログを見ると、攻撃者が同じパスワード (｢password123｣) を使用して、同じ Web サーバー上のさまざまなアカウント (｢admin｣、｢user1｣、｢user2｣など) にログインしようとしていることがわかります。これはパスワード スプレーの典型的なパターンで、攻撃者は少なくとも 1 つのアカウントに、試行中のパスワードと一致する弱いパスワードがあることを期待しています。攻撃者は Hydra というツールも使用しています。これは、ネットワーク認証のパスワードをクラッキングする際によく使用される、最も人気のあるブルート フォース ツールの 1 つです3。
アカウント偽造は正しい答えではありません。これは、正当なユーザーまたはエンティティになりすますために偽のアカウントまたは資格情報を作成することを伴うためです。攻撃者は新しいアカウントを作成したり、偽造された資格情報を使用したりしていないため、ログにはアカウント偽造の証拠はありません。
Pass-the-hash は正解ではありません。ハッシュ化されたユーザー認証情報を盗み、それを使用して同じネットワーク上に新しい認証セッションを作成するからです。Pass-the-hash では、攻撃者は保存されたパスワード バージョンを使用して新しいセッションを開始するため、パスワードを知ったり解読したりする必要はありません4。ログには、攻撃者がハッ

シュではなくプレーン テキスト パスワードを使用して Web サーバーにログインしようとしていることが示されています。
ブルートフォースは正解ではありません。これは、正しいパスワードが見つかるまでさまざまなバリエーションの記号や単語を試す、さまざまな種類の攻撃を包括するより広い用語だからです。パスワード スプレーは、複数のアカウントに対して 1 つの共通パスワードを使用する特定の種類のブルートフォース攻撃です5。ログは、攻撃者が一般的なブルートフォースではなく、パスワード スプレーを使用して Web サーバーにアクセスしようとしていることを示しています。参考文献 = 1: パスワード スプレー: パスワード スプレー攻撃の概要... - Norton、2: セキュリティ: クレデンシャル スタッフィングとパスワード スプレー - Baeldung、3: ブルートフォース攻撃: 定義と知っておくべき 6 つのタイプ | Norton、4: パスザハッシュ攻撃とは何ですか? - CrowdStrike、5: ブルートフォース攻撃とは何ですか? | 定義、タイプ、および仕組み - Fortinet

最新問題: **168**
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。
Answer: C (メーッセージを残す)
= 変更管理リクエストとは、システムへの提案された変更、変更の理由、予想される影響、承認プロセス、テスト計画、実装計画、ロールバック計画、およびコミュニケーション計画を記述した文書です。変更管理リクエストは、変更が承認され、文書化され、テストされ、伝達されることを保証するため、特に優先度の高いシステムにパッチを適用する際のベストプラクティスです。また、変更管理リクエストは、システムのダウンタイム、データ損失、セキュリティ侵害などの意図しない結果のリスクを最小限に抑えます。参考資料 = 500 問を超える模擬試験問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 6 章、235 ページ。CompTIA Security+ SY0-701 試験目標、ドメイン 4.1、13 ページ。

最新問題: **169**
セキュリティ アナリストは、誤った構成や脆弱性を特定するために、アプリケーションのソース コードをレビューしています。このレビューを最もよく表す分析は次のうちどれですか。
A. ダイナミック
B. 静的
C. ギャップ
D. 影響
Answer: B (メーッセージを残す)

アプリケーションのソース コードをレビューして、構成ミスや脆弱性を特定することを、静的分析と呼びます。静的分析では、プログラムを実行せずにコードを検査します。コード自体を分析することで、潜在的なセキュリティ問題、コーディング エラー、脆弱性を見つけることに重点を置いています。
静的分析: プログラムを実行せずに、ソース コードまたはコンパイルされたコードの脆弱性を分析します。
動的分析: プログラムの実行中にテストと評価を行い、脆弱性を特定します。
ギャップ分析: 現在の状態と望ましい状態の違いを識別します。コンプライアンスやプロセス改善によく使用されます。
影響分析: システムまたはプロセスの変更による潜在的な影響を評価します。

最新問題**: 170**
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。
会社が設定しているプログラムを最もよく表しているのはどれですか?
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
Answer: B (メーッセージを残す**)**
バグ報奨金は、アプリケーションまたはシステムの脆弱性を発見して報告したセキュリティ研究者に報奨金を与えるプログラムです。バグ報奨金は、セキュリティ体制を改善し、倫理的なハッキングを奨励するために、企業でよく使用されます。バグ報奨金プログラムでは通常、研究者の範囲、ルール、報酬が定義されます。参考資料 = 500 問以上の練習問題を含む CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 1 章、10 ページ。CompTIA Security+ (SY0-701) 認定試験の目標、ドメイン 1.1、2 ページ。

最新問題**: 171**
データ センターのセキュリティを強化するために、セキュリティ管理者は CCTV システムを実装し、撮影される可能性があることを示す標識をいくつか掲示します。次のうち、これらの種類の制御を最もよく表すものはどれですか (2 つ選択してください)。
A. 予防的
B. 抑止力
C. 修正
D. ディレクティブ
E. 補償
F. 探偵
Answer: (解答を表示する**)**

CCTV システムと、撮影される可能性があることを示す標識は、抑止力と検出制御の両方の役割を果たします。
抑止制御: 潜在的な攻撃者が不正な行動を試みないようにすることを目的とします。CCTV に関する標識を掲示することは、個人の行動が監視されていることを警告することで抑止力として機能します。
検出制御: 不正な活動や疑わしい活動を識別して記録します。CCTV システム自体は、後で確認できる映像をキャプチャして記録することで、検出制御として機能します。
予防的管理: セキュリティ インシデントを防止することを目的としていますが、このコンテキストでは CCTV や標識によって直接対処されるものではありません。
是正管理: セキュリティ インシデントの影響を修正または軽減することを目的とします。
指示制御: ガイドラインや指示を提供しますが、CCTV や標識では直接示されません。
補償制御: 主要な制御の欠如または障害を補償するための代替手段を提供します。

最新問題**: 172**
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
Answer: D (メーッセージを残す**)**
侵入防止システム (IPS) は、ネットワーク トラフィックを監視し、定義済みのルールまたはシグネチャに基づいて悪意のあるパケットをブロックまたは変更するセキュリティ デバイスです。IPS は、悪意のあるパケットがターゲット システムに到達する前に検出してドロップすることで、古いバージョンのブラウザーの既知の脆弱性を悪用する攻撃を防止できます。IPS は、レート制限、暗号化、リダイレクトなどの他の機能も実行できます。

最新問題**: 173**
ある組織が、コストと利益を主な要件とし、RTO と RPO の値が約 2 日である新しいバックアップ データ センターを構築しています。このシナリオに最適なサイトは次のうちどれですか。
A. リアルタイムリカバリ
B. ホット
C. 冷たい
D. 暖かい
Answer: (解答を表示する**)**
説明

コールド サイトは、IT 運用をサポートするために必要なインフラストラクチャを備えているものの、事前構成されたハードウェアやソフトウェアを備えていないタイプのバックアップ データ センターです。コールド サイトは、バックアップ データ センター タイプの中で最も安価なオプションですが、目標復旧時間 (RTO) と目標復旧ポイント (RPO) の値も最も長くなります。コールド サイトは、コストと利益が主な要件であり、RTO と RPO の値がそれほど厳しくないシナリオに適しています。コールド サイトでは、災害後に通常の運用を回復するのに最大 2 日以上かかることがあります。参考資料 = CompTIA Security + SY0-701 認定試験ガイド、ページ
387; バックアップ タイプ - SY0-601 CompTIA Security+: 2.5、ビデオの 4:50。

最新問題: **174**
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
Answer: B (メーッセージを残す**)**
転送中のデータとは、ネットワークや無線などを通じて、ある場所から別の場所へ移動するデータのことです。転送中のデータは、悪意のある人物による傍受、変更、盗難の危険にさらされています。VPN (仮想プライベート ネットワーク) は、2 つのエンドポイント間に安全なトンネルを作成し、そこを通過するデータを暗号化することで、転送中のデータを保護するテクノロジーです2。

最新問題: **175**
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. 暗号化=オフ\
B. http://
C. www.*.com
D. :443
Answer: B (メーッセージを残す**)**
http:// は、ポート 80 で実行される安全でないプロトコルで、認証されていない保護されていない Web サイトでの通信に暗号化されていない追跡可能なデータを使用します。Web 検索 URL に警告が表示されたり、南京錠が表示されなかったりすることで、これらの安全でない Web サイトのいずれかにアクセスしていることが示されます。

最新問題: **176**

セキュリティ意識向上プログラムのコミュニケーション要素として含まれる可能性が高いのは次のどれですか?
A. フィッシング詐欺やその他の疑わしい行為を報告する
B. 異常行動認識による内部脅威の検出
C. 電信送金データを変更する際の情報の確認
D. サードパーティの侵入テストの一環としてソーシャルエンジニアリングを実行する
Answer: (解答を表示する**)**
セキュリティ意識向上プログラムは、組織のユーザーと従業員にセキュリティ ポリシー、手順、ベスト プラクティスについて教育し、情報提供することを目的とした一連のアクティビティとイニシアチブです。セキュリティ意識向上プログラムは、ソーシャル エンジニアリング、フィッシング、マルウェア、データ侵害、内部脅威などのセキュリティ リスクにおける人的要因の削減に役立ちます。セキュリティ意識向上プログラムには、セキュリティ メッセージを配信し、セキュリティ文化を強化するために、ニュースレター、ポスター、ビデオ、ウェビナー、クイズ、ゲーム、シミュレーション、フィードバック メカニズムなどのさまざまなコミュニケーション要素を含める必要があります。セキュリティ意識向上プログラムに含まれる可能性が最も高いコミュニケーション要素の 1 つは、フィッシングの試みやその他の疑わしいアクティビティの報告です。これは、一般的な種類のサイバー攻撃とその対応方法について、ユーザーと従業員の認識を高めるのに役立ちます。フィッシングの試みやその他の疑わしいアクティビティを報告すると、セキュリティ チームに警告を発し、攻撃の影響を防止または軽減するための適切な措置を講じることもできます。したがって、これは、与えられたオプションの中で最適な回答です。
その他のオプションは、技術的または運用上のタスクであり、ユーザーや従業員のセキュリティ意識に直接関連しないため、セキュリティ意識向上プログラムのコミュニケーション要素として含まれる可能性は低くなります。異常な行動認識を使用して内部脅威を検出することは、セキュリティ ツールまたはシステムを使用してユーザーや従業員のアクティビティと行動を監視および分析し、悪意のあるまたは許可されていないアクションを示す可能性のある逸脱や異常を特定する技術的なタスクです。このタスクは通常、セキュリティ チームまたはセキュリティ オペレーション センターによって実行され、ユーザーや従業員のコミュニケーションや参加は必要ありません。電信送金データを変更するときに情報を確認することは、電話、電子メール、デジタル署名などの検証方法を使用して、口座番号、金額、受取人などの電信送金に関連する情報の信頼性と正確性を確認する運用上のタスクです。このタスクは通常、財務部門または経理部門によって実行され、ユーザーや従業員のセキュリティ意識には関係しません。
サードパーティの侵入テストの一環としてソーシャル エンジニアリングを実行することは、フィッシング、ビッシング、なりすましなどの欺瞞または操作の手法を使用して、セキュリティ体制と、ソーシャル エンジニアリング攻撃に対するユーザーおよび従業員の脆弱性をテストする技術的なタスクです。このタスクは通常、外部のセキュリティ専門家またはコンサルタントによって実行され、ユーザーおよび従業員とのコミュニケーションや同意は必要ありません。したがって、これらのオプションはこの質問に対する最適な回答

ではありません。参考資料 = セキュリティ認識とトレーニング - CompTIA Security+ SY0-701: 5.2、ビデオの 0:00、CompTIA Security+ SY0-701 認定学習ガイド、263 ページ。

最新問題: **177**
研究開発事業部門の従業員は、会社のデータを保護する最善の方法を理解できるよう、広範囲にわたるトレーニングを受けています。これらの従業員が日常業務で最もよく使用するデータの種類は次のどれですか。
A. 暗号化
B. 知的財産
C. クリティカル
D. 転送中のデータ
Answer: B (メーッセージを残す**)**
知的財産とは、商業的価値があり、法律で保護されているアイデア、発明、デザイン、その他の創作物で構成されるデータの一種です。研究開発事業部門の従業員は、会社の新製品や新サービスの開発に携わっているため、日常業務で知的財産データを使用する可能性が最も高くなります。知的財産データは、会社に市場での競争上の優位性を与える可能性があるため、不正使用、開示、盗難から保護する必要があります。したがって、これらの従業員は、この種のデータを最も効果的に保護する方法を確実に理解できるように、広範囲にわたるトレーニングを受けます。参考資料 = CompTIA Security+ SY0-701 認定試験学習ガイド、90 ページ、Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、ビデオ 1.2 - セキュリティの概念、7:57 - 9:03。

最新問題: **178**
オンボーディング プロセス中に、従業員はイントラネット アカウントのパスワードを作成する必要があります。パスワードには、10 文字の英数字と特殊文字 2 文字を含める必要があります。パスワードが作成されると、会社はイントラネット プロファイルに基づいて、従業員に会社所有の他の Web サイトへのアクセスを許可します。
イントラネット アカウントを保護し、ユーザーのイントラネット アカウントに基づいて複数のサイトへのアクセスを許可するために、企業が使用するアクセス管理の概念は次のどれですか (2 つ選択)。
A. 連邦
B. 本人確認
C. パスワードの複雑さ
D. デフォルトのパスワードの変更
E. パスワードマネージャー
F. オープン認証
Answer: A,C (メーッセージを残す**)**
フェデレーションは、ユーザーが一度認証するだけで、異なるドメインや組織にまたがる複数のリソースやサービスにアクセスできるようにするアクセス管理の概念です。フェデ

レーションは、ユーザーの資格情報を保存し、それを公開せずに要求されたリソースやサービスに提供する信頼できるサードパーティに依存します。
パスワードの複雑さは、長さ、文字の種類、一意性など、特定の基準を満たすパスワードをユーザーに作成させるセキュリティ対策です。パスワードの複雑さにより、パスワードの解読や推測が困難になり、ブルートフォース攻撃、パスワード推測、クレデンシャル スタッフィングを防ぐことができます。参考文献: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、308 ～ 309 ページおよび 312 ～
313 1

最新問題: **179**
ある企業が災害復旧サイトを計画しており、単一の自然災害によって規制対象のバックアップ データが完全に失われないようにする必要があります。企業が考慮すべき事項は次のうちどれですか。
A. 地理的分散
B. プラットフォームの多様性
C. ホットサイト
D. 負荷分散
Answer: A (メーッセージを残す**)**
地理的分散とは、単一の自然災害が両方のサイトに影響を与えるリスクを最小限に抑えるために、十分に離れた異なる場所にバックアップ データを保存する方法です。これにより、プライマリ サイトで災害が発生した場合でも、企業は規制対象のデータを回復できます。プラットフォームの多様性、ホット サイト、および負荷分散は、自然災害からのバックアップ データの保護とは直接関係ありません。

最新問題: **180**
グラフィック画像内にコードやテキストを隠すプロセスを説明しているのは次のどれですか?
A. 対称暗号化
B. ハッシュ
C. データマスキング
D. ステガノグラフィー
Answer: D (メーッセージを残す**)**
説明
ステガノグラフィーとは、画像、音声、動画、テキスト ファイルなどの別のメディア内に情報を隠すプロセスです。隠された情報は、一般の人には見えず、気付かれず、特定の技術やキーを使用することでのみ抽出できます。ステガノグラフィーは、秘密のメッセージの隠蔽、透かし、ウイルス対策ソフトウェアによる検出の回避など、さまざまな目的で使用できます12 参考文献:
1: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 5 章: 暗号化と PKI、ページ

233 2: CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 5 章: 暗号化と PKI、235 ページ

最新問題**: 181**
セキュリティアナリストが次のログを確認しています:
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
Answer: (解答を表示する**)**
パスワード スプレーは、複数のアカウントで共通のパスワードを試して一致するものを探すブルート フォース攻撃の一種です。これは、アカウント ロックアウト プロトコルを回避できる大規模な試行錯誤のアプローチです。これにより、ハッカーは個人または企業のアカウントや情報にアクセスできます。これは標的型攻撃ではなく、辞書や一般的なパスワードや脆弱なパスワードのリストを使用する大規模な攻撃戦術です12。
ログを見ると、攻撃者が同じパスワード (「password123」) を使用して、同じ Web サーバー上のさまざまなアカウント (「admin」、「user1」、「user2」など) にログインしようとしていることがわかります。これはパスワード スプレーの典型的なパターンで、攻撃者は少なくとも 1 つのアカウントに、試行中のパスワードと一致する弱いパスワードがあることを期待しています。攻撃者は Hydra というツールも使用しています。これは、ネットワーク認証のパスワードをクラッキングする際によく使用される、最も人気のあるブルート フォース ツールの 1 つです3。
アカウント偽造は正しい答えではありません。これは、正当なユーザーまたはエンティティになりすますために偽のアカウントまたは資格情報を作成することを伴うためです。攻撃者は新しいアカウントを作成したり、偽造された資格情報を使用したりしていないため、ログにはアカウント偽造の証拠はありません。
Pass-the-hash は正解ではありません。ハッシュ化されたユーザー認証情報を盗み、それを使用して同じネットワーク上に新しい認証セッションを作成するからです。Pass-the-hash では、攻撃者は保存されたパスワード バージョンを使用して新しいセッションを開始するため、パスワードを知ったり解読したりする必要はありません4。ログには、攻撃者がハッシュではなくプレーン テキスト パスワードを使用して Web サーバーにログインしようとしていることが示されています。
ブルートフォースは正解ではありません。これは、正しいパスワードが見つかるまでさまざまな記号や単語のバリエーションを試す、さまざまな種類の攻撃を包括するより広い用語だからです。パスワード スプレーは、複数のアカウントに対して 1 つの共通パスワードを使用する、特定の種類のブルートフォース攻撃です5。ログは、攻撃者が一般的なブルートフォースではなく、パスワード スプレーを使用して Web サーバーにアクセスしようと

していることを示しています。参考文献 = 1: パスワード スプレー: パスワード スプレー攻撃の概要
... - Norton、2: セキュリティ: クレデンシャル スタッフィングとパスワード スプレー - Baeldung、3: ブルート フォース攻撃: 定義と知っておくべき 6 つの種類 | Norton、4: パスザ ハッシュ攻撃とは何ですか? - CrowdStrike、5: ブルート フォース攻撃とは何ですか? | 定義、種類、仕組み - Fortinet

最新問題: **182**
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
Answer: (解答を表示する**)**
送信トラフィックを監視することは、システムからの不正なデータ流出を検出するために不可欠です。マルウェアがデータを不正に移動できるようにする新しい脆弱性は、通常、このデータをネットワーク外に送信しようとします。送信トラフィックを監視することで、セキュリティ ツールは異常なデータ転送を検出し、アラートをトリガーし、機密情報の流出を防ぐことができます。
参考文献
* CompTIA Security+ SY0-701 コース内容: ドメイン 04 セキュリティ運用。
* CompTIA Security+ SY0-601 学習ガイド: 脅威の検出と対応に関する章。

最新問題: **183**
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
Answer: (解答を表示する**)**
ソーシャル エンジニアリングとは、他人になりすましたり、緊急性や信頼感を演出したりして、人を操作して行動を起こさせたり、機密情報を漏らさせたりすることです。このシナリオの疑わしい発信者は、CFO になりすまして支払いを要求し、ソーシャル エンジニアリングを使用してユーザーを騙してクレジットカード情報を渡させようとしていました。ユーザーはこれを詐欺の可能性があると認識し、IT ヘルプデスクに報告しました。その他のトピックはこの状況とは関係ありません。

最新問題**: 184**
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
Answer: C (メーッセージを残す**)**
データ分類は、機密性、価値、侵害された場合の組織への影響のレベルに基づいてデータを分類するプロセスです。データ分類は、不正アクセス、開示、または変更からデータを保護するための適切なセキュリティ制御とポリシーを決定するのに役立ちます。組織によってデータ分類スキームは異なりますが、一般的なのは、パブリック、プライベート、機密、およびクリティカルのカテゴリで構成される 4 層モデルです。
公開データは、一般の人がアクセスして公開することを目的としたデータであり、侵害されても組織には影響がありません。公開データの例としては、マーケティング資料、プレスリリース、公開 Web ページなどがあります。
個人データは、内部使用のみを目的としたデータであり、侵害された場合に組織に与える影響は低から中程度です。個人データの例には、従業員記録、財務レポート、内部ポリシーなどがあります。
機密データとは、許可された使用のみを目的としたデータであり、侵害されると組織に大きな影響を及ぼします。機密データの例としては、個人情報、健康記録、知的財産などが挙げられます。
重要なデータとは、組織の運営と存続に不可欠なデータであり、侵害されると組織に重大な影響を及ぼします。重要なデータの例としては、暗号化キー、災害復旧計画、システムバックアップなどがあります。
患者データは、法律と倫理基準によって保護されている個人情報と健康情報を含んでいるため、機密データの一種です。患者データは、正当な目的で許可された担当者のみが使用

し、不正アクセス、開示、または変更から保護する必要があります。したがって、システム管理者は機密データ分類を使用して患者データを保護する必要があります。
参考資料 = CompTIA Security+ SY0-701 認定試験学習ガイド、90 ～ 91 ページ、Messer 教授の CompTIA SY0-701 Security+ トレーニング コース、ビデオ 5.5 - データ分類、0:00 ～ 4:30。

最新問題: **185**
次のどれが VoIP 関連の一般的な脆弱性ですか? (2 つ選択してください)。
A. スピム
B. ヴィッシング
C. VLANホッピング
D. フィッシング
E. DHCPスヌーピング
F. テールゲート
Answer: (解答を表示する**)**
SPIM (インターネット メッセージング経由のスパム) は、帯域幅を消費し、リソースを転用し、サービス拒否攻撃を引き起こす可能性があるため、VoIP システムに脅威をもたらします。SPIM メッセージの流入により、VoIP 通話の品質が低下し、サーバーが過負荷になり、ソーシャル エンジニアリング攻撃のプラットフォームとして機能して、VoIP ユーザーのセキュリティが危険にさらされる可能性があります。これらのリスクを軽減するには、組織はスパム フィルター、侵入検知システム、定期的なソフトウェア更新を実装するとともに、SPIM に関連する潜在的な脅威を認識して回避するようにユーザーを教育する必要があります。

最新問題: **186**
管理者は、すべてのユーザー ワークステーションとサーバーに、拡張子 .ryk を含むファイルに関連付けられたメッセージが表示されていることに気付きました。システムに存在する感染の種類は次のどれですか。
A. ウイルス
B. トロイの木馬
C. スパイウェア
D. ランサムウェア
Answer: D (メーッセージを残す**)**
ランサムウェアは、被害者のファイルを暗号化し、復号キーと引き換えに身代金を要求するマルウェアの一種です。ランサムウェアは通常、感染したシステムにメッセージを表示し、身代金を支払ってファイルを復元する方法を指示します。.ryk 拡張子は、大規模な組織をターゲットにして高額の身代金を要求する Ryuk と呼ばれるランサムウェアの亜種に関連付けられています1。
参考資料: CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 1 章、17 ページ。

最新問題: **187**
CIRT は、人事採用担当者による機密性の高い企業データの流出に関わるインシデントを調査しています。CIRT は、採用担当者がポート 53 経由で HTTP を使用して Web サーバーにドキュメントをアップロードできることを発見しました。次のセキュリティ インフラストラクチャ デバイスのどれが、このアクティビティを識別してブロックできたでしょうか。
A. SSL復号化を利用したWAF
B. アプリケーション検査を活用したNGFW
C. 脅威フィードを利用したUTM
D. IPSec を活用した SD-WAN
Answer: B (メーッセージを残す**)**
アプリケーション検査を利用する NGFW (次世代ファイアウォール) は、ポート 53 経由の HTTP の異常な使用を識別してブロックできます。アプリケーション検査により、NGFW はアプリケーション層でトラフィックを分析し、DNS ポート 53 上の HTTP トラフィックなど、疑わしいプロトコルまたは非標準のプロトコルの使用を識別してブロックできます。
アプリケーション検査を利用する NGFW: アプリケーション層でトラフィックを検査し、ポート 53 経由の HTTP などの非標準プロトコルの使用をブロックできます。
SSL 復号化を利用する WAF: Web アプリケーションの保護と SSL トラフィックの復号化に重点を置いていますが、ポート 53 経由の HTTP の使用を検出できない場合があります。
脅威フィードを利用した UTM: 包括的なセキュリティを提供しますが、アプリケーション層の検査に特に焦点を当てていない可能性があります。
IPSec を利用した SD-WAN: 安全な WAN 接続を強化しますが、特定のアプリケーション トラフィックを検査およびブロックするようには主に設計されていません。

最新問題: **188**
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
Answer: D (メーッセージを残す**)**
ダッシュボードは、セキュリティ イベントやインシデントに関連する主要なパフォーマンス指標、メトリック、傾向を視覚的に表示するグラフィカル ユーザー インターフェイスです。ダッシュボードを使用すると、取締役会は、特定の期間に組織に影響を与えたインシデントの数と影響、およびセキュリティ制御とプロセスのステータスと有効性を把握できま

す。また、ダッシュボードを使用すると、取締役会は特定の詳細をドリルダウンしたり、さまざまな基準でデータをフィルター処理したりすることもできます。
パケット キャプチャは、デバイスまたはネットワーク セグメントを通過するネットワーク トラフィックをキャプチャして分析する方法です。パケット キャプチャでは、各パケットの送信元、送信先、プロトコル、およびコンテンツに関する詳細な情報を提供できますが、取締役会にインシデントの概要を提示するには適していません。
脆弱性スキャンは、攻撃者に悪用される可能性のあるシステムまたはネットワークの弱点と露出を特定して評価するプロセスです。脆弱性スキャンは、組織がリスクの優先順位付けと修復を行い、セキュリティ体制を改善するのに役立ちますが、四半期に発生したインシデントの数を報告する適切な方法ではありません14。メタデータは、他のデータの形式、発生元、構造、コンテキストなどを説明するデータです。メタデータは、データの特性とプロパティに関する有用な情報を提供できますが、取締役会にインシデントの影響と頻度を伝えるための有意義な方法ではありません。

最新問題: **189**
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。
. 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
Answer: C (メーッセージを残す**)**
説明
正解は C です。パスワード、認証トークン、拇印です。この認証要素の組み合わせは、ユーザーが知っていること、ユーザーが持っているもの、ユーザー自身を使用する多要素認証を実装するというマネージャーの目標を満たします。
ユーザーが知っていることとは、パスワード、PIN、セキュリティの質問など、ユーザーが秘密または個人情報を知っていることに依存する認証要素の一種です。パスワードは、VPN にアクセスするために使用できるユーザーが知っていることの一般的な例です12 ユーザーが持っていることとは、スマート カード、トークン、スマートフォンなどの物理的なオブジェクトまたはデバイスをユーザーが所有していることに依存する認証要素の一種です。認証トークンは、VPN にアクセスするために使用できるワンタイム パスワード (OTP) またはコードを生成するために使用できるユーザーが持っていることの一般的な例です12 ユーザーが何かであることとは、指紋、顔、虹彩など、ユーザーの生体認証特性に依存する

認証要素の一種です。拇印は、VPN にアクセスするためにユーザーの ID をスキャンして検証するために使用できるユーザーが何かであることの一般的な例です12 参照:
1: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 4 章: アイデンティティとアクセス管理、177 ページ 2: CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 4 章:
アイデンティティとアクセス管理、179 ページ

最新問題: **190**
ある企業は、ランサムウェア攻撃に対する補償を削除することで、年間サイバー保険のコストを削減することを決定しました。
企業がこの決定を下す際に最も使用した分析要素は次のどれでしょうか?
A. MTBF
B. IMTR
C. RTO
D. ARO
Answer: (解答を表示する**)**

最新問題: **191**
ある組織は、リモート ワークが原因で、VPN コンセントレータとインターネット回線のスケーリングの問題に悩まされています。組織は、データ センターへの暗号化されたトンネル アクセスとリモート従業員のインターネット トラフィックの監視を提供しながら、VPN とインターネット回線のトラフィックを削減できるソフトウェア ソリューションを探しています。次のどれがこれらの目的の達成に役立ちますか。
A. リモート従業員への SASE ソリューションの導入
B. 冗長インターネットを備えた負荷分散VPNソリューションの構築
C. VPNトラフィック用の低コストのSD-WANソリューションの購入
D. クラウドプロバイダーを使用して追加のVPNコンセントレータを作成する
Answer: A (メーッセージを残す**)**
SASE は Secure Access Service Edge の略です。これは、ネットワークとセキュリティ機能を 1 つの統合ソリューションに組み合わせたクラウドベースのサービスです。SASE は、リモート ワーカーにデータ センターとクラウド アプリケーションへの安全で最適化されたアクセスを提供することで、VPN とインターネット回線のトラフィックを削減するのに役立ちます。また、SASE は、場所やデバイスに関係なく、リモート ワーカーのインターネット トラフィックを監視してセキュリティ ポリシーを適用することもできます。SASE は、従来の VPN ソリューションと比較して、コストの削減、パフォーマンスの向上、拡張性、柔軟性などの利点があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-
701、第9版、457-458ページ1

最新問題: **192**

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
Answer: A (メーッセージを残す**)**
アクティブ偵察は、ターゲットにパケットまたはリクエストを送信し、応答を分析する偵察の一種です。アクティブ偵察では、開いているポート、サービス、オペレーティング システム、脆弱性などの情報が明らかになることがあります。ただし、アクティブ偵察は、ターゲットまたはそのセキュリティ デバイス (ファイアウォールや侵入検知システムなど) によって検出される可能性が高くなります。ポート スキャンとサービス スキャンは、ターゲットをプローブして特定の情報を取得するため、アクティブ偵察手法の例です。参考資料 = CompTIA Security+ 認定試験の目標、ドメイン 1.1: シナリオが与えられた場合、適切な手法とツールを使用して偵察を実施します。CompTIA Security+ 学習ガイド (SY0-701)、第 2 章: 偵察と情報収集、47 ページ。CompTIA Security+ 認定試験 SY0-
701 模擬テスト 1、質問 1。

最新問題**: 193**
最近、会社のシステムがランサムウェア攻撃を受けた後、管理者はログ ファイルを確認しました。管理者は次のどの制御タイプを使用しましたか?
A. 補償
B. 探偵
C. 予防的
D. 修正
Answer: B (メーッセージを残す**)**
検出コントロールは、システムまたはネットワーク上の悪意のあるアクティビティや異常を識別して監視するように設計されたセキュリティ対策です。攻撃のソース、範囲、影響を発見し、さらに分析や調査を行うための証拠を提供するのに役立ちます。検出コントロールには、ログ ファイル、セキュリティ監査、侵入検知システム、ネットワーク監視ツール、ウイルス対策ソフトウェアが含まれます。この場合、管理者はログ ファイルを検出コントロールとして使用し、会社のシステムに対するランサムウェア攻撃を確認しました。ログ ファイルは、ユーザー アクション、システム エラー、ネットワーク トラフィック、セキュリティ アラートなど、システムまたはネットワークで発生するイベントとアクティビティの記録です。トラブルシューティング、監査、フォレンジックに役立つ貴重な情報を提供できます。
参考文献:
Security+ (Plus) 認定 | CompTIA IT 認定、 試験について」の箇条書き 3:

ガバナンス、リスク、コンプライアンスの原則を含む、適用される規制とポリシーを認識して運用します。」CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 1 章、14 ページ: 検出コントロールは、システムまたはネットワーク上の悪意のあるアクティビティや異常を識別して監視するように設計されています。」コントロール タイプ - CompTIA Security+ SY0-401: 2.1 - Professor Messer IT ...、検出コントロール」の項: 検出コントロールは、システムまたはネットワーク上の悪意のあるアクティビティや異常を識別して監視するセキュリティ対策です。」

最新問題: **194**
訪問者がロビーのネットワーク ジャックにラップトップを接続し、会社のネットワークに接続できます。このアクティビティを最も効果的に防止するには、既存のネットワーク インフラストラクチャで次のどれを構成する必要がありますか。
A. 仮想プライベートネットワーク
B. トランスポート層セキュリティ
C. ポートセキュリティ
D. Web アプリケーション ファイアウォール
Answer: (解答を表示する)

最新問題: **195**
ある企業は、SIEM システムを導入し、アナリストを任命して毎週ログを確認することを計画しています。企業が導入しようとしている制御の種類は次のどれですか。
A. 修正
B. 予防的
C. 探偵
D. 抑止力
Answer: C (メーッセージを残す)
検出制御は、イベントを監視および分析して、潜在的または実際のセキュリティ インシデントを検出して報告するタイプのセキュリティ制御です。SIEM システムは、さまざまなソースからセキュリティ データを収集、相関、分析し、セキュリティ チームに警告を生成するため、検出制御の一例です。是正制御、予防制御、抑止制御は、それぞれセキュリティ侵害の回復、保護、または阻止を目的とした異なるタイプのセキュリティ制御です。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、33 ページ、セキュリティ情報およびイベント管理 (SIEM) とは何ですか?

最新問題: **196**
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
Answer: A (メーッセージを残す**)**
保存時の暗号化は、ノート PC などのデバイスに保存されているデータを、復号化キーまたはパスワードでのみアクセスできる読み取り不可能な形式に変換することで保護する戦略です。保存時の暗号化は、デバイスが物理的に侵害された場合でも、データへの不正アクセスを防止することで、盗難されたノート PC のデータ損失を防ぐことができます。保存時の暗号化は、データ保護を必要とするデータ プライバシー規制および標準に準拠するのにも役立ちます。マスキング、データ分類、およびアクセス許可の制限は、データ保護に役立つその他の戦略ですが、ノート PC に保存されているデータには十分ではないか、適用できない可能性があります。マスキングは、クレジットカード番号などの機密データ要素をランダムな文字または記号で隠す手法ですが、通常は転送中または使用中のデータに使用され、保存中のデータには使用されません。データ分類は、機密性とビジネスへの影響に基づいてデータにラベルを割り当てるプロセスですが、データ自体を保護するものではありません。アクセス許可の制限は、データにアクセス、変更、または削除できるユーザーを定義するルールですが、ノート PC が盗まれ、セキュリティ制御がバイパスされた場合、不正アクセスを防ぐことができない可能性があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、17-18 ページ、372-373

最新問題**: 197**
2 つの同一サイト間でトラフィックを分割してアプリケーションの回復力を高めるために、システム管理者が設定する必要があるのは次のうちどれですか。
A. 負荷分散
B. 地理的混乱
C. フェイルオーバー
D. 並列処理
Answer: A (メーッセージを残す**)**
2 つの同一サイト間でトラフィックを分割してアプリケーションの回復力を高めるには、システム管理者が負荷分散を設定する必要があります。負荷分散により、ネットワークまたはアプリケーションのトラフィックが複数のサーバーまたはサイトに分散され、単一の

サーバーが過負荷になることがなくなり、アプリケーションの可用性と信頼性が向上します。
負荷分散: 複数のサーバーにトラフィックを分散し、高い可用性と信頼性を確保します。負荷を効率的に管理し、サーバーの過負荷を防ぐのに役立ちます。
地理的混乱: 回復力に関連する標準的な用語ではありません。地理的に分散したサイトの使用を意味する可能性がありますが、説明されている正確なソリューションではありません。
フェイルオーバー: プライマリ サーバーまたはシステムに障害が発生したときに、スタンバイ サーバーまたはシステムに切り替えることを指します。本質的にはトラフィックを分割するのではなく、障害が発生したときに引き継ぎます。
並列処理: タスクの同時処理を指します。Web トラフィックの負荷分散とは特に関係ありません。

最新問題: **198**
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
Answer: A (メーッセージを残す**)**
説明
IPS は侵入防止システムの略で、悪意のあるトラフィックをリアルタイムで監視してブロックするネットワーク セキュリティ デバイスです。IPS は、悪意のあるトラフィックを検出して警告するだけでブロックしない IDS とは異なります。IPS は、ハッカーがフィッシング リンク経由でシステムにアクセスするのを防止したり、ランサムウェアがコマンド アンド コントロール サーバーと通信したりファイルを暗号化したりするのを阻止したりすることで、ランサムウェアの拡散を軽減します。

最新問題: **199**
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

Answer: (解答を表示する**)**

F) 誤情報は、虚偽または誤解を招く情報を広めて、対象の信念、意見、または行動に影響を与えるソーシャル エンジニアリング手法の一種です。誤情報は、世論を操作したり、混乱を引き起こしたり、評判を傷つけたり、議題を推進したりするために使用される可能性があります。誤情報は、テキスト メッセージや資格情報の検証とは関係ありません。

参照 = 1: スミッシングとは? | 定義と例 | Kaspersky 2: スミッシング - Wikipedia 3: なりすまし攻撃: なりすまし攻撃とは何か、また、それに対してどのように防御するか? 4: なりすまし - Wikipedia 5: タイポスクワッティングとは? | 定義と例 | Kaspersky 6: タイポスクワッティング - Wikipedia 7: フィッシングとは? | 定義と例 | Kaspersky 8: フィッシング - Wikipedia 9: ヴィッシングとは? | 定義と例 | Kaspersky : ヴィッシング - Wikipedia : 誤情報とは? | 定義と例 | Britannica : 誤情報 - Wikipedia 説明:

スミッシングは、テキスト メッセージ (SMS) を使用して被害者を騙し、機密情報を漏らしたり、悪意のあるリンクをクリックさせたり、マルウェアをダウンロードさせたりするためのソーシャル エンジニアリング手法の一種です。スミッシング メッセージは、銀行、政府機関、サービス プロバイダーなどの正当なソースから送信されたように見えることが多く、緊急または脅迫的な言葉を使用して受信者に行動を起こさせようとします12。このシナリオでは、給与部門からのテキスト メッセージであると主張するテキスト メッセージは、スミッシングの一例です。

なりすましは、権威のある人物、信頼できる人物、同僚など、別の人物になりすましてターゲットの信頼や協力を得るというソーシャル エンジニアリング手法の一種です。なりすましは、電話、メール、テキスト メッセージ、直接の訪問など、さまざまなチャネルを通じて実行され、被害者から情報、アクセス、または金銭を取得するために使用されます34。このシナリオでは、給与部門からのテキスト メッセージになりすましたものがなりすましの例です。

A) タイポスクワッティングは、人気のあるウェブサイトやよく知られているウェブサイトに似ているが、意図的にスペルミスや異なる拡張子を持つドメイン名を登録するサイバー攻撃の一種です。タイポスクワッティングは、ユーザーがウェブアドレスを入力する際に犯す一般的な間違いを悪用し、悪意のあるサイトや詐欺サイトにリダイレクトして、情報を盗んだり、マルウェアをインストールしたり、広告を表示したりすることを目的としています56。タイポスクワッティングは、テキストメッセージや資格情報の検証とは関係ありません。

B) フィッシングは、詐欺メールを使用して受信者を騙し、機密情報を開示させたり、悪意のあるリンクをクリックさせたり、マルウェアをダウンロードさせたりするためのソーシャルエンジニアリング手法の一種です。フィッシングメールは、銀行、小売業者、サービスプロバイダーなどの正当な組織の外観や口調を模倣することが多く、欺瞞的または緊急の言葉を使用して受信者に行動を起こさせます78。フィッシングは、テキストメッセージや資格情報の検証とは関係ありません。

D) ビッシングは、音声通話を利用して被害者を騙し、パスワード、クレジットカード番号、銀行口座の詳細などの機密情報を漏らすソーシャルエンジニアリング手法の一種です。ビッシングの電話は、法執行機関、政府機関、テクニカルサポートなどの正当なソースから発信されたように見えることが多く、脅迫や偽りの約束を使って受信者に従わせようとします9。ビッシングは、テキストメッセージや認証情報の確認とは関係ありません。

最新問題**: 200**
マーケティング部門は、関係部門に通知せずに独自のプロジェクト管理ソフトウェアを導入しました。このシナリオを説明するのは次のどれですか。
A. シャドーIT
B. 内部脅威
C. データの引き出し
D. サービス中断
Answer: A (メーッセージを残す**)**
説明
シャドー IT とは、組織内での無許可または承認されていない IT リソースの使用を表す用語です。マーケティング部門は、IT、セキュリティ、コンプライアンスなどの適切な部門に通知せずに、独自のプロジェクト管理ソフトウェアを設定しました。これにより、組織のセキュリティ体制、データの整合性、規制コンプライアンスにリスクが生じる可能性があります1。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、35 ページ。

最新問題**: 201**
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て、どのホストが感染元であるかを判断し、残りの各ホストをクリーンまたは感染として拒否します。

Answer:
Explanation:
ログによると、感染の発信元ホストは 192.168.10.22 のようです。このホストには、ポート 443 で実行されている svchost.exe という疑わしいプロセスがありますが、これは Windows サービスとしては珍しいことです。また、ポート 443 にはさまざまな IP アドレスへの多数の送信接続があり、ボットネットの一部であることを示しています。
ファイアウォール ログには、このホストがエンジニアリング ネットワーク上の別の感染ホストである 10.10.9.18 と通信していたことが示されています。このホストには、ポート 443 で実行されている svchost.exe という疑わしいプロセスがあり、ポート 443 上のさまざまな IP アドレスへの多数の送信接続があります。
R&D ネットワーク上の他のホスト (192.168.10.37 および 192.168.10.41) には、疑わしいプロセスや接続がないため、クリーンです。

最新問題: **202**
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
Answer: (解答を表示する**)**
脅威ハンティングとは、アラートや侵害の兆候 (IOC) が表示されるのを待つのではなく、ネットワーク内で悪意のあるアクティビティや侵害の兆候を積極的に探すプロセスです。脅威ハンティングは、悪意のある行為者が使用する新しい戦術、テクニック、手順 (TTP) を特定したり、セキュリティ ツールによる検出を逃れた可能性のある隠れた脅威やステルス性の高い脅威を発見したりするのに役立ちます。脅威ハンティングには、仮説の生成、データの収集と分析、脅威インテリジェンス、インシデント対応などのスキル、ツール、方法論の組み合わせが必要です。脅威ハンティングは、セキュリティ改善のためのフィードバックと推奨事項を提供することで、組織のセキュリティ体制を改善するのにも役立ちます。
参照 = CompTIA Security+ 認定試験の目標、ドメイン 4.1: シナリオが与えられた場合、悪意のあるアクティビティの潜在的な兆候を分析します。CompTIA Security+ 学習ガイド (SY0-701)、第 4 章: 脅威の検出と対応、153 ページ。脅威ハンティング - SY0-701 CompTIA Security+: 4.1、ビデオ 3:18。CompTIA Security+ 認定試験 SY0-701 模擬テスト 1、質問 3。

最新問題: **203**
次の侵入テスト チームのうち、攻撃者の戦術を使用して組織を侵害することにのみ焦点を当てているのはどれですか?
A. 白
B. 赤
C. 紫
D. 青
Answer: B (メーッセージを残す**)**
レッドチームは、攻撃者の戦術を使用して組織を侵害することにのみ焦点を当てています。
実際の攻撃をシミュレートして、組織のセキュリティ防御の有効性をテストし、脆弱性を特定します。
レッドチーム: 敵として行動し、攻撃をシミュレートしてセキュリティ上の弱点を見つけます。
ホワイト チーム: 侵入テスト中に交戦規則が遵守されているかどうかを監視および確認します。

パープル チーム: レッド チームとブルー チーム間のコラボレーションを促進し、セキュリティを強化します。
ブルーチーム: 攻撃を防御し、セキュリティインシデントに対応します。

最新問題: **204**
リスクを移転するための長期コストがリスクの影響よりも小さいかどうかを判断するのに最も役立つのは次のどれですか?
A. ARO
B. RTO
C. RPO
D. エール
E. SLE
Answer: D (メーッセージを残す**)**
年間損失予測 (ALE) は、リスクを移転するための長期的なコストがリスクの影響よりも小さいかどうかを判断するのに最も役立ちます。ALE は、単一損失予測 (SLE) に年間発生率 (ARO) を掛けて計算されます。これは、特定のリスクによる年間予想損失の見積もりを提供するため、長期的な財務計画やリスク管理の決定に役立ちます。参考資料:
CompTIA Security+ SY0-701 コース コンテンツと公式 CompTIA 学習リソース。

最新問題: **205**
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
Answer: C (メーッセージを残す**)**
IPSec は、IP ネットワーク上で安全な通信を提供するプロトコル スイートです。IPSec を使用すると、2 つ以上のパーティ間で交換されるデータを暗号化して認証する仮想プライベート ネットワーク (VPN) を作成できます。また、IPSec はデータの整合性、機密性、リプレイ保護、およびアクセス制御も提供します。セキュリティ コンサルタントは、IPSec を使用してクライアントのネットワークとの VPN トンネルを確立し、クライアント環境への安全なリモート アクセスを実現できます。

最新問題: **206**
セキュリティ管理者が元従業員のラップトップを再発行しています。管理者が実行するデータ処理アクティビティの組み合わせとして最適なものはどれですか? (2 つ選択してください。)
A. 認証

B. サニタイズ
C. 破壊
D. データ保持
E. 分類
F. 列挙
Answer: A,B (メーッセージを残す**)**

最新問題**: 207**
ある企業は、天候によるサーバールームの損傷やダウンタイムを懸念しています。企業が考慮すべき事項は次のうちどれですか?
A. クラスタリングサーバー
B. 地理的分散
C. ロードバランサー
D. オフサイトバックアップ
Answer: B (メーッセージを残す**)**
地理的分散とは、サーバーやデータ センターをさまざまな地理的場所に分散させる戦略です。地理的分散により、企業は天候によるサーバー ルームの損傷やダウンタイムのリスクを軽減できるほか、ネットワークの可用性、パフォーマンス、回復力も向上します。地理的分散により、地域的な停電や混乱が発生した場合にバックアップやフェイルオーバーのオプションを提供できるため、企業の災害復旧機能や事業継続機能も強化されます12。
その他の選択肢は、会社の懸念に対処する最善の方法ではありません。
サーバーのクラスタリング: これは、複数のサーバーをグループ化して 1 つのシステムとして動作させる手法です。サーバーのクラスタリングは、ネットワークのパフォーマンス、スケーラビリティ、フォールト トレランスの向上に役立ちますが、特にサーバーが同じ部屋や建物内にある場合、天候による物理的な損傷やダウンタイムからサーバーを保護することはできません3。
ロード バランサ: ネットワーク トラフィックまたはワークロードを複数のサーバーまたはリソースに分散するデバイスまたはソフトウェアです。ロード バランサは、ネットワークの使用率、効率、信頼性を最適化するのに役立ちますが、特にサーバーが同じ部屋または建物内にある場合、天候によるサーバーの損傷や中断を防ぐことはできません4。
オフサイト バックアップ: 元のソースとは別の場所に保存されるデータまたはファイルのコピーです。オフサイト バックアップは、気象現象によるデータの損失や破損を防ぐのに役立ちますが、気象現象によるサーバーの損傷や中断を防ぐことはできません。また、ネットワーク サービスの可用性や継続性を保証することもできません。
参考資料 = 1: CompTIA Security+ SY0-701 認定試験学習ガイド、97 ページ2: 高可用性 - CompTIA Security+ SY0-701 - 3.4、メッサー教授によるビデオ3: CompTIA Security+ SY0-701 認定試験学習ガイド、98 ページ4: CompTIA Security+ SY0-701 認定試験学習ガイド、99 ページ。:
CompTIA Security+ SY0-701 認定試験学習ガイド、100 ページ。

最新問題: **208**
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
Answer: A (メーッセージを残す**)**
RBAC はロールベースのアクセス制御の略で、ユーザーの役割や責任に基づいてデータやリソースへのアクセスを制限する方法です。RBAC は、個々のユーザーではなく、ユーザーに役割を割り当て、役割にアクセス権を付与することで、権限の管理を簡素化します。RBAC は、最小権限の原則を強制し、不正アクセスやデータ漏洩のリスクを軽減するのに役立ちます。その他のオプションは、責任に基づいてアクセスを防止しないか、簡素化された形式を適用しないため、RBAC ほどこのシナリオには適していません。

最新問題: **209**
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
Answer: A (メーッセージを残す**)**
説明
要塞ホストは、攻撃に耐え、内部リソースへの安全なアクセスを提供するように設計された特殊用途のサーバーです。要塞ホストは通常、ネットワークのエッジに配置され、内部ネットワークへのゲートウェイまたはプロキシとして機能します。要塞ホストは、SSH や HTTP などの特定の種類のトラフィックのみを許可し、他のすべてのトラフィックをブロックするように構成できます。要塞ホストは、ファイアウォール、侵入検知システム、ウイルス対策プログラムなどのセキュリティ ソフトウェアを実行して、着信トラフィックと発信トラフィックを監視およびフィルタリングすることもできます。要塞ホストは、強力な認証と暗号化を要求し、監査目的ですべてのアクティビティをログに記録することで、内部リソースへの管理アクセスを提供できます12。
要塞ホストは、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、単一の制御ポイントと防御ポイントを提供するため、与えられたオプションの中で最も安全な方法です。要塞ホストは、内部ネットワークをインターネットやその他の信頼できないネット

ワークへの直接的な露出から分離し、攻撃対象領域と侵害のリスクを軽減することもできます3。
境界ネットワークを展開することは正しい答えではありません。境界ネットワークは、内部ネットワークを外部ネットワークから分離するネットワーク セグメントだからです。境界ネットワークは通常、インターネットからアクセスする必要がある Web サーバー、電子メール サーバー、DNS サーバーなどの公開サービスをホストします。境界ネットワークは内部リソースへの管理アクセスを提供するのではなく、不正アクセスから保護します。境界ネットワークは、ネットワーク管理とセキュリティの複雑さとコストを増大させる可能性もあります4。
WAF をインストールすることは正解ではありません。WAF は、HTTP トラフィックを監視、フィルタリング、ブロックすることで、一般的な Web ベースの攻撃から Web アプリケーションを保護するセキュリティ ツールだからです。WAF は、クロスサイト スクリプティング、SQL インジェクション、ファイル インクルードなどの攻撃を防ぐことができます。WAF は内部リソースへの管理アクセスを提供するのではなく、Web アプリケーションの脆弱性から内部リソースを保護します。また、WAF はアプリケーション層でのみ動作し、他の種類の攻撃や脅威から保護しないため、ネットワーク セキュリティの包括的なソリューションではありません5。
シングル サインオンを利用するのは正解ではありません。シングル サインオンは、ユーザーが 1 つのユーザー名とパスワードで複数のサイト、サービス、またはアプリケーションにアクセスできる認証方法だからです。シングル サインオンを使用すると、ユーザーのサインイン プロセスが簡素化され、覚えて管理しなければならないパスワードの数を減らすことができます。シングル サインオンでは、内部リソースへの管理アクセスは提供されませんが、ユーザーが使用を許可されているさまざまなリソースへのアクセスが可能になります。また、ユーザーの資格情報が侵害されたり、シングル サインオン プロバイダーが侵害されたりすると、シングル サインオンによってセキュリティ リスクが発生する可能性があります6。参考資料 = 1: Bastion ホスト
- Wikipedia、2: SSH Bastion ホストを保護するための 14 のベスト プラクティス - goteleport.com、3: ネットワーク セキュリティにおける Bastion ホストの重要性、4: ネットワーク境界とは何ですか? | Cloudflare、5: WAF とは何ですか? | Web アプリケーション ファイアウォールの説明、6: [シングル サインオン (SSO) とは何ですか? - WhatIs.com からの定義]

最新問題**: 210**
プロセスに 2 人による整合性セキュリティ制御が必要な理由を最もよく説明しているのはどれですか。
A. アクティビティが、1 人のユーザーで完了する場合の半分の時間で完了する可能性を高める
B. 別の部門の2人のユーザーが、許可されたユーザーによって実行されているアクティビティを観察することを許可する

C. 手順が誤って実行されたり、権限のないユーザーによって実行されたりするリスクを軽減するため
D. 1人がCCTVカメラで録画されながら活動を行うことを許可する
Answer: C (メーッセージを残す**)**
エラーや不正なアクションのリスクを最小限に抑えるために、2 人による整合性セキュリティ制御が実装されています。
この制御により、少なくとも 2 人の担当者が重要な操作に関与することが保証され、プロセスの正確性を検証し、権限のないユーザーが単独で操作するのを防ぐことができます。これは、金融取引や重要なシステムへのアクセスなどの機密性の高い操作で説明責任と正確性を確保するためによく使用されるセキュリティ対策です。
参考文献
* CompTIA Security+ SY0-701 コース内容: ドメイン 05 セキュリティ プログラムの管理と監視。
* CompTIA Security+ SY0-601 学習ガイド: セキュリティ運用と管理の章。

最新問題**: 211**
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。
Answer:
Explanation:
Web サーバーボットネット DDoS 保護を有効にするユーザー RAT ホストベースの IPS を実装するデータベース サーバー ワーム デフォルトのアプリケーション パスワードを変更するエグゼクティブ キーロガー脆弱なサービスを無効にするアプリケーション バックドア プッシュ通知を使用して 2FA を実装するコンピュータ プログラムのスクリーンショット 信頼性の低い自動生成された説明

最新問題**: 212**

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
Answer: (解答を表示する**)**
転送中のデータとは、ネットワークや無線などを通じて、ある場所から別の場所へ移動しているデータのことです。
転送中のデータは、悪意のある人物による傍受、変更、盗難に対して脆弱です。VPN (仮想プライベート ネットワーク) は、2 つのエンドポイント間に安全なトンネルを作成し、そこを通過するデータを暗号化することで、転送中のデータを保護するテクノロジーです2。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 4 章、145 ページ。

最新問題**: 213**
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
Answer: B (メーッセージを残す**)**
説明
SQL インジェクションは、データベースの設定ミスや、データベースとやりとりするアプリケーション コードの欠陥を悪用する攻撃の一種です。攻撃者は、ユーザー入力フィールドやデータベース サーバーに送信される URL パラメータに悪意のある SQL 文を挿入できます。これらの文は、データの読み取り、変更、削除、作成、さらにはデータベース サーバーの乗っ取りなど、許可されていないコマンドを実行できます。SQL インジェクションは、データとシステムの機密性、整合性、可用性を損なう可能性があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、215 ページ 1

最新問題**: 214**
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
Answer: D (メーッセージを残す**)**

最小権限の原則は、ユーザー、プログラム、またはデバイスが正当な機能を実行するために必要な最小限のレベルにリソースへのアクセスを制限するセキュリティ コンセプトです。これは、高価値データと資産を侵害や内部の脅威から保護するサイバー セキュリティのベスト プラクティスです。最小権限は、プロセス、システム、接続されたデバイスなど、コンピューティング環境のさまざまな抽象化レイヤーに適用できます。ただし、実際に実装されることはほとんどありません。
このシナリオでは、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へのアクセスを、IT マネージャーとヘルプ デスク リーダーの 2 人の承認済みユーザーのみに制限することで、最小権限の原則を設定しています。これにより、IT マネージャーは、他のヘルプ デスク スタッフによるソフトウェア構成、データ、または機能への不正な変更や偶発的な変更を防ぐことができます。
その他のヘルプデスク スタッフは、ソフトウェアの通常のユーザー インターフェイスにのみアクセスできますが、これは職務を遂行するのに十分です。
他のオプションは正しくありません。強化とは、不要なソフトウェアの削除、デフォルトのパスワードの変更、不要なサービスの無効化などにより、システムの脆弱性の表面を減らすことでシステムを保護するプロセスです。従業員の監視とは、Web の閲覧、アプリケーションの使用、キー入力、スクリーンショットの追跡などにより、従業員のアクティビティを監視することです。構成の適用とは、パッチ、ポリシー、テンプレートの適用などにより、システムが事前に定義された一連のセキュリティ設定に準拠していることを確認するプロセスです。

最新問題: **215**
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. なりすまし
B. スミッシング
C. 誤情報
D. タイプミススクワッティング
E. フィッシング
F. ヴィッシング
Answer: (解答を表示する**)**

最新問題: **216**
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. 本番ネットワークでポリシーを有効にする前に、非本番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、「deny any」ポリシーの侵入防止シグネチャを無効にする
D. 「deny any*」ポリシーの上に「allow any1」ポリシーを含める
Answer: (解答を表示する**)**
説明
ファイアウォール ポリシーは、ネットワーク上で許可または拒否されるトラフィックを定義する一連のルールです。ファイアウォール ポリシーは、誤って構成されたポリシーによってネットワークが中断したりセキュリティが侵害されたりする可能性があるため、実装する前に慎重に設計およびテストする必要があります。一般的なベスト プラクティスは、実稼働ネットワークでポリシーを有効にする前に、ラボやシミュレーションなどの非実稼働環境でポリシーをテストすることです。この方法により、技術者は実稼働ネットワークに影響を与えることなく、ポリシーの機能とパフォーマンスを確認し、問題や競合を特定して解決できます。非実稼働環境でポリシーをテストすると、技術者が実稼働ネットワークにポリシーを適用する前に問題を検出して修正できるため、「すべて拒否」ポリシーによって複数の会社のサーバーがアクセス不能になるという問題を防ぐことができます。
変更要求に新しいポリシーを文書化して変更管理に要求を送信するのは良い方法ですが、それだけでは問題を防ぐことはできません。変更管理は、ネットワークへの変更が承認され、文書化され、伝達されることを保証するプロセスですが、変更にエラーがないことや機能することを保証するものではありません。技術者は、ポリシーを実装する前にテストする必要があります。
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しても、問題は回避できず、ネットワークのセキュリティが低下する可能性があります。侵入防止シグネチャは、悪意のあるトラフィックや不要なトラフィックを識別し、ファイアウォールがそのようなトラフィックをブロックまたは警告できるようにするパターンです。
これらのシグネチャを無効にすると、ファイアウォールによる攻撃の検出と防止の効果が低下しますが、会社のサーバーの到達可能性には影響しません。
「すべて許可」ポリシーを「すべて拒否」ポリシーの上に含めても、問題は防げず、「すべて拒否」ポリシーは役に立たなくなります。ファイアウォール ポリシーは上から下に向かって処理され、最初に一致したルールが適用されます。「すべて許可」ポリシーは、送信元、送信先、プロトコルに関係なく、すべてのトラフィックに一致し、ファイアウォールの通過を許可します。これでは、「すべて拒否」ポリシーの目的、つまり以前のルールのいずれにも一致しないトラフィックをブロックするという目的が無効になります。さらに、「すべて許可」ポリシーは、許可されていないトラフィックや悪意のあるトラフィックがネットワークに出入りすることを許可するため、セキュリティ リスクを生み出します。参考資料 = CompTIA Security+ SY0-701 認定試験学習ガイド、204 ～ 205 ページ、Messer 教授の

CompTIA SY0-701 Security+ トレーニング コース、ビデオ 2.1 - ネットワーク セキュリティ デバイス、8:00 ～ 10:00。

最新問題: **217**
セキュリティ エンジニアがワークステーションとサーバーで不正な変更やソフトウェアが適切に監視されていることを確認するために実行できるアクションは次のどれですか。
A. スケジュールされたタスクをログに記録するようにすべてのシステムを構成します。
B. ネットワークから出るすべてのトラフィックを収集して監視します。
C. 既知の悪意のあるシグネチャに基づいてトラフィックをブロックします。
D. すべてのシステムにエンドポイント管理ソフトウェアをインストールします。
Answer: (解答を表示する**)**
説明
エンドポイント管理ソフトウェアは、セキュリティ エンジニアがワークステーションやサーバーの構成、セキュリティ、パフォーマンスを中央コンソールから監視および制御できるようにするツールです。エンドポイント管理ソフトウェアは、不正な変更やソフトウェアのインストールを検出して防止し、ポリシーとコンプライアンスを適用し、エンドポイントの状態に関するレポートとアラートを提供するのに役立ちます。他のオプションは、この目的にはエンドポイント管理ソフトウェアほど効果的でも包括的でもありません。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、137 ページ 1

最新問題: **218**
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. www.*.com
B. :443
C. http://
D. 暗号化=オフ\
Answer: C (メーッセージを残す**)**

最新問題: **219**
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

Answer: (解答を表示する**)**
説明
バッジ アクセスとアクセス コントロール ベスティビュールは、許可された人だけが安全な施設にアクセスできるようにする最良の方法です。バッジ アクセスでは、人員は有効な認証バッジをリーダーまたはスキャナーに提示する必要があります。リーダーまたはスキャナーは、事前定義されたルールと権限に基づいてアクセスを許可または拒否します。アクセス コントロール ベスティビュールは、2 つのドアがある小さな部屋またはチャンバーで構成される物理的なセキュリティ対策です。1 つは外部に通じ、もう 1 つは安全なエリアに通じています。人員はベスティビュールに入り、最初のドアが閉まってロックされるまで待ってから、2 番目のドアを開ける必要があります。これにより、許可されていない人による追突や相乗りを防止できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 1 章
4、197-1981ページ

最新問題**: 220**
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
Answer: C (メーッセージを残す**)**
デューデリジェンスとは、特定の業界内で情報セキュリティを管理する法律、規制、ベストプラクティスを調査して理解するプロセスを指します。組織は、法的および規制上の要件に準拠していることを確認するためにデューデリジェンスを実施する必要があります。これにより、リスクを軽減し、罰金を回避することができます。
* コンプライアンス レポートには、法律または規制基準への準拠を証明するレポートの生成が含まれます。
* GDPR は、EU におけるデータ プライバシーを管理する特定の規制であり、法律を調査する一般的な慣行ではありません。
* 認証とは、組織が一連の基準に準拠していることを正式に宣言することであり、法律を調査する行為ではありません。

最新問題**: 221**
最近、サブネット全体でマルウェアが蔓延し、多数の PC にルートキットがインストールされ、修復作業が無効になり、マルウェアが永続化しました。将来的にルートキットの存在を最もよく検出できるのは次のうちどれですか。
A. FDE
B. NIDS
C. EDR

D. DLP
Answer: C (メーッセージを残す**)**
EDR (エンドポイント検出と対応) は、ルートキットの存在を検出するためのオプションの中で最も適したソリューションです。EDR ソリューションは、ルートキットを含むマルウェアの存在を示す可能性のある疑わしいアクティビティや動作パターンを探しながら、エンドポイントを継続的に監視してデータを収集します。また、セキュリティ インシデントの調査と対応のためのツールも提供しているため、従来のウイルス対策ソリューションを回避できる高度な脅威に対処するのに効果的です。

最新問題**: 222**
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
Answer: A (メーッセージを残す**)**
IPS は侵入防止システムの略で、悪意のあるトラフィックをリアルタイムで監視してブロックするネットワーク セキュリティ デバイスです。IPS は、悪意のあるトラフィックを検出して警告するだけでブロックしない IDS とは異なります。IPS は、ハッカーがフィッシング リンク経由でシステムにアクセスするのを防止したり、ランサムウェアがコマンド アンド コントロール サーバーと通信したりファイルを暗号化したりするのを阻止したりすることで、ランサムウェアの拡散を軽減します。

最新問題**: 223**
セキュリティ アナリストは、業務時間外の短時間に、内部システムがインターネット上のシステムに大量の異常な DNS クエリを送信しているという警告を受け取ります。次のどれが最も発生していると考えられますか。
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。
Answer: B (メーッセージを残す**)**
データ流出は、攻撃者が DNS クエリと応答を介して機密データを送信し、ターゲット システムまたはネットワークから機密データを盗むために使用する手法です。この方法は、攻撃者がターゲット環境での検出を継続的に回避しようとする、高度で持続的な脅威 (APT) 攻撃でよく使用されます。営業時間外の短時間にインターネット上のシステムに対して大量の異常な DNS クエリが送信されることは、データ流出の強力な指標です。ワーム、ロ

ジック ボム、およびランサムウェアは、コマンド アンド コントロール サーバーと通信したり、悪意のあるアクションを実行したりするために DNS クエリを使用することはありません。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、487 ページ、DNS データ流出の概要、今回は現実ではなかった DNS 流出攻撃の特定

最新問題: **224**
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
Answer: C (メーッセージを残す**)**
説明
マスキングは、クレジットカード データを保護する方法の 1 つで、数字の一部またはすべてをアスタリスク、ダッシュ、X などの記号に置き換え、元の数字の一部をそのまま表示します。マスキングは、クレジットカードの最後の 4 桁のみを表示する必要がある場合に最適です。これにより、カード番号全体への不正アクセスを防ぎながら、カード所有者の識別と検証が可能になります。マスキングでは、アルゴリズムを使用してデータをさまざまな形式に変換する暗号化、ハッシュ化、トークン化とは異なり、元のデータは変更されません。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章: コンプライアンスと運用セキュリティ、721 ページ。CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 2 章:
コンプライアンスと運用セキュリティ、722 ページ。

最新問題: **225**
ある企業は、SIEM システムを導入し、アナリストを任命して毎週ログを確認することを計画しています。この企業が導入しようとしているコントロールのタイプは次のどれですか。
A. 修正
B. 予防的
C. 探偵
D. 抑止力
Answer: (解答を表示する**)**
検出制御は、システムまたはネットワーク内のイベントとアクティビティを監視および分析し、インシデントまたは違反が発生したときに警告または報告するタイプの制御です。SIEM (セキュリティ情報およびイベント管理) システムは、ファイアウォール、ルーター、サーバー、アプリケーションなどのさまざまなソースからログを収集、相関、分析し、セキュリティの状態とインシデントの集中ビューを提供するツールです。アナリストは毎

週ログを確認し、潜在的な脅威または違反を示す異常、傾向、またはパターンを特定して調査できます。検出制御は、企業がインシデントに迅速かつ効果的に対応し、セキュリティ体制と回復力を向上させるのに役立ちます。

最新問題: **226**
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
Answer: A (メーッセージを残す)
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は、新しい脆弱性が明らかになったときに組織全体のリスクを測定するために不可欠です。これは、セキュリティ アナリストが脆弱性の影響を受けるシステムを特定し、修復作業の優先順位を決定できるためです。完全なインベントリがないと、セキュリティ アナリストは脆弱なシステムを見逃したり、無関係なシステムに時間とリソースを浪費したりする可能性があります。システム分類のドキュメント、システム所有者とその部門のリスト、およびサードパーティのリスク評価ドキュメントはすべてリスク管理に役立ちますが、新しい脆弱性の影響を測定するには十分ではありません。参照: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、1221 ページ、リスク評価および分析方法: 定性的および定量的3

最新問題: **227**
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
Answer: B (メーッセージを残す)
SQL インジェクションは、データベースの設定ミスや、データベースとやりとりするアプリケーション コードの欠陥を悪用する攻撃の一種です。攻撃者は、ユーザー入力フィール

ドやデータベース サーバーに送信される URL パラメータに悪意のある SQL 文を挿入できます。これらの文は、データの読み取り、変更、削除、作成、さらにはデータベース サーバーの乗っ取りなど、許可されていないコマンドを実行できます。SQL インジェクションは、データとシステムの機密性、整合性、可用性を損なう可能性があります。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、215 ページ 1

最新問題: **228**
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. VPN IPアドレス、会社ID、顔の構造
B. パスワード、認証トークン、拇印
C. 会社の URL、TLS 証明書、自宅住所
D. ドメイン名、PKI、GeoIP ルックアップ
Answer: B (メーッセージを残す**)**

最新問題: **229**
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. RPO
C. SDLC
D. DRP
Answer: (解答を表示する**)**
説明
災害復旧計画 (DRP) は、システム障害、自然災害、その他の緊急事態が発生した場合に組織の通常の業務を回復することを目的とした一連のポリシーと手順です。DRP には通常、次の要素が含まれます。
組織の重要な資産とプロセスに対する潜在的な脅威と影響を特定するリスク評価。
最も重要な機能とデータの回復を優先するビジネス影響分析。
復旧チームの役割と責任、必要なリソースとツール、システムを復元するための手順を定義する復旧戦略。
DRP が定期的に更新され、検証されることを保証するテストおよびメンテナンス プラン。DRP は、災害からの復旧とダウンタイムおよびデータ損失の最小化のための明確で構造化されたフレームワークを提供するため、組織がシステム障害発生時に復元プロセスを適切に管理するために必要です。参考資料 = CompTIA Security+ 学習ガイド (SY0-701)、第 7 章: 回復力と回復、325 ページ。

最新問題**: 230**
ラボシミュレーション1
システム管理者は、2 つのブランチ オフィス間のサイト間 VPN を構成しています。一部の設定は既に正しく構成されています。構成を完了するために、システム管理者には次の要件が提供されています。
- 最も安全なアルゴリズムを選択する必要があります
- すべてのトラフィックはVPN経由で暗号化される必要があります
- 2つのVPNを認証するために秘密のパスワードが使用されます
コンセントレータ

Answer:
提供された要件に従って 2 つのブランチ オフィス間のサイト間 VPN を構成するには、VPN コンセントレータに適用する必要がある詳細な手順と設定を次に示します。
要件：
最も安全なアルゴリズムを選択する必要があります。
すべてのトラフィックは VPN 経由で暗号化される必要があります。
2 つの VPN コンセントレータを認証するために秘密のパスワードが使用されます。
VPN コンセントレータ 1 の構成:
フェーズ1:
ピア IP アドレス: 5.5.5.10 (VPN コンセントレータ 2 の IP アドレス)
認証方法: PSK (事前共有キー)
交渉モード: MAIN
暗号化アルゴリズム: AES256
ハッシュアルゴリズム: SHA256
DHキーグループ: 14
フェーズ2:
モード: トンネル
プロトコル: ESP (カプセル化セキュリティペイロード)
暗号化アルゴリズム: AES256
ハッシュアルゴリズム: SHA256
ローカルネットワーク/マスク: 192.168.1.0/24
リモートネットワーク/マスク: 192.168.2.0/24
VPN コンセントレータ 2 の構成:
フェーズ1:
ピア IP アドレス: 5.5.5.5 (VPN コンセントレータ 1 の IP アドレス)
認証方法: PSK (事前共有キー)
交渉モード: MAIN
暗号化アルゴリズム: AES256
ハッシュアルゴリズム: SHA256
DHキーグループ: 14

フェーズ2:
モード: トンネル
プロトコル: ESP (カプセル化セキュリティペイロード)
暗号化アルゴリズム: AES256
ハッシュアルゴリズム: SHA256
ローカルネットワーク/マスク: 192.168.2.0/24
リモートネットワーク/マスク: 192.168.1.0/24
まとめ：
ピア IP アドレス: リモート VPN コンセントレータの IP アドレスに設定します。
認証方法: 事前共有キーを使用するための PSK。
ネゴシエーション モード: 初期設定の場合は MAIN。
暗号化アルゴリズム: 強力で安全なアルゴリズムである AES256。
ハッシュ アルゴリズム: 強力なハッシュを提供する SHA256。
DH キー グループ: 強力な Diffie-Hellman キー交換の場合は 14。
フェーズ 2 プロトコル: 暗号化と整合性のための ESP。
ローカルおよびリモート ネットワーク: 各ブランチ オフィスのサブネットに一致するように、ローカルおよびリモート ネットワーク アドレスを適切に構成します。
両方の VPN コンセントレータでこれらの設定を構成することにより、サイト間 VPN は強力なセキュリティ アルゴリズム、すべてのトラフィックの暗号化、事前共有キーを使用した認証の要件を満たすようになります。

最新問題: **231**
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. 修正
B. 予防的
C. 探偵
D. 補償
Answer: (解答を表示する**)**

最新問題: **232**
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
Answer: D (メーッセージを残す**)**
説明
ホエーリングは、企業の重役、著名人、政治家などの著名人をターゲットにしたフィッシング攻撃の一種です。攻撃者は権威や影響力のある人物になりすまし、被害者を騙して金銭

の送金、機密情報の漏洩、悪意のあるリンクのクリックなどのアクションを実行させようとします。ホエーリングは、CEO 詐欺やビジネス メール詐欺とも呼ばれます2。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 3 章、97 ページ。

最新問題**: 233**
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
Answer: B (メーッセージを残す**)**
説明: 可用性とは、システムまたはサービスが必要に応じてアクセスおよび使用できる能力です。個人が健康上の緊急事態をデジタルで報告できるようにする Web アプリケーションの場合、ダウンタイムや遅延がユーザーの健康と安全に重大な影響を及ぼす可能性があるため、可用性は開発中に最も重要な考慮事項です。Web アプリケーションは、高トラフィックを処理し、サービス拒否攻撃を防ぎ、障害が発生した場合に備えたバックアップおよびリカバリ プランを持つように設計する必要があります。

最新問題**: 234**
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. 抑止力
B. 修正
C. 補償
D. 予防的
Answer: (解答を表示する**)**
重要なレガシー サーバーをプライベート ネットワークに分割する場合、使用されるセキュリティ制御は補償的です。補償制御とは、主要な制御が実行不可能または実用的でない場合に、セキュリティ要件を満たすために導入される代替手段です。この場合、レガシー サーバーをプライベート ネットワークに分割することは、直接軽減できない潜在的な脆弱性からサーバーを保護する補償制御として機能します。
補償: 主な制御が不可能な場合に、望ましいセキュリティ結果を達成するための代替方法を提供します。
抑止力: 潜在的な攻撃者を阻止することを目的としていますが、セグメンテーションに直接対処するものではありません。
是正: インシデントが発生した後にその影響を修正または軽減するために使用されます。
予防的: セキュリティ インシデントを防止することを目的としていますが、セグメンテーションのコンテキストに固有のものではありません。

最新問題: **235**
セキュリティ アナリストは、大量の従業員の資格情報が盗まれ、ダーク ウェブで販売されていることを発見しました。アナリストが調査した結果、一部の時間給従業員の資格情報が侵害されたが、給与制従業員の資格情報は影響を受けていないことがわかりました。
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の 1 つを使用して出勤と退勤を記録していました。しかし、帰宅後に退勤を記録した従業員もいました。建物内にいる間に出勤と退勤を記録した従業員だけが資格情報を盗まれました。各キオスクは異なるフロアにあり、ビジネスが特定の業務機能のために環境をセグメント化しているため、複数のルーターがあります。
時間給従業員は、acmetimekeeping.com という Web サイトを使用して出勤と退勤を記録する必要があります。この Web サイトはインターネットからアクセスできます。この侵害の最も可能性の高い理由はどれですか?
A. タイムキーピング Web サイトに対してブルート フォース攻撃が行われ、一般的なパスワードがスキャンされました。
B. 悪意のある人物が、サイト上のパッチ未適用の脆弱性を利用して悪意のあるコードで時間管理 Web サイトを侵害し、資格情報を盗みました。
C. 内部 DNS サーバーが汚染され、acmetimkeeping.com を悪意のあるドメインにリダイレクトして、資格情報を傍受し、それを実際のサイトに渡していました。
D. ARP ポイズニングが建物内のマシンに影響を与え、キオスクが送信されたすべての資格情報のコピーを machine.machine に送信しました。
Answer: (解答を表示する**)**
このシナリオでは、建物内のキオスクを使用した従業員だけが認証情報を侵害されたことが示唆されています。タイムキーピング Web サイトはインターネットからアクセスできるため、悪意のある人物がサイトのパッチ未適用の脆弱性を悪用し、キオスクからログインしたユーザーの認証情報を取得する悪意のあるコードを挿入した可能性があります。これは、Web アプリケーションから認証情報を盗むための一般的な攻撃ベクトルです。
参考文献
* CompTIA Security+ SY0-701 コース内容: このコースでは、Web アプリケーションの脆弱性と、攻撃者がそれを悪用して資格情報を盗む方法について説明します。

最新問題: **236**
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
Answer: B (メーッセージを残す**)**
説明

転送中のデータとは、ネットワークや無線などを通じて、ある場所から別の場所へ移動しているデータのことです。
転送中のデータは、悪意のある人物による傍受、変更、盗難に対して脆弱です。VPN (仮想プライベート ネットワーク) は、2 つのエンドポイント間に安全なトンネルを作成し、そこを通過するデータを暗号化することで、転送中のデータを保護するテクノロジーです2。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 4 章、145 ページ。

最新問題**: 237**
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。
. 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
Answer: (解答を表示する**)**
正解は C です。パスワード、認証トークン、拇印です。この認証要素の組み合わせは、ユーザーが知っていること、ユーザーが持っているもの、ユーザー自身を使用する多要素認証を実装するというマネージャーの目標を満たします。
ユーザーが知っていることとは、パスワード、PIN、セキュリティの質問など、ユーザーが秘密または個人情報を知っていることに依存する認証要素の一種です。パスワードは、VPN にアクセスするために使用できるユーザーが知っていることの一般的な例です12 ユーザーが持っていることとは、スマート カード、トークン、スマートフォンなどの物理的なオブジェクトまたはデバイスをユーザーが所有していることに依存する認証要素の一種です。認証トークンは、VPN にアクセスするために使用できるワンタイム パスワード (OTP) またはコードを生成するために使用できるユーザーが持っていることの一般的な例です12 ユーザーが何かであることとは、指紋、顔、虹彩など、ユーザーの生体認証特性に依存する認証要素の一種です。拇印は、VPN にアクセスするためにユーザーの ID をスキャンして検証するために使用できるユーザーが何かであることの一般的な例です12 参照:
1: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 4 章: アイデンティティとアクセス管理、177 ページ 2: CompTIA Security+ 認定キット: 試験 SY0-701、第 7 版、第 4 章:
アイデンティティとアクセス管理、179 ページ

最新問題**: 238**
組織がインシデント対応プロセスを改善するために使用すべき演習は次のどれですか?
A. テーブルトップ

B. レプリケーション
C. フェイルオーバー
D. 回復
Answer: A (メーッセージを残す**)**
説明
卓上演習は、組織のインシデント対応計画と手順をテストするシミュレートされたシナリオです。
主要な関係者と意思決定者が参加し、仮想的なインシデントに対応して役割と行動について話し合います。インシデント対応プロセスにおけるギャップ、弱点、改善領域を特定するのに役立ちます。また、参加者間のコミュニケーション、調整、コラボレーションを強化することもできます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、525 ページ 1

最新問題**: 239**
ある企業は、セキュリティ運用を主導するために、組織外からセキュリティ マネージャーを雇用しました。
セキュリティ マネージャーがこの新しい役割で最初に実行する必要があるアクションは次のうちどれですか。
A. セキュリティ ベースラインを確立します。
B. セキュリティ ポリシーを確認します。
C. セキュリティベンチマークを採用します。
D. ユーザー ID の再検証を実行します。
Answer: (解答を表示する**)**
セキュリティ マネージャーを組織外から雇用してセキュリティ運用を指揮させる場合、最初に行うべきことは既存のセキュリティ ポリシーを確認することです。現在のセキュリティ ポリシーを理解することで、強み、弱み、改善が必要な領域を特定するための基盤が得られ、セキュリティ プログラムが組織の目標や規制要件に合致していることが保証されます。
セキュリティ ポリシーを確認する: 既存のセキュリティ フレームワークを包括的に理解し、新しいマネージャーがギャップや強化すべき領域を特定できるようにします。
セキュリティ ベースラインを確立する: 重要ですが、既存のポリシーとプラクティスを十分に理解した上で行う必要があります。
セキュリティ ベンチマークを採用する: 標準を設定するのに役立ちますが、現在のポリシーを確認することが前提条件となります。
ユーザー ID の再検証を実行します。ユーザー アクセスが適切であることを確認するために重要ですが、全体的なセキュリティ操作を理解するための最初のステップではありません。

最新問題**: 240**

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
Answer: (解答を表示する**)**
可用性とは、システムまたはサービスが必要に応じてアクセスおよび使用できる能力です。個人が健康上の緊急事態をデジタルで報告できるようにする Web アプリケーションの場合、ダウンタイムや遅延がユーザーの健康と安全に重大な影響を及ぼす可能性があるため、可用性は開発中に最も重要な考慮事項です。Web アプリケーションは、高トラフィックを処理し、サービス拒否攻撃を防ぎ、障害が発生した場合に備えたバックアップおよびリカバリ プランを備えるように設計する必要があります2。
参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 2 章、41 ページ。

最新問題**: 241**
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
Answer: (解答を表示する**)**
エンゲージメント ルールは、侵入テストなどの情報セキュリティ テストの実行に関する詳細なガイドラインと制約です。テストの範囲、目的、方法、境界、およびテスト担当者とクライアントの役割と責任を定義します。エンゲージメント ルールは、テストが合法的、倫理的、専門的な方法で実施され、結果が正確で信頼できるものであることを保証するのに役立ちます。

最新問題**: 242**

エンジニアがネットワーク デバイスの廃止を推奨すべきケースは次のうちどれですか (2 つ選択)。
A. デバイスは実稼働環境からテスト環境に移動されました。
B. デバイスはクリアテキスト パスワードを使用するように構成されています。
C. デバイスは企業ネットワーク上の分離されたセグメントに移動されます。
D. デバイスが企業内の別の場所に移動されます。
E. デバイスの暗号化レベルが組織の標準を満たすことができません。
F. デバイスは承認された更新を受信できません。
Answer: B,E (メーッセージを残す**)**
B: デバイスはクリアテキスト パスワードを使用するように設定されています。これは重大なセキュリティ上の脆弱性であり、不正アクセスの重大なリスクをもたらします。クリアテキスト パスワードを使用しているデバイスは廃止し、安全な認証方法を使用するデバイスに置き換える必要があります。
E: デバイスの暗号化レベルが組織の標準を満たしていません。デバイスがデータを必要なレベルまで暗号化できない場合、機密情報の機密性が損なわれるため、デバイスの使用を停止する必要があります。組織のセキュリティ ポリシーでは、ネットワーク デバイスに許容される最低限の暗号化レベルを規定する必要があります。

最新問題**: 243**
次のリスクのうち、HTTP ヘッダーによって軽減できるものはどれですか?
A. SQLi
B. XSS
C. DoS
D. SSL
Answer: B (メーッセージを残す**)**
HTTP ヘッダーを使用すると、クロスサイト スクリプティング (XSS) に関連するリスクを軽減できます。コンテンツ セキュリティ ポリシー (CSP) や X-XSS-Protection などのセキュリティ関連の HTTP ヘッダーを構成すると、Web ページのコンテキストで悪意のあるスクリプトが実行されることを防ぐことができます。
XSS (クロスサイト スクリプティング): 攻撃者が他のユーザーが閲覧する Web ページに悪意のあるスクリプトを挿入できる脆弱性。CSP などの HTTP ヘッダーは、読み込みを許可する動的リソースを指定することにより、XSS 攻撃を防ぐのに役立ちます。
SQLi (SQL インジェクション): 通常は、HTTP ヘッダーではなく、パラメーター化されたクエリと入力検証を使用して軽減されます。
DoS (サービス拒否): HTTP ヘッダーではなく、ネットワークおよびアプリケーション レベルの防御によって軽減されます。
SSL (Secure Sockets Layer): 通信のセキュリティ保護を指し、HTTP ヘッダーによって直接緩和されるのではなく、SSL/TLS プロトコルを使用して実装されます。

最新問題: **244**
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
Answer: (解答を表示する**)**
シャドー IT とは、組織の明示的な承認なしに組織内で使用される情報技術システムを指します。

最新問題: **245**
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
Answer: A (メーッセージを残す**)**
ゼロ トラストは、ネットワーク境界の内外を問わず、いかなるエンティティも信頼しないことを前提とし、ID と権限の継続的な検証を必要とするセキュリティ モデルです。ゼロ トラストは、機密データとリソースを分離して不正アクセスから保護することで、安全なゾーンを提供できます。また、ゼロ トラストは、ユーザー、デバイス、アプリケーションに対して最小権限の原則と細分化されたセグメンテーションを適用することで、会社全体のアクセス制御ポリシーを実施することもできます。ゼロ トラストは、横方向の移動を防ぎ、攻撃対象領域を最小限に抑えることで、脅威の範囲を縮小できます。
参照：
5: この情報源では、ゼロ トラスト セキュリティの概念と利点、および従来のセキュリティ モデルとの違いについて説明します。
8: この情報源では、ゼロ トラスト ID セキュリティの概要と、それがユーザーとデバイスの ID と整合性の検証にどのように役立つかについて説明します。

最新問題: **246**
絶えず変化する環境に最も適しているのはどれでしょうか?
A. RTOS
B. コンテナ
C. 組み込みシステム

D. SCADA
Answer: B (メーッセージを残す**)**
説明
コンテナは、アプリケーションを独自の依存関係、ライブラリ、および構成を持つ分離された環境で実行できるようにする仮想化の方法です。コンテナは軽量で、移植性があり、拡張性があり、展開と更新が容易であるため、常に変化する環境に最適です。また、コンテナはマイクロサービス アーキテクチャをサポートできるため、ソフトウェア機能をより迅速かつ頻繁に提供できます。参考資料: CompTIA Security+ 学習ガイド: 試験 SY0-701、第 9 版、第 10 章: モバイル デバイス セキュリティ、512 ページ 1

最新問題**: 247**
マーケティング部門は、関係部門に通知せずに独自のプロジェクト管理ソフトウェアを導入しました。このシナリオを説明するのは次のどれですか。
A. シャドーIT
B. 内部脅威
C. データの引き出し
D. サービス中断
Answer: (解答を表示する**)**
説明: シャドー IT とは、組織内での無許可または承認されていない IT リソースの使用を説明するために使用される用語です。マーケティング部門は、IT、セキュリティ、コンプライアンスなどの適切な部門に通知せずに、独自のプロジェクト管理ソフトウェアを設定しました。これにより、組織のセキュリティ体制、データの整合性、および規制コンプライアンスにリスクが生じる可能性があります。