EC-COUNCIL.212-89.v2026-07-25.q191

試験コード:	212-89
試験名称:	EC Council Certified Incident Handler (ECIH v3)
認定資格:	EC-COUNCIL
無料問題数:	191
バージョン:	v2026-07-25
アクセス数:	109
ページビュー数:	1910
https://www.jpnpdf.com/EC-COUNCIL.212-89.v2026-07-25.q191-mondaishu.html	

最新問題: **1**
DDoS攻撃では、攻撃者はまず複数のシステムに感染させ、それらのシステムを使って特定の標的を直接攻撃します。これらのシステムは以下のとおりです。
A. ゾンビ
B. ハンドラー
C. リレー
D. ハニーポット
Answer: A (メーッセージを残す**)**

最新問題: **2**
大手ソフトウェア開発会社であるDigitalSoftは最近、自社のコードベースへの不正アクセスを発見した。犯人は昇進を見送られたことに不満を抱いた従業員だった。同社は今後、このような内部犯行による脅威を防ぎたいと考えている。同社が実施できる最も効果的な対策は何だろうか？
A. 30日ごとにパスワードの変更を義務付ける。
B. 上級社員のみが機密データにアクセスできるような厳格な階層構造を導入する。
C. 機密データへのアクセスには生体認証を使用します。
D. ユーザーのアクセスと使用行動分析の定期的な監査を実施する。
Answer: D (メーッセージを残す**)**
説明（H&Rのベストプラクティスに準拠）：
内部脅威を最も効果的に軽減するには、最小権限の原則と異常行動の継続的な検出を組み合わせることが有効です。定期的なアクセスレビューにより、ユーザーはそれぞれの役割に必要な権限のみを保持することが保証され（権限の肥大化」が抑制されます）、行動分析は「正当な」アクセス内で発生する不正使用の検出に役立ちます。パスワードのローテーション（A）は、主に衛生対策であり、既に承認されたアクセス権限を持つ悪意のある内部関係者を防ぐことはできません。頻繁な強制変更は、安全でない行動（パスワードの書き留

め、予測可能なパターン）を助長する可能性もあります。厳格な階層構造（B）は実用的ではなく、「知る必要性」に対応していません。適切な制御境界は、役職ではなく職務機能です。生体認証（C）は認証を強化しますが、このシナリオの問題は本人確認の不確実性ではなく、正当な内部関係者による不正使用です。したがって、最も効果的なアプローチはガバナンスとモニタリングの組み合わせです。（1）データアクセス基準を定義する、（2）権限を定期的に見直す、（3）リポジトリの異常なクローン作成、大量ダウンロード、通常時間外のアクセス、または通常とは異なるブランチなど、疑わしい操作を警告する、（4）人事／法務プロセスを用いて迅速に調査する。これらの対策は、早期発見と被害範囲の縮小を可能にすることで、悪意のある不正利用に直接対処します。これは、影響を受けるシステム／データの特定、範囲の把握、および再発防止のためのインシデント後の管理改善という、より広範なインシデント対応の重点事項と一致しています。

最新問題: **3**
ある組織は、不満を抱いた従業員が機密情報にアクセスしたという情報セキュリティインシデントに直面した。
競合他社への情報管理。組織のインシデント対応マネージャーは調査の結果、
事業継続性を維持するためには、事件を同日中に数時間以内に処理する必要があり、
市場競争力。このような情報セキュリティインシデントをどのように分類しますか？
A. 低レベルのインシデント
B. 超高レベル事件
C. 高レベルの事件
D. 中級レベルの事件
Answer: (解答を表示する)

最新問題: **4**
攻撃者または内部関係者は、ファイアウォール内にセキュリティ対策が施されていないアクセスポイントを設置することで、信頼できるネットワークへのバックドアを作成します。そして、そのソフトウェアまたはハードウェアのアクセスポイントを利用して攻撃を実行します。
次のうち、このタイプの攻撃はどれですか？
A. パスワードベースの攻撃
B. メール感染
C. 不正アクセスポイント攻撃
D. マルウェア攻撃
Answer: (解答を表示する)

最新問題: **5**
ネットワークセキュリティアナリストのローガンは、社内サブネット内の広範囲のIPアドレスに対して、ICMPエコー要求が繰り返し送信されているパターンに気づいた。偵察活動

の可能性を疑うローガンは、Wiresharkを起動し、異常なスキャン動作がないかトラフィックの分析を開始した。
攻撃者はどのような手法を用いている可能性が最も高いですか？
A. DNSポイズニング
B. ピングスイープ
C. ポートスキャン
D. SYNフラッディング
Answer: (解答を表示する**)**
今回説明した活動（多数のIPアドレスに対してICMPエコー要求を順次送信する）は、ネットワーク上の稼働中のホストを特定するために使用される偵察手法である、典型的なピングスイープです。ECIHのネットワークインシデント対応では、偵察は攻撃の初期段階の活動であり、多くの場合、悪用につながると認識されています。
正解はBです。なぜなら、ピングスキャンはICMPエコー要求を使用して応答するホストを特定し、攻撃者がネットワークをマッピングできるようにするからです。これは観測されたトラフィックと完全に一致します。
オプションAはDNS操作を伴う。オプションCはICMPではなくTCP/UDPポートのプローブを伴う。オプションDは偵察ではなく、サービス拒否攻撃の手法を説明する。
偵察活動を早期に認識することで、防御側は悪用される前に対策を講じることができ、ECIHの検出および防止に関する指針に沿った対応が可能となる。

最新問題**: 6**
ジェイソンはマルウェア関連の事案に対応するインシデントハンドラーです。彼は、あらゆるプログラムの基本機能に関する情報を収集するために、メモリダンプ分析を実行するよう依頼されました。この任務の一環として、プログラムが実行できる有害な動作を特定できる悪意のある文字列を検索するために、文字列検索分析を実行する必要があります。
ジェイソンが目的のタスクを実行するために使用する必要がある文字列検索ツールは次のうちどれですか？
A. プロセスエクスプローラ
B. Dependency Walker リソースに関する情報はレスポンスボディに含まれています。
C. PEビュー
D. ビンテキスト
Answer: D (メーッセージを残す**)**

最新問題**: 7**
攻撃者または内部関係者は、ファイアウォール内にセキュリティ対策が施されていないアクセスポイントを設置することで、信頼できるネットワークへのバックドアを作成します。そして、任意のソフトウェアまたはハードウェアのアクセスポイントを使用して攻撃を実行します。次のうち、このタイプの攻撃はどれですか？
A. 不正アクセスポイント攻撃
B. パスワードベースの攻撃

C. マルウェア攻撃
D. メール感染
Answer: A (メーッセージを残す**)**
不正アクセスポイント攻撃とは、攻撃者または内部関係者が、ファイアウォールの内側など、信頼できるネットワーク内にセキュリティ対策が施されていないアクセスポイントを設置し、バックドアを作成する攻撃です。これにより、攻撃者はネットワークセキュリティ対策を回避し、様々な悪意のある活動を検知されることなく実行できます。不正アクセスポイント攻撃は、ソフトウェアまたはハードウェアのアクセスポイントを利用して不正アクセスを行い、攻撃を実行する行為です。これは、パスワード攻撃、マルウェア攻撃、電子メール感染とは対照的です。これらの攻撃は、それぞれ認証情報の窃盗、悪意のあるソフトウェアの配布、電子メールシステムを介した拡散など、異なる手法と目的を持っています。
参考資料 :ECIH v3認定資料では、不正アクセスポイント攻撃を含むさまざまな種類のネットワーク攻撃について説明し、攻撃者に不正なネットワークアクセスを提供することで生じるリスクを強調しています。

最新問題**: 8**
悪意のある、セキュリティを侵害するプログラムが、便利なプログラムを装って存在します。このような実行可能プログラムは、ファイルを開いたときにインストールされ、他者がユーザーのシステムを制御できるようにします。この種のプログラムは何と呼ばれますか？
A. スパイウェア
B. ウイルス
C. ワーム
D. トロイの木馬
Answer: D (メーッセージを残す**)**

最新問題**: 9**
マーリーは、インシデント対応 -復旧 IH&R)チームのリーダーから、被害者システムのレジストリ、キャッシュ、RAMに存在するシステム情報やネットワーク情報などの揮発性データを収集するよう依頼された。
マーリーが揮発性データを収集するために採用しなければならないデータ取得方法を特定してください。
A. ライブデータ取得
B. 静的データ取得
C. データ取得の検証
D. リモートデータ取得
Answer: A (メーッセージを残す**)**

最新問題**: 10**

リチャードは企業ネットワークを分析しています。ネットワークのIPSでアラートが発生した後、彼はすべてのサーバーがウェブサイトabc.xyzに大量のトラフィックを送信していることを特定しました。このネットワークに影響を与えた情報セキュリティ攻撃ベクトルはどのようなものですか？
A. ランサムウェア
B. ボットネット
C. 前進持続三は
D. IoTの脅威
Answer: B (メーッセージを残す**)**

最新問題: **11**
パスワード解析ツールのインストール、ポルノ画像のダウンロード、同僚を不快にさせるメールの送信、会社のコンピュータ上で許可されていないウェブサイトをホストすることなどが該当します。
A. ネットワークベースの攻撃
B. 不正アクセス攻撃
C. マルウェア攻撃
D. 不適切な使用事例
Answer: D (メーッセージを残す**)**

最新問題: **12**
Dashは、256個のターゲットURLに対して同時にDoS攻撃を実行しようとしています。ダッシュが目的を達成するために利用できるツールは次のうちどれですか？
A. HOIC
B. IDAPro
C. Ollydbg
D. OpenVAS
Answer: (解答を表示する**)**
High Orbit Ion Cannon (HOIC) は、ネットワークやサーバーのストレステストを実行するために設計されたツールです。攻撃者が HTTP POST および GET リクエストでターゲットを圧倒することで、分散型サービス拒否 (DDoS) 攻撃を実行できます。HOIC の際立った特徴は、設定可能な HTTP フラッド攻撃で複数のターゲット (最大 256 URL) を同時に攻撃できることです。この機能により、大規模なサービス妨害を目的とする攻撃者にとって最適なツールとなっています。デバッグや脆弱性スキャン用に設計されたツール (IDA Pro、Ollydbg、OpenVAS など) とは異なり、HOIC は DoS/DDoS 攻撃を実行するために特化して設計されているため、Dash の目的に最適なツールです。
参考資料 :インシデントハンドラー（ECIH v3）コースと学習ガイドでは、HOICを含むさまざまなサイバー攻撃ツールについて詳しく解説し、包括的なサイバーセキュリティ脅威の状況に関する教育の一環として、それらの機能と潜在的な影響について説明しています。

最新問題: **13**
次のうち、ネットワークフォレンジックツールではないものはどれですか？
A. Wireshark
B. Advancec NTFS ジャーナリングパーサー
C. Capsaネットワークアナライザー
D. Tcpdurnp
Answer: B (メーッセージを残す**)**

最新問題: **14**
キャンパスネットワークに接続されたデバイスに悪意のあるプログラム（トロイの木馬、メール爆弾、ウイルスなど）を導入する行為を説明しているのは、次のうちどれですか？
A. 不適切な使用
B. ネットワークアクセス
C. 認証済みアクセス
D. 不正アクセス
Answer: B (メーッセージを残す**)**

最新問題: **15**
クラークはTechSoft Solutions社で発生したサイバー犯罪を捜査している。捜査にあたっては、実行中のサービス、そのプロセスID、起動モード、状態、ステータスといった、不安定な情報を収集する必要がある。
以下のコマンドのうち、クラークが実行中のサービスからそのような情報を収集するのに役立つのはどれですか？
A. wmic
B. netstat -ab
C. ファイルを開く
D. ネットファイル
Answer: (解答を表示する**)**

最新問題: **16**
クラウドストレージ企業であるAlphaTechは、最近データ漏洩の被害に遭いました。調査の結果、従業員が機密性の高い顧客データを個人のメールアドレスに送信していたことが判明しました。AlphaTechは、このような事態を監視・防止するためのソリューションを導入したいと考えています。彼らは何を優先すべきでしょうか？
A. 従業員に毎月サイバー衛生ワークショップへの参加を義務付ける。
B. 機密データの移動を監視するために、データ損失防止（DLP）ツールを導入する。
C. すべての従業員に対して、メールの添付ファイルをSMBに制限する。
D. 会社のネットワーク上で、すべての個人用メールドメインをブロックします。
Answer: B (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：

このシナリオは、正規のユーザーが許可されたアクセス権を悪用して機密情報を組織の境界外に持ち出すという、典型的な内部犯行によるデータ漏洩事件を表しています。ECIHの内部脅威モジュールは、このような行為を検知・防止するための主要な技術的対策として、データ損失防止（DLP）を明確に示しています。
選択肢Bが正解です。DLPソリューションは、転送中、保存中、使用中の機密データを監視、分類、制御するように設計されています。DLPは、規制対象データや機密データが電子メールで送信されたり、クラウドサービスにアップロードされたり、外部にコピーされたりした際にそれを検知し、ポリシー違反をリアルタイムでブロックしたり、警告を発したりすることができます。
ECIHは、DLPは特に、境界防御をすり抜ける低速かつ低レベルの内部情報漏洩に対して効果的であると強調している。
オプションAは意識向上には役立つものの、管理体制の強化には繋がらない。オプションCは過度に制限的で、他の情報漏洩経路を防ぐことができない。オプションDは粗雑で容易に回避可能であり、正当な業務利用を阻害する。
ECIHのガイダンスでは、ポリシー、監視、および執行を組み合わせた多層的な内部脅威対策が重視されています。DLPは、ユーザーの行動だけに頼ることなく可視性と制御を提供するため、最も効果的な優先対策となります。

最新問題: **17**
組織内で発生したセキュリティインシデントに対応するためのアプローチとして、また、セキュリティインシデント発生時に従うべき手順を対応チームが正確に把握できるようにすることで、対応を可能にするものとして、次のうちどれが挙げられますか？
A. 脅威評価
B. インシデント対応のオーケストレーション
C. 脆弱性管理
D. リスク評価
Answer: D (メーッセージを残す**)**

最新問題: **18**
次のうち、デジタルフォレンジック分析ツールではないものはどれですか？
A. EAR/ピラール

B. ヘリックス
C. アクセスデータFTK
D. ガイダンスソフトウェア EnCase Forensic
Answer: A (メーッセージを残す**)**

最新問題**: 19**
ローズはインシデント対応担当者であり、ネットワーク上で悪意のある攻撃者によるあらゆる種類のスキャン行為を検知し、排除する責任を負っています。ローズはWiresharkツールを使用してネットワークを監視し、発生している悪意のある活動を検出します。
攻撃者によるTCPクリスマススキャン攻撃を検出するために、彼女が使用できるWiresharkフィルタは次のうちどれですか？
A. tcp.dstport==7
B. tcp.flags==0X000
C. tcp.flags.reset==1
D. tcp.flags==0X029
Answer: D (メーッセージを残す**)**
TCP Xmasスキャンは、攻撃者がターゲットマシンの開いているポートを特定するために使用するネットワークスキャン手法の一種です。 Ҡmas」という名前は、パケット内でオンにされる一連のフラグに由来しており、パケットが クリスマスツリーのように点灯する」ように見えます。具体的には、TCPヘッダーのflagsフィールドの16進数値0X029に対応するFIN、PSH、URGフラグが設定されます。一般的なネットワークプロトコルアナライザであるWiresharkでは、ユーザーがカスタムフィルタを作成して、悪意のあるスキャン試行を含む特定の種類のネットワークトラフィックを検出できます。Rose
は、filtertcp.flags==0X029を使用することで、これらの特定のフラグが設定されているパケットを検出し、潜在的なTCP Xmasスキャン試行を示すことができます。
参考資料 :Wiresharkを使用してTCP Xmasスキャンなどの特定の種類のスキャンを検出する手法は、ECIH認定に関連するものなど、ネットワーク分析とインシデント処理に関連するサイバーセキュリティトレーニング資料やドキュメントで説明されています。

最新問題**: 20**
ブランは組織のネットワークを評価しているインシデント対応担当者です。彼はWiresharkを使用して、ネットワーク上でのpingスイープ攻撃を検出したいと考えています。
ブランはこのタスクを達成するために、次のうちどのW re sharkフィルターを使用するでしょうか？
A. icmp.redir_gw
B. icmp.seq
C. icmp.type== 8
D. icmp.ident
Answer: C (メーッセージを残す**)**

最新問題: **21**
デジタル化を進めている中規模の医療機関が、ISO/IEC 27001認証の取得を目指しています。準備状況のレビュー中に、CISOはいくつかの課題を特定しました。具体的には、システムの弱点について懸念を表明するための明確なチャネルがスタッフに欠けていること、有害事象発生後の結果追跡が一貫していないこと、そしてシステム障害発生後に何がうまくいったのか、何がうまくいかなかったのかを評価する正式な方法がないことです。ISO/IEC 27001附属書A.16に準拠するために、どの対策を優先すべきでしょうか？
A. 内部脅威シナリオをシミュレートする机上演習を実施する。
B. リアルタイムアラートのための集中型SIEMダッシュボードを実装する。
C. 欠陥のエスカレーションとインシデント後の対応知識の統合のための構造化された手順を定義し、実装する。
D. エンドポイント全体にEDRエージェントを展開し、自動隔離を実行します。
Answer: C (メーッセージを残す)
ISO/IEC 27001附属書A.16は、情報セキュリティインシデント管理（報告 評価、対応、学習を含む）に焦点を当てています。ECIHのカリキュラムはこれらの要件に密接に準拠しており、体系的な手順と継続的な改善を重視しています。
選択肢Cが正解です。なぜなら、明確なエスカレーション経路、一貫した成果追跡、教訓の活用といった、特定された課題に直接対処しているからです。ECIHは、見落とされがちな事後対応活動が、準備態勢の向上と再発防止に不可欠であることを強調しています。
オプションAは準備態勢を強化するものの、システム的なプロセス上のギャップには対処しません。オプションBは可視性を向上させますが、ガバナンスには影響しません。オプションDは、インシデントの学習やエスカレーションとは無関係な技術的な制御策です。
したがって、構造化されたインシデントエスカレーションとインシデント後の知識統合を実施することが、コンプライアンスとレジリエンスのための最優先事項となる。

最新問題: **22**
マイケルはサイバーテック ·ソリューションズのインシデントハンドラーです。彼はクラウドセキュリティインシデントの検出と分析を行っています。ストレージユニットのファイルシステム、スラック領域、メタデータを分析し、隠れたマルウェアや悪意のある行為の証拠を探しています。
マイケルが対応したクラウドセキュリティインシデントを特定してください。
A. ネットワーク関連のインシデント
B. 保管関連のインシデント
C. アプリケーション関連のインシデント
D. サーバー関連のインシデント
Answer: B (メーッセージを残す)
マイケルの活動内容は、ファイルシステム、スラック領域、ストレージユニットのメタデータを分析して、隠れたマルウェアや悪意の証拠を探し出すことであり、彼がストレージ関連のクラウドセキュリティインシデントに対応していることを示している。

この種のインシデントは、クラウド環境に保存されているデータへの不正アクセス、改ざん、またはデータ漏洩を指します。マイケルは、ファイルシステムやメタデータといったストレージの側面に着目することで、データストレージに特に影響を与える侵害の兆候を探しており、これはクラウドにおけるストレージ関連のセキュリティインシデントを示唆するものです。
参考資料 :インシデントハンドラー（ECIH v3）認定資料では、さまざまな種類のクラウドセキュリティインシデントについて説明し、機密データが標的になったり侵害されたりする可能性のあるストレージに関連するインシデントを含め、それらを検出して対応する方法を詳しく解説しています。

最新問題: **23**
組織は、幹部がスピアフィッシング攻撃の一環として作成された不正なメールに返信したことで、金銭的な損失を被りました。影響を受けたシステムを隔離し、内部関係者に通知した後、インシデント対応チームは、攻撃のタイムライン、疑わしいIPアドレス、メールのメタデータ、電話詐欺の詳細、損失額を概説した詳細なレポートを作成します。このレポートは、さらなる調査と賠償の可能性を支援するために、サイバー犯罪を専門とする政府機関に転送されます。組織は、復旧プロセスのどの側面に取り組んでいるのでしょうか？
A. 法的エスカレーションおよび調査支援
B. データ冗長性計画
C. エンドポイント保護の展開
D. 内部サーバー再構成
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
このシナリオは、ECIHカリキュラムで概説されている、インシデント発生後の復旧および報告段階を反映している。
封じ込めと根絶の後、組織は、特に金融詐欺や経営幹部の不正行為が関与している場合、法的、規制的、および捜査上の要件に対処しなければならない。
選択肢Aが正解です。詳細なインシデントレポートを政府のサイバー犯罪対策機関に送付することは、法的措置の拡大と捜査支援に相当します。ECIHは、詐欺、金銭的損失、または国境を越えた犯罪行為に関わる事件において、法執行機関との協力が重要であることを強調しています。適切な文書化は、訴追、賠償請求、および規制遵守を後押しします。
オプションB、C、Dは、法的措置とは無関係な技術的な復旧措置です。
検証済みの証拠を当局に提示することで、組織は技術的な修復にとどまらず、復旧義務を果たし、ECIHのベストプラクティスに沿った活動を行う。

最新問題: **24**
ボニーのシステムは、恐ろしいマルウェアによって侵害された。
マルウェア感染の拡大を食い止めるために、ボニー社がまず取るべき対策は何ですか？
A. 組織の法務部に連絡し、事件について報告する。
B. 感染した機器の電源を切る

C. ネットワーク管理者に任せましょう
D. 事件に関して警察に正式に苦情を申し立てる
Answer: A (メーッセージを残す**)**

最新問題**: 25**
コンピュータメディアのバイナリコピーを作成するために使用されるLinuxコマンド、および入力として生のディスクデバイスが与えられた場合のディスクイメージングツールとしてのコマンドは次のとおりです。
A. "dd" コマンド
B. "nslookup" コマンド
C. ﬁetstat」コマンド
D. ﬁnd」コマンド
Answer: A (メーッセージを残す**)**

最新問題**: 26**
ある地方空港は最近、スマートIoTベースの手荷物処理システムとセキュリティカメラシステムを導入し、業務をアップグレードしました。機器の障害を想定した定例のサイバーレジリエンス訓練中に、運用スタッフは割り当てられた業務の遂行に混乱が生じ、コミュニケーションの流れも不明確でした。サードパーティベンダーとの連絡方法、影響を受けたシステムからの診断ログの取得方法、業務継続のために優先的に対応すべきユニットなどについて、不明確な点がありました。これらの準備上のギャップに最も効果的に対処できるのは次のうちどれでしょうか？
A. 監視ツールを使用して、IoTネットワーク全体における異常なアクティビティに対するアラートを自動化する
B. 脆弱なIoTエンドポイントに対して定期的なファームウェアパッチ適用をスケジュールする
C. 現実的なシミュレーションを実施し、各関係者の責任を明確に文書化する。
D. 緊急事態発生時には、重要な空港インフラをフォールバックの手動モードに切り替える。
Answer: C (メーッセージを残す**)**
EC-Councilのインシデントハンドラー（ECIH）カリキュラムでは、インシデント対応において準備が最も重要な段階であることを強調しています。組織は、インシデントが発生する前に、明確に定義された役割、コミュニケーションチャネル、エスカレーション手順、および文書化された対応ワークフローを確立する必要があります。このシナリオでは、レジリエンス訓練中の混乱、特に利害関係者の責任の不明確さ、コミュニケーションの断絶、ベンダーとの連携およびログ取得における不確実性に焦点を当てています。
ECIHは、現実的なシミュレーション、机上演習、レッドチーム／ブルーチーム演習を実施することで、組織の準備態勢が強化されると強調しています。これらの演習は、エスカレーション経路の検証、第三者との連携手順の明確化、診断ログの取得などの証拠収集手順が運用チームに十分に理解されていることの確認に役立ちます。

オプションA（自動アラート）は検出精度を向上させますが、役割の曖昧さを解消するものではありません。オプションB（ファームウェアパッチ適用）は脆弱性管理に対応しますが、コミュニケーションのギャップは解消されません。オプションD（手動フォールバックモード）は事業継続性をサポートしますが、訓練で明らかになった責任分担やエスカレーション経路の混乱を解消するものではありません。
ECIHのガイドラインでは、効果的な初期対応は、文書化された手順書、明確に定義された関係者の責任、ベンダー間の連携手順、およびインシデント対応計画の継続的なテストに依存すると明確に述べています。シミュレーションベースのトレーニングは、手順上の弱点を明らかにし、各部門がそれぞれの運用およびコミュニケーション上の責務を確実に理解できるようにします。
したがって、現実的なシミュレーションを実施し、各関係者の責任を明確に文書化することが、演習中に明らかになった準備上のギャップを埋めるための最も適切な是正措置である。

最新問題: **27**
コンピュータ犯罪の際にデジタル形式で保存または送信される、証拠価値のある情報はすべて、次のように呼ばれます。
A. デジタル証拠
B. デジタルフォレンジック調査官
C. デジタル捜査
D. コンピュータメール
Answer: A (メーッセージを残す**)**

最新問題: **28**
著名なIT企業であるZaimasoft社は、ハードウェアを直接標的とした攻撃を受け、ハードウェアに修復不可能な損傷を負った。結果として、ハードウェアの交換または再インストールが唯一の解決策となった。
Zaimasoftに対して行われたサービス拒否攻撃の種類を特定してください。
A. DDoS
B. DoS
C. PDoS
D. DRDoS
Answer: C (メーッセージを残す**)**
永続的サービス拒否（PDoS）攻撃（「ブリックング」とも呼ばれる）は、ハードウェアを標的とした攻撃の一種で、ハードウェアコンポーネントに修復不可能な損傷を与え、交換または大規模なハードウェア介入なしにはデバイスを使用不能にします。Zaimasoftで説明されているシナリオでは、攻撃者がハードウェアコンポーネントに損傷を与えた行為は、PDoS攻撃の特徴と一致しています。分散型サービス拒否（DDoS）攻撃やサービス拒否（DoS）攻撃は、一般的にシステムのリソースを一時的に過負荷にすることを目的としており、また、サードパーティのサーバーを使用した増幅技術を伴うDRDoS（分散型反射型サービス拒

否）攻撃とは異なり、PDoS攻撃は物理的なハードウェアに直接損傷を与えるため、交換または再インストールが必要になります。このため、PDoSは標的組織のハードウェアインフラストラクチャに永続的な影響を与えるため、特に深刻な攻撃となります。参考資料：インシデントハンドラー（ECIH v3）の教育リソースでは、PDoSを含むさまざまな種類のサービス拒否攻撃について詳しく説明し、各攻撃の特異な性質と影響を受けるシステムへの影響を強調しています。PDoSは、ハードウェアコンポーネントに物理的で修復不可能な影響を与えることで知られています。

最新問題: **29**
組織は、幹部がスピアフィッシング攻撃の一環として作成された不正なメールに返信したことで、金銭的な損失を被りました。影響を受けたシステムを隔離し、内部関係者に通知した後、インシデント対応チームは、攻撃のタイムライン、疑わしいIPアドレス、メールのメタデータ、電話詐欺の詳細、損失額を概説した詳細なレポートを作成します。このレポートは、さらなる調査と賠償の可能性を支援するために、サイバー犯罪を専門とする政府機関に転送されます。組織は、復旧プロセスのどの側面に取り組んでいるのでしょうか？
A. 法的エスカレーションおよび調査支援
B. データ冗長性計画
C. エンドポイント保護の展開
D. 内部サーバー再構成
Answer: (解答を表示する**)**
このシナリオは、ECIHカリキュラムで概説されている、インシデント発生後の復旧および報告段階を反映している。
封じ込めと根絶の後、組織は、特に金融詐欺や経営幹部の不正行為が関与している場合、法的、規制的、および捜査上の要件に対処しなければならない。
選択肢Aが正解です。詳細なインシデントレポートを政府のサイバー犯罪対策機関に送付することは、法的措置の拡大と捜査支援に相当します。ECIHは、詐欺、金銭的損失、または国境を越えた犯罪行為に関わる事件において、法執行機関との協力が重要であることを強調しています。適切な文書化は、訴追、賠償請求、および規制遵守を後押しします。
オプションB、C、Dは、法的措置とは無関係な技術的な復旧措置です。
検証済みの証拠を当局に提示することで、組織は技術的な修復にとどまらず、復旧義務を果たし、ECIHのベストプラクティスに沿った活動を行う。

最新問題: **30**
あるグローバル銀行のIH&Rチームは、複雑なサイバー諜報活動を調査し中です。高度な持続的脅威（APT）攻撃者は、ソフトウェアの脆弱性と人的ミスを悪用し、数か月にわたり機密性の高い金融データを不正に持ち出しました。IH&Rチームが取るべき最も適切な即時対応は何でしょうか？
A. 組織全体でサイバーセキュリティ意識向上トレーニングを実施する。
B. 法律を遵守するために違反を公表する。

C. 既知の脆弱性の修正にのみ注力する。
D. インシデント対応自動化およびオーケストレーション（IRAO）ツールを活用してデータを関連付け、脅威ハンティングを自動化します。
Answer: (解答を表示する**)**
高度な持続的脅威（APT）への対応には、連携のとれた、情報に基づいた対応が不可欠です。ECIHは、APT調査によってエンドポイント、ネットワーク、クラウドプラットフォーム全体にわたる膨大な量のテレメトリデータが生成されることを強調しています。
選択肢Dが正解です。インシデント対応自動化・オーケストレーション（IRAO）ツールは、異なるデータソースを関連付け、データエンリッチメントを自動化し、脅威ハンティングを加速します。これにより、対応者は隠れた永続化メカニズムや攻撃者のTTP（戦術、技術、手順）を効率的に特定できます。
選択肢A、B、Cは重要ではあるが、直ちに調査を行うべきものではない。
ECIHは、APT攻撃のような複雑で複数の攻撃経路が絡むインシデントに対して、オーケストレーションプラットフォームを明確に推奨しています。

最新問題**: 31**
すべてのクラウドサービスモデルにおいて、適切なネットワークサービスの提供とネットワーク関連のインシデントへの対応を主に担当するのは誰ですか？
A. クラウドコンシューマー
B. クラウド監査ツール
C. クラウドブローカー
D. クラウドサービスプロバイダー
Answer: (解答を表示する**)**
クラウドコンピューティング環境では、ネットワークサービスの提供と管理、およびこれらのサービスに関連するインシデントへの対応は、主にクラウドサービスプロバイダーの責任となります。これには、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）、SaaS（Software as a Service）モデルが含まれます。クラウドサービスプロバイダーは、提供するネットワークサービスの可用性、完全性、およびセキュリティを確保する責任を負います。この責任には、セキュリティ侵害からパフォーマンスの問題まで、これらのサービスに影響を与える可能性のあるインシデントの管理と対応が含まれます。クラウドサービスプロバイダーは、ネットワークを監視し、潜在的な脅威を特定し、サービスとそのユーザーへの影響を軽減するための是正措置を実施するために、さまざまなツールと技術を使用します。
参考資料：インシデントハンドラー（ECIH v3）コースおよび学習ガイドは、クラウドコンピューティングにおける役割と責任に焦点を当てており、クラウドサービスプロバイダーとクラウドコンシューマー間の責任の区別が強調されています。具体的には、クラウド環境におけるネットワークサービスの管理とインシデント処理は、サービスプロバイダーの重要な責任として強調されています。

最新問題: **32**
10億人以上のユーザーを抱える大手eコマース企業WebMegaは、財務情報を含む機密性の高いユーザーデータが漏洩する大規模なデータ侵害に見舞われた。封じ込め段階において、IH&Rチームは複数のセキュリティ層を迂回する巧妙な攻撃パターンを発見し、内部関係者の関与を示唆した。調査の結果、最近解雇された3人の従業員が、競合他社と関係があり、犯行の動機と手段があった可能性が浮上した。WebMegaは今後どのように対応すべきか？
A. 潜在的な内部脅威に直接対処することなく、従業員のアクセス制御に重点を置き、セキュリティ対策を全体的に強化する。
B. 外部の法医学専門家や法執行機関と協力して、機密保持を維持しながら徹底的な調査を実施する。
C. 競合他社の経営陣に接触し、法的手段を介さずに非公式な解決を図る。
D. ライバル企業を企業スパイ行為で公に告発し、初期証拠に基づいて法的措置を開始する。
Answer: B (メーッセージを残す)
包括的かつ詳細な説明（ECIH準拠）：
このシナリオは、悪意のある内部犯行の疑いと、外部との共謀の可能性を伴うものであり、法的、規制的、および証拠に関する要件が著しく高まります。ECIHのカリキュラムでは、内部犯行が疑われる場合、特に解雇された従業員や企業スパイの可能性が絡む場合、組織はフォレンジックの完全性、機密性、および合法的な調査を最優先事項としなければならないことを強調しています。
選択肢Bが正解です。外部の法医学専門家や法執行機関と連携することで、中立的で法的にも妥当な調査が保証されます。ECIHは、内部犯行事件では、内部チームだけでは持ち合わせていない専門的な法医学的能力、証拠保全、法的権限が必要となる場合が多いと強調しています。事実関係の解明が進む間、機密保持を徹底することで、組織の評判の低下や法的リスクへの対応を防ぐことができます。
選択肢Aは内部関係者の関与を無視しており、同様の事件が繰り返されるリスクがある。選択肢Cは法的保護措置を回避しており、妨害行為または共謀行為と解釈される可能性がある。選択肢Dは時期尚早であり、確証のないまま組織を名誉毀損や法的リスクにさらすことになる。

ECIHのガイダンスでは、複雑な内部事件は法的および鑑識的な厳密さをもって適切にエスカレーションされるべきであると明確に示されています。したがって、オプションBが推奨される手順に最も合致しています。

最新問題: **33**
あるテクノロジー企業のサイバーセキュリティアナリストが、研究開発専用のネットワークセグメント上で不審な活動を発見した。初期兆候から、複数のエンドポイントが侵害され、知的財産が盗まれた可能性が示唆されている。関係するデータの機密性を考慮すると、アナリストがセキュリティインシデントを検出・検証する最も効果的な方法は何か？
A. 直ちに法執行機関および規制当局に通知してください。
B. 影響を受けているネットワークセグメントを隔離し、各エンドポイントを手動で検査します。
C. エンドポイント検出および対応（EDR）ソリューションを導入し、不審なアクティビティを特定して調査します。
D. ネットワーク全体の脆弱性スキャンを実行します。
Answer: C (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
ECIHのエンドポイントセキュリティモジュールでは、現代のエンドポイントにおけるインシデントには、従来のウイルス対策ソフトや手動検査を超えた高度な検出機能が必要であることを強調しています。知的財産の窃盗は、多くの場合、基本的な対策を回避する巧妙な手口で行われます。
選択肢Cが正解です。エンドポイント検出・対応（EDR）ソリューションは、プロセス実行、メモリアクティビティ、ファイル変更、横方向の移動など、エンドポイントの動作を詳細に可視化します。EDRにより、アナリストは複数のエンドポイントにわたるインシデントを効率的に検出、調査、検証できます。
オプションBは処理が遅く、エラーが発生しやすい。オプションAは検証なしでは時期尚早である。オプションDは脆弱性を特定するものであり、実際の侵害を特定するものではない。
ECIHは、エンドポイントにおけるインシデントの検出と検証のための基盤技術としてEDRを強調しており、特に研究開発ネットワークのような高価値環境においてその重要性が高いとしている。

最新問題: **34**
IH&Rチームの一員であるイーサンは、従業員を標的としたフィッシングメールを受け取った。そのメールにはパスワードをリセットするためのリンクが含まれていた。
彼はリンクにカーソルを合わせ、表示されているURLとハイパーリンクに不一致があることに気づきます。さらに、送信者のメールの構造と件名のトーンを照合して、さらなる危険信号を検出します。イーサンはどのようなフィッシング検出方法を用いているのでしょうか？

A. コンテンツエンコーディング検証
B. ファイアウォール署名の照合
C. URL短縮検出
D. 手動によるフィッシングメールの検証
Answer: D (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
このシナリオは、ECIHメールセキュリティモジュールで教えられる基本的な検出技術である、フィッシングメールの手動検証を示しています。手動検証では、送信者アドレスの異常、URLの不一致、不自然な口調、緊急性、文脈の矛盾など、メールの特徴を人間が検査します。
選択肢Dが正解です。なぜなら、イーサンはリンクにカーソルを合わせたり、送信者の書式を確認したり、メッセージのトーンを評価したりすることで、メールを手動で検査しているからです。これらの行動は、自動ツールに頼らずにフィッシング詐欺を特定するための重要な指標となります。
オプションAはエンコーディング分析に関するものですが、ここでは説明されていません。オプションBはネットワークベースの自動検出に関するものです。オプションCは短縮URLに焦点を当てていますが、ここでは短縮URLは使用されていません。
ECIHは、自動化された防御策は重要であるものの、特に技術的な制御を回避する標的型フィッシング攻撃においては、人間の検証が依然として不可欠であることを強調しています。したがって、選択肢Dは使用されている検出方法を正しく示しています。

最新問題**: 35**
マイケルは、ある企業のコンピュータインシデント対応チームの一員です。彼の職務の一つは、メール関連のインシデントに対応することです。会社は送信元不明のメールを受信しました。彼が取るべき手順の一つは、そのメールの正当性を確認することです。
彼は以下のどのツールを使うべきでしょうか？
A. はい、ウェア
B. G Suite Toolbox
C. ゼンディオ
D. メールフォルダ
Answer: D (メーッセージを残す**)**

最新問題**: 36**
ジェームズはプロのハッカーであり、ある組織に雇われてクラウドサービスを悪用しています。この目的を達成するために、ジェームズはクラウドサービスへの匿名アクセスを作成し、パスワードや鍵のクラッキング、悪意のあるデータのホスティング、DDoS攻撃など、さまざまな攻撃を実行しました。彼がクラウドプラットフォームに及ぼす脅威は次のうちどれでしょうか？
A. 安全性の低いインターフェースとAPI
B. データ漏洩／データ損失

C. デュオの努力が不十分
D. クラウドサービスの悪用および不正利用
Answer: D (メーッセージを残す**)**
ジェームズの活動には、クラウド サービスへの匿名アクセスを作成してパスワードや鍵のクラッキングなどの攻撃を実行したり、悪意のあるデータをホストしたり、DDoS 攻撃を実行したりすることが含まれており、クラウド サービスの悪用と不正使用の典型例です。この脅威は、クラウド コンピューティング リソースを悪用して悪意のある活動を実行することを含み、クラウド サービス プロバイダーだけでなく、クラウド サービスの他のユーザーにも影響を与える可能性があります。この悪用は、クラウド プラットフォームのリソースをパスワードや暗号化キーのクラッキングなどの計算負荷の高いタスクに使用することから、正当なユーザーのサービスを妨害する可能性のある DDoS 攻撃を実行することまで多岐にわたります。参考資料:インシデント ハンドラー (ECIH v3) 認定では、クラウド サービスの悪用を含むクラウド固有のセキュリティ 課題の理解を重視し、そのようなリスクを軽減するための戦略を推奨し、クラウド環境を保護するための包括的なセキュリティ対策の必要性を強調しています。

最新問題**: 37**
ホストは脆弱なサービスを介して増殖するワームに感染します。
虫には以下が含まれます:
A. システムが不安定になる、またはクラッシュする
B. ネットワーク使用量の減少
C. 上記すべて
D. 脆弱なサービスを標的とした接続試行が確立されました
Answer: A (メーッセージを残す**)**

最新問題**: 38**
以下のファジングテスト戦略のうち、新しいデータがゼロから生成され、生成されるデータ量がテストモデルに基づいて事前に定義されるのはどれですか？
A. ログベースのファジングテスト
B. 変異ベースのファジングテスト
C. プロトコルベースのファジングテスト
D. 世代ベースのファジングテスト
Answer: (解答を表示する**)**

最新問題**: 39**
次のうち、インシデントの根本原因を取り除き、将来同様のインシデントを防ぐためにすべての攻撃経路を遮断するECIHフェーズはどれですか？
A. 根絶
B. 封じ込め
C. 回復

D. 脆弱性管理フェーズ
Answer: A (メーッセージを残す**)**

最新問題**: 40**
ファーヒーンは、フロリダに拠点を置く評判の高いIT企業でインシデント対応担当者として働いている。ファーヒーンは、同社が最近直面したサイバー犯罪の調査を依頼された。その過程で、彼女は被害を受けたシステムから静的データを収集した。
彼女はDDツールコマンドを使用してフォレンジック複製を実行し、元のディスクのNTFSイメージを取得しました。彼女はディスクのセクターごとのミラーイメージを作成し、出力イメージファイルをimage.ddとして保存しました。
Farheenが静的データを収集する際に実行した静的データ収集プロセスの手順を特定してください。
A. 比較
B. 行政上の考慮事項
C. システム保存
D. 物理的なプレゼンテーション
Answer: (解答を表示する**)**
Farheen が DD ツールを使用して元のディスクのセクターごとのミラーイメージを作成したことは、システム保存の一例です。このプロセスは、調査中に元のデータが変更されないようにストレージ デバイスの正確なコピーを作成するためにデジタル フォレンジックで非常に重要です。ディスクのフォレンジック複製、つまりイメージを作成することで、Farheen は、元の証拠を変更することなく、ディスク上の静的データが徹底的な分析のために現在の状態で保存されることを保証します。この手順により、調査官はデータの正確なレプリカを使用して作業することができ、元の証拠の完全性が保護されます。参考資料: インシデント ハンドラー (ECIH v3) 認定資料では、データ取得と保存のためのさまざまな方法とツールについて説明し、フォレンジック分析の初期段階におけるシステム保存の重要性を強調しています。

最新問題**: 41**
コンピュータウイルス詐欺とは、実際には存在しないコンピュータウイルスの脅威を警告するメッセージのことです。通常、このメッセージはチェーンメールの形式で、受信者に対し、知り合い全員に転送するよう指示します。
次のうち、ウイルス詐欺メッセージの症状ではないものはどれですか？
A. ユーザーが適切な措置を講じない場合、特定のファイルを削除するよう警告するメッセージです。
B. このメッセージは、エンドユーザーにメールの連絡先リストに転送するよう促し、そうすることで金銭的な利益が得られると謳っています。
C. このメッセージは、ユーザーにウイルス対策ソフトのインストールを促します。
D. 既知のメールアドレスからのメッセージが、フィルタ設定の変更によりスパムフィルタに引っかかっています。

Answer: (解答を表示する**)**

最新問題**: 42**
軽微なリスクを吸収しつつ、重大なリスクへの対応準備をすることは、次のように呼ばれます。
A. リスク想定
B. リスク軽減
C. リスク移転
D. リスク回避
Answer: (解答を表示する**)**

最新問題**: 43**
キャンパスネットワークに接続されたデバイスに悪意のあるプログラム（トロイの木馬、メール爆弾、ウイルスなど）を導入することを何と呼びますか？
A. 不適切な使用
B. アクセスを承認する
C. ネットワークアクセス
D. 不正アクセス
Answer: (解答を表示する**)**

最新問題**: 44**
イケオ株式会社は、企業セキュリティを評価するためにインシデント対応チームを雇用しました。インシデント処理および対応プロセスの一環として、IRチームは企業が現在実施しているセキュリティポリシーをレビューしています。IRチームは、組織の従業員がインターネットアクセスに関して何の制限も受けていないことを発見しました。従業員は、任意のサイトにアクセスし、任意のアプリケーションをダウンロードし、リモートの場所からコンピュータやネットワークにアクセスすることが許可されています。IRチームはこれを主なセキュリティ上の脅威とみなし、攻撃者によって容易に悪用される可能性があるため、このポリシーを変更することを計画しています。IRチームが変更を計画しているセキュリティポリシーは次のうちどれですか？
A. 乱交ポリシー
B. 慎重な方針
C. 寛容な方針
D. 偏執的な政策
Answer: C (メーッセージを残す**)**

最新問題**: 45**
フランシスは、銀行口座情報を要求するなりすましメールを受け取った。彼はメールヘッダーを分析するツールを使うことにした。
彼は次のうちどれを使うべきでしょうか？

A. メールチェッカー
B. 丁寧なメール
C. Mx Toolbox
D. イベントログアナライザー
Answer: C (メーッセージを残す**)**

最新問題: **46**
内部脅威対応計画は、組織が悪意のある内部者によって引き起こされる損害を最小限に抑えるのに役立ちます。これらの脅威を軽減するためのアプローチの1つは、人事部による管理体制の構築です。人事部は、次のうちどのガイドラインを利用できますか？
A. ユーザーに付与されたアクセス権限は文書化され、管理者によって審査される必要があります。
B. 責任の所在を明確にするため、デフォルトの管理者アカウントを無効にします。
C. バックアッププロセスと物理メディアを保護するために、個人間のルールを実装します。
D. 組織の物理的環境を監視し、安全を確保する。
Answer: A (メーッセージを残す**)**
内部脅威を軽減するための重要なアプローチの 1 つは、アクセス制御ポリシーが厳密に実装され、監視されていることを確認することです。これには、ユーザーに付与されたアクセスが徹底的に文書化され、上司によって検証される必要があるというガイドラインが含まれます。この制御により、ユーザーが職務を遂行するために必要なアクセスのみを持つことが保証され、不適切なアクセスや情報の悪用のリスクが軽減されます。適切な文書化と上司の承認は、アクセス決定の説明責任と追跡可能性も保証し、内部脅威を検出して対応するために不可欠です。人事部は、このプロセスにおいて重要な役割を果たし、IT チームやセキュリティ チームと緊密に連携してアクセス制御ポリシーを強制し、アクセス権限の定期的なレビューを実施し、アクセス権限が適切に更新されるようにオンボーディングおよびオフボーディング プロセスを管理します。参考資料: インシデント ハンドラー (ECIH v3) の資料では、包括的なアクセス制御対策の重要性と、従業員の組織リソースへのアクセスのライフサイクルを管理することによって内部脅威を防止する人事部の役割がしばしば強調されています。

最新問題: **47**
攻撃手段として発行される電子メール、つまり、メールボックスに複数のメッセージを送信して容量オーバーを引き起こす電子メールを最も適切に説明しているのは、次のうちどれですか？
A. 仮装
B. なりすまし
C. スマーフの攻撃
D. メール爆撃
Answer: D (メーッセージを残す**)**

最新問題: **48**
対策を実施した後に残るリスクは、次のように呼ばれます。
A. 低リスク
B. 残存リスク
C. 許容できないリスク
D. 重大なリスク
Answer: (解答を表示する**)**

最新問題: **49**
以下の手法のうち、事件処理プロセスを妨げたり、誤った方向に導いたりする可能性があり、かつ鑑識捜査プロセスの収集、保存、および識別段階にも影響を与える可能性があるものはどれですか？
A. スキャン
B. 足跡
C. 列挙
D. 反鑑識
Answer: (解答を表示する**)**
フォレンジック対策技術は、インシデント処理プロセスを妨害、誤誘導、または阻害するように設計されており、フォレンジック調査プロセスの収集、保存、および識別フェーズに影響を与えます。これらの技術には、情報の消去、暗号化、または変更、データ復旧の困難化、データの隠蔽（ステガノグラフィーなど）、またはその他のフォレンジック分析および調査活動の妨害方法が含まれます。フォレンジック対策は、セキュリティインシデントまたは犯罪の事実を確立するインシデント対応者およびフォレンジック調査官の取り組みを著しく阻害する可能性があります。参考資料：インシデントハンドラー（ECIH v3）コースおよび学習ガイドでは、フォレンジック対策方法およびフォレンジック調査の有効性への影響など、デジタルフォレンジックにおけるさまざまな課題について説明しています。
トップフォーム

最新問題: **50**

インシデント対応プロセスにおいて、インシデントハンドラーがファイルシステムを表示したり、削除されたデータを取得したり、タイムライン分析やWebアーティファクトなどを実行したりする際に役立つツールは次のうちどれですか？
A. プロセスエクスプローラ
B. 笑顔で
C. 解剖
D. netstat
Answer: C (メーッセージを残す**)**

最新問題**: 51**
ネットワークへの攻撃を最も効果的に阻止できるのは、次のうちどれですか？
A. IPSデバイスインライン
B. ヒップ
C. ロードバランサー
D. ウェブプロキシ
Answer: A (メーッセージを残す**)**

最新問題**: 52**
セキュリティアラートを受け、ある法律コンサルティング会社のインシデント対応チームは、従業員がUSBストレージデバイスを使用して機密性の高い顧客データを外部に持ち出した疑いがあると判断しました。どのUSBデバイスが接続されていたかを確認し、タイムスタンプと識別子を収集するには、どの方法が最も効果的でしょうか？
A. WindowsレジストリのEnum\USBエントリを確認してください。
B. ネットワークログをスキャンしてUSBファイルのアップロードパターンを検出します。
C. Windows SetupAPI.dev.log ファイルのエントリを確認します。
D. WHOIS検索を使用してUSBアクティビティを追跡します。
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
ECIHのフォレンジック準備ガイドラインでは、WindowsレジストリがUSBデバイスの痕跡の主要な情報源であるとされています。Enum\USBレジストリキーには、ベンダーID、製品ID、シリアル番号、および接続履歴が格納されます。
選択肢Aが正しいのは、どのUSBデバイスが接続されたか、いつインストールされたか、どのシステムにインストールされたかを直接的に示す証拠となるため、内部犯行の調査にとって非常に重要だからです。
オプションBでは、物理的なUSBの使用状況を確実に識別できません。オプションCにはドライバのインストールデータが含まれていますが、オプションBほど包括的ではありません。オプションDは無関係です。
レジストリ分析はECIHにおける基礎的な鑑識技術であるため、選択肢Aが正解となる。

最新問題**: 53**

世界的な医療サービスプロバイダーであるメガヘルス社は、MRI装置に突然の不具合が発生した。
調査の結果、MRI検査結果を改ざんし、外部のコマンド＆コントロールサーバーと通信するマルウェアが発見された。高度なエンドポイント保護システムやネットワークモニターといったツールを活用する場合、最初にとるべき対策は何だろうか？
A. 患者にデータ侵害の可能性について知らせる。
B. ネットワークモニターを使用して、C&Cサーバーとの通信を特定してブロックします。
C. MRI装置のファームウェアとソフトウェアを更新します。
D. MRI装置にエンドポイント保護を導入して、マルウェアを検出して停止します。
Answer: (解答を表示する**)**
包括的かつ詳細な説明（ECIH準拠）：
今回の事案は、医療機器にマルウェアが積極的に影響を与え、患者の安全を脅かす事態です。ECIHのマルウェア事案対応原則によれば、最優先事項はエンドポイントレベルでの封じ込めと駆除です。
選択肢Dが正解です。エンドポイント保護を導入することで、MRI装置上でマルウェアの実行を直接検知して停止させることができ、結果の改ざんやさらなる悪意のある活動を阻止できます。ネットワークレベルや復旧措置の前に、エンドポイントの封じ込めは不可欠です。
オプションBは通信に関する事項を扱いますが、ローカル操作を阻止するものではありません。オプションCは、封じ込め措置なしにシステム状態を変更します。オプションAは、バリデーションに続く規制上のステップです。
ECIHは、重要インフラおよび医療環境においては、安全性とデータ完全性を保護するために、エンドポイントの即時封じ込めが不可欠であることを強調している。

最新問題**: 54**
インシデント対応と処理の正しい手順は以下のとおりです。
A. 事案の特定、初期対応、連絡、記録、封じ込め
B. 事案の特定、記録、初期対応、封じ込め、および通信
C. 事案の特定、記録、初期対応、連絡、封じ込め
D. 事案の特定、連絡、記録、初期対応、封じ込め
Answer: C (メーッセージを残す**)**

最新問題**: 55**
ある大手多国籍企業は最近、応募者の書類提出と書類収集を効率化するために、デジタル人事オンボーディングシステムを導入しました。サイバーセキュリティ監査中に、攻撃者が公式の人事書類提出ポータルを模倣したフィッシングサイトを設置していたことが判明しました。複数の従業員と新入社員が、正規のものだと信じて履歴書をアップロードし、入力済みのフォームテンプレートをダウンロードしました。ダウンロードしたWord文書を開くと、システムはユーザーの同意やマクロ実行の警告なしに、外部サーバーに密かに接続

し、追加のテンプレートデータを取得しました。これにより、メールゲートウェイのフィルタやエンドポイントのウイルス対策ツールが回避され、人事、財務、法務部門で使用されるシステム全体にマルウェアが拡散しました。
デジタルフォレンジック分析の結果、これらの文書には目に見えるスクリプトやマクロは含まれておらず、攻撃者が制御するサーバーから悪意のあるペイロードを動的に取得するために、隠された構造定義に依存していたことが判明した。
以下のウェブベースのマルウェア配布手法のうち、観測された挙動を最もよく説明できるのはどれですか？
A. リモートホスト型RTFインジェクションによるマルウェアの配布。
B. ソーシャルメディアの連絡先になりすましたスピアフィッシングメールによるマルウェアの配布。
C. PDFレンダリングエンジンに組み込まれた侵害されたブラウザ拡張機能を介したマルウェアの配布。
D. 内部ネットワーク内でのピアツーピアファイル伝播メカニズムを介したマルウェアの配布。
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
この事例は、文書ベースのWebマルウェア配信メカニズム、特にリモートホストされたリッチテキストフォーマット（RTF）の注入を利用したメカニズムを示しています。これは、ECIHのWebおよびマルウェア処理モジュールで詳しく説明されています。RTF文書は外部オブジェクトやテンプレートを参照できるため、マクロやユーザーの操作を必要とせずに、文書を開いた際に悪意のあるペイロードを動的に取得することが可能です。
選択肢Aが正解です。なぜなら、説明されている動作はリモートテンプレートインジェクションと完全に一致するからです。マクロの欠如、サイレントな外部接続、構造化されたドキュメント要素の使用は、RTFベースのマルウェア配信の典型的な兆候です。ECIHは、この手法が従来のマクロベースの検出およびユーザー警告メカニズムを回避するため、高リスクの手法として指摘しています。
選択肢Bは、ペイロードがダウンロードされたドキュメントを介して配信されたのであって、ソーシャルコンタクトを装ったメールによる配信ではないため、誤りです。選択肢Cはブラウザ拡張機能とPDFに言及していますが、これらは関係ありません。選択肢Dは、初期配信ではなく、横方向への拡散について説明しています。
ECIHは、現代のウェブベースの攻撃では、制御を回避するために、信頼できるドキュメント形式やリモートオブジェクト参照が悪用されるケースが増えていることを強調しています。これらの手法を理解することで、対応者はドキュメントのサニタイズ、送信トラフィックの監視、コンテンツの無害化と再構築（CDR）といった制御機能を向上させることができます。

最新問題: **56**

Google Cloud Platform (GCP) に新しいアプリケーションをデプロイした後、セキュリティエンジニアは、許可されていないエンティティがアプリケーションのバックエンドサービスにアクセスしていることを発見しました。このセキュリティインシデントに対処するために、エンジニアはまず次のうちどの対策を講じるべきでしょうか？
A. IAMロールと権限を見直し、過剰なアクセスがないか確認し、セキュリティ制御を強化してください。
B. Google Cloud セキュリティ コマンド センターを有効にして、将来の脅威を検出できるようにします。
C. アプリケーションサービスを、セキュリティ設定がより強力な別の GCP プロジェクトに移行します。
D. VPC サービス コントロールを使用して、影響を受けるサービスの周囲に安全な境界を作成します。
Answer: (解答を表示する**)**
包括的かつ詳細な説明（ECIH準拠）：
クラウド環境におけるバックエンドサービスへの不正アクセスは、多くの場合、過度に寛容なIDおよびアクセス管理（IAM）設定が原因で発生します。ECIHのクラウドインシデント対応ガイドラインでは、ID制御がクラウドプラットフォームにおける主要なセキュリティ境界であることを強調しています。
選択肢Aが正解です。IAMロールを見直して強化することで、攻撃対象領域が即座に縮小し、悪用される可能性のある過剰な権限が取り消されます。この対策は、不正アクセスの根本原因に直接対処するものです。
オプションDは強力な追加制御策ですが、IAMの設定ミスを修正した後に行うべきです。オプションBは将来の検出精度を向上させますが、現在のインシデントを封じ込めるものではありません。オプションCは混乱を招くため、初期対応としては不要です。
したがって、IAMの見直しと権限の厳格化は、ECIHのベストプラクティスに沿った、適切な最初の対策である。

最新問題**: 57**
ジェームズはプロのハッカーであり、ある組織に雇われてクラウドサービスを悪用しています。この目的を達成するために、ジェームズはクラウドサービスへの匿名アクセスを作成し、パスワードや鍵のクラッキング、悪意のあるデータのホスティング、DDoS攻撃など、さまざまな攻撃を実行しました。彼がクラウドプラットフォームに及ぼす脅威は次のうちどれでしょうか？
A. 安全性の低いインターフェースとAPI
B. データ漏洩／データ損失
C. デュオの努力が不十分
D. クラウドサービスの悪用および不正利用
Answer: D (メーッセージを残す**)**

ジェームズの行為、例えばクラウドサービスへの匿名アクセスを作成してパスワードや鍵のクラッキングなどの攻撃を実行したり、悪意のあるデータをホストしたり、DDoS攻撃を実行したりといった行為は、クラウドサービスの悪用と不正利用の典型例である。この脅威は、クラウドコンピューティングリソースを悪用して悪意のある活動を行うことであり、クラウドサービスプロバイダーだけでなく、クラウドサービスの他のユーザーにも影響を及ぼす可能性がある。
この不正利用は、クラウドプラットフォームのリソースをパスワードや暗号鍵の解読といった計算負荷の高いタスクに利用することから、正規ユーザーのサービスを妨害する可能性のあるDDoS攻撃を行うことまで多岐にわたる。
参考資料 :インシデントハンドラー（ECIH v3）認定資格は、クラウドサービスの悪用を含むクラウド特有のセキュリティ上の課題を理解することを重視し、そのようなリスクを軽減するための戦略を推奨し、クラウド環境を保護するための包括的なセキュリティ対策の必要性を強調しています。

最新問題: **58**
従業員が解雇された場合、組織は次にどのような措置を直ちに講じるべきでしょうか？
A. 組織は、機密情報へのアクセス権限を持つシステム管理者および特権ユーザーの活動を監視する必要があります。
B. 組織は職務分掌を徹底すべきである
C. 従業員の物理的な場所、ネットワーク、システム、アプリケーション、データへのすべてのアクセス権限を無効にする必要があります。
D. 従業員に付与されたアクセス要求は文書化され、上司によって審査される必要がある。
Answer: C (メーッセージを残す**)**

最新問題: **59**
次の用語のうち、インシデント対応チームがインシデントを報告し、必要な許可を得るために連絡しなければならない担当者を指すのはどれですか？
A. 民事訴訟
B. 接点
C. 刑事告発
D. チケット販売
Answer: B (メーッセージを残す**)**
インシデント対応（IH&R）の文脈において、「連絡担当者」とは、インシデント発生時にIH&Rチームから連絡を受けるよう指定された組織内の個人または部署を指します。これらの担当者は、報告プロセスおよびインシデント対応活動を進めるために必要な許可を取得する上で極めて重要です。彼らは、インシデント対応チームと、インシデント対応プロセスに関与する組織内の他の部署、外部機関、またはパートナーとの間の連絡役を務めます。連絡担当者は、コミュニケーションの円滑化、行動の調整、および適切な関係者がインシデント対

応に関与することの確保を担当します。この役割は、セキュリティインシデントへの迅速かつ効果的な対応、被害の最小化、および業務の復旧を確保する上で極めて重要です。
参考資料:インシデントハンドラー (ECIH v3) コースおよび学習ガイドでは、通常、連絡先の指定を含め、インシデント対応プロセスにおける明確に定義された役割と責任の重要性が強調されています。

最新問題: **60**
以下の方法のうち、インシデント対応担当者が誤検知アラート率を低減し、最優先事項に焦点を当てることで潜在的なリスクや企業の責任を軽減するのに役立つものはどれですか？
A. 脅威の文脈化
B. 脅威の帰属
C. 脅威相関
D. 脅威プロファイリング
Answer: D (メーッセージを残す**)**

最新問題: **61**
デジタルファーストレスポンダーの資格を持つデビッドは、企業の人事部で発生したセキュリティ侵害の報告現場に到着した。侵害は、デスクトップシステムやモバイルデバイスなど、複数のデジタルエンドポイントに及んでいる。現場に到着したデビッドは、デスクトップコンピュータの1台がまだ電源が入っていてログイン状態になっており、画面に機密性の高い財務ダッシュボードが表示されていることに気づいた。証拠を保全することの重要性を認識したデビッドは、キーボードを直接操作したり、アプリケーションを実行したりすることを控えた。代わりに、画面の高解像度写真を撮影し、開いているアプリケーションや時間制限のあるデータなど、現在のセッションの詳細を記録した。システムの状態を変更しないように、デビッドはマウスをクリックせずにそっと動かし、画面に変化を与えることなくスクリーンセーバーを終了させた。彼はシステムの動作を記録し、表示されている警告や実行中のプログラムを記録し、適切な文書化のために接続されているすべてのケーブルと周辺機器ポートにタグを付けた。デビッドは証拠処理プロセスのどのステップを示しているか？
A. オフサイトバックアップの取得
B. 活性システムからの揮発性証拠の保存
C. Linux上でシャットダウンスクリプトを実行する
D. 電源オフ状態のデバイスの取り扱い
Answer: B (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
このシナリオは、ECIHフォレンジック準備モジュールにおける重要な初期対応原則である、揮発性証拠の保全を実証するものです。揮発性証拠とは、アクティブなセッション、実行中のプロセス、開いているファイル、画面上の情報など、システムの電源が入っている間だけ存在するデータのことです。

選択肢Bが正解です。なぜなら、デイビッドは証拠を改変するような操作をすることなく、稼働中のシステムの状態を記録しているからです。画面の撮影、目に見える動作の記録、接続状況の記録は、電源が入っているシステムを扱う際に推奨されるECIH（電子犯罪情報管理）の実践方法です。
オプションAは無関係です。オプションCはシステムの状態を変更します。オプションDは非アクティブなデバイスにのみ適用されます。
ECIHは、稼働中のシステムを誤って取り扱うと、重要な証拠が失われる可能性があると強調している。デイビッドの行動は、救急隊員の最善の行動規範に完全に合致しており、したがって選択肢Bが正しい。

最新問題**: 62**
証拠保全方針によれば、法医学捜査官は少なくとも.....画像を作成する必要がある。
デジタル証拠のコピー。
A. 画像コピー1枚
B. 画像コピー2枚
C. 画像コピー3枚
D. 画像コピー4枚
Answer: (解答を表示する**)**
説明／参考資料：

最新問題**: 63**
多国籍企業における大規模な情報漏洩事件の調査後、インシデントハンドラーは、侵害され、グローバルなボットネット作戦の一部として利用されていると考えられるサーバーからデジタル証拠を保存、パッケージ化、輸送するという重要な役割を担うことになった。課題は、作戦の技術的な複雑さだけでなく、証拠が法廷で認められるよう、厳格な法的および手続き上の枠組みを遵守することにもあった。以下の選択肢のうち、輸送中の証拠の完全性を最も確実に保証するのはどれか？
A. サーバーのデータをオンサイトで暗号化し、その後、安全なクラウドストレージにアップロードします。

B. サーバーのドライブのフォレンジックイメージを作成し、イメージハッシュを検証し、イメージを暗号化されたドライブに保存し、詳細なトランスポートログを維持します。
C. サーバーを帯電防止包装材で覆い、保管管理記録ラベルを貼付する。
D. 書き込みブロッカーとGPS追跡を使用して、サーバーデータを新しいドライブに転送します。
Answer: B (メーッセージを残す**)**
ECIHのフォレンジック準備ガイドラインでは、ハッシュ検証付きフォレンジックイメージングが証拠の完全性を維持するためのゴールドスタンダードであると強調されています。オプションBは、データの完全性、真正性、否認防止を保証するため、正解です。
ビット単位のフォレンジックイメージを作成することで、オリジナルの証拠を保存しつつ、コピー上での分析が可能になります。ハッシュ検証により、取得時や転送時に改ざんが行われていないことが確認できます。暗号化されたストレージは機密性を保護し、詳細なログは証拠保全の連鎖を裏付けます。
オプションA、C、Dは、ハッシュ検証や証拠の分離といった、重要なフォレンジック要件の1つ以上を欠いています。ECIHは、物理的な輸送やリアルタイムのデータ転送のみに依存することに対して明確に警告しています。

最新問題**: 64**
Alexaが映画ファイルをダウンロードした。しかし、実行時に危険なプログラムが起動し、Alexaのクレジットカード情報が攻撃者に送信された。
映画ファイルに偽装したこの悪意のあるプログラムとは一体何ですか？
A. ルートキット
B. ランサムウェア
C. トロイの木馬
D. バックドア
Answer: C (メーッセージを残す**)**

最新問題**: 65**
インシデント対応担当者のデビッドは、CFOのメールアカウントが侵害され、ベンダーに請求書の変更依頼が送信されたというメールベースの侵害事件を調査している。ログによると、CFOがメールで送られてきた偽のMicrosoft 365ログインプロンプトをクリックした後、攻撃者は有効な認証情報を使用してアカウントにアクセスしたことが判明した。
攻撃者はどの手法を用いた可能性が最も高いか？
A. 郵便爆弾
B. ファーミング
C. スピミング
D. スピアフィッシング
Answer: D (メーッセージを残す**)**
今回の事件は典型的なスピアフィッシング攻撃であり、標的となった人物が騙されて偽のログインページに認証情報を入力させられるというものです。ECIHのメールセキュリティ

モジュールでは、スピアフィッシングは高度に標的を絞った攻撃であり、多くの場合、経営幹部などの特定の役割に合わせて仕組まれていると説明しています。
選択肢Dが正解です。CFOは巧妙に偽装されたMicrosoft 365ログイン画面の標的となり、認証情報が盗まれました。その後、有効な認証情報が使用されたことから、技術的な悪用ではなく、ソーシャルエンジニアリングが成功したことが確認できます。
オプションAはメールの大量送信を伴う。オプションBはDNS操作によってトラフィックをリダイレクトする。オプションCはモバイルメッセージングプラットフォームを標的とする。
スピアフィッシングを認識することは非常に重要です。なぜなら、認証情報のリセット、多要素認証の実施、経営幹部向けの意識向上トレーニングなど、ECIHのガイダンスで強調されている対策を講じる上で役立つからです。

最新問題: **66**
以下の選択肢のうち、フィッシングメールの一般的な特徴を説明しているのはどれですか？
A. 緊急性、脅迫性、または約束的な件名
B. BCCフィールドなし
C. フランス語で書かれています
D. 友人や同僚から送られてきた
Answer: A (メーッセージを残す**)**

最新問題: **67**
フランシスはインシデント対応担当者であり、セキュリティ専門家です。彼はオーストラリアのシドニーに拠点を置くモリソン -テック -ソリューションズに勤務しています。彼はクライアント企業のためにフィッシングメールやスパムメールを検出する任務を任されました。
以下のツールのうち、フランシスが要求された作業を実行するのに役立つものはどれですか？
A. ネッソス
B. ネットクラフト
C. BTクラック
D. カインとアベル
Answer: B (メーッセージを残す**)**

最新問題: **68**
クラウドセキュリティアナリストが、クラウドホスト型アプリケーションを標的とした複雑なマルチベクター攻撃（DDoS攻撃、フィッシング攻撃、マルウェア侵入）を特定しました。クラウドインシデント対応において、効果的に対応するために克服すべき最も重要な課題は何でしょうか？
A. 金融業界の規制を遵守しながら対応すること。

B. クラウドサービスプロバイダーと効果的にコミュニケーションを取り、範囲を理解する。
C. 正当なトラフィックと攻撃トラフィックを区別して、混乱を最小限に抑えます。
D. さまざまなクラウドサービスとプラットフォーム間で対応活動を調整する。
Answer: D (メーッセージを残す)
説明（クラウドIRの現実）：
複数の攻撃経路が絡むクラウドインシデントにおいて、最も重要な課題は、アイデンティティ管理（IAM）、ネットワーク（WAF/CDN/LB）、コンピューティング（VM/コンテナ/関数）、メール/コラボレーション、エンドポイント、サードパーティSaaS統合といった階層化されたサービス間の連携です。それぞれの攻撃経路は異なる領域に影響を及ぼすことが多く、フィッシングはアイデンティティを侵害し、マルウェアはエンドポイントやワークロードに常駐し、DDoS攻撃はエッジ/ネットワーク層に負荷をかけます。効果的な対応には、これらの領域全体にわたる封じ込め対策を整合させ、ある対策によって別の脆弱性が残らないようにする必要があります（例えば、DDoS攻撃は阻止するものの、侵害されたアイデンティティがアクティブなままになる、あるいは悪意のあるOAuthトークンが有効なままワークロードをクリーンアップするなど）。
（B）は重要ですが、調整のサブセットです。CSP通信は、より広範なマルチサービス対応における依存関係の1つです。（C）は戦術的なDDoS問題であり重要ですが、このインシデントにはフィッシングとマルウェアが含まれているため、トラフィック分類のみに焦点を当てるのは不十分です。（A）は規制対象企業にとって重要ですが、積極的な対応中は、コンプライアンスは通常、事前に定義された手順で対処されるため、マルチベクターキャンペーンを阻止する上での主な運用上の障害ではありません。
したがって、（D）はクラウド特有の複雑さを最もよく捉えています。つまり、分散された所有権、共有された責任の境界、そしてキルチェーンを真に断ち切るために同期されたアクション（トークンの取り消し、ワークロードの分離、セキュリティグループの調整、WAFルール、メール保護、エンドポイントの封じ込め）が必要であるということです。

最新問題: **69**
アレックスはTech-o-Tech Inc.のインシデントハンドラーであり、組織内の潜在的な内部脅威を特定する任務を負っています。アレックスは、個人およびグループにおける疑わしい従業員の行動に基づいて内部脅威を検出するために、次のうちどの内部脅威検出手法を使用できますか？
A. 行動分析
B. 物理的検出
C. プロファイリング
D. ほくろ検出
Answer: A (メーッセージを残す)
行動分析は、従業員の行動を個人およびグループの両方で分析し、通常とは異なる行動を特定することで、内部脅威を検出するために使用される手法です。この方法は、ユーザーア

クティビティ、アクセスパターン、および組織内部からの悪意や潜在的なセキュリティリスクを示す可能性のあるその他の行動に関連するデータを監視および分析することに依存しています。行動分析は、機密データへの異常なアクセス、異常なデータ転送アクティビティ、および内部脅威のその他の指標を検出できます。このアプローチはプロアクティブであり、組織に重大な損害を与える前に潜在的な内部脅威を特定するのに役立ちます。参考資料: インシデントハンドラー (ECIH v3) 認定資料では、内部脅威検出のさまざまな手法について説明しており、内部者によってもたらされる潜在的なセキュリティリスクを特定するための重要な方法としての行動分析の重要性についても説明しています。

最新問題: **70**
悪意のあるメールを検出して封じ込める過程で、インシデント対応担当者は、メールの発信元IPアドレスを調査する必要があります。
発信元IPアドレスを調査する手順は以下のとおりです。
1. WHOISデータベースでIPアドレスを検索する
2. メールを開いてヘッダーを探します
3. 受信したメールのヘッダーから送信者のIPアドレスを取得する
4. WHOISデータベースで送信者の地理的住所を検索する
インシデント対応担当者がメールの発信元IPアドレスを調査するために実行すべき正しい手順を特定してください。
A. 4-->1-->2-->3
B. 2-->1-->4-->3
C. 1-->3-->2-->4
D. 2-->3-->1-->4
Answer: (解答を表示する**)**
メールの送信元IPアドレスを調べる正しい手順は、まずメールのヘッダーにアクセスしてIPアドレスを特定し、次に外部リソースを使用してそのアドレスをさらに調査することです。手順は以下のとおりです。
* ステップ 2: メールを開いてヘッダーを探します。ヘッダーには、送信元の IP アドレスなど、メールがインターネット上を通過する経路に関する貴重な情報が含まれているため、これが最初のステップとなります。
* ステップ3：受信したメールのヘッダーから送信者のIPアドレスを取得します。この情報は、調査の次のステップにおいて非常に重要です。
* ステップ 1: WHOIS データベースで IP アドレスを検索します。このデータベースには、ISP や場合によっては地理的な場所など、IP アドレスの所有者に関する情報が含まれています。
* ステップ 4: WHOIS データベースで送信者の地理的な住所を検索します。WHOIS 検索で取得した IP アドレス情報から、メールの地理的な場所や発信国を推測できる場合が多く、メールの正当性の分析に役立ちます。
参考資料：電子メールヘッダーを分析して発信元IPアドレスを追跡し、それらのアドレスをさらに調査するプロセスは、インシデント対応における一般的な手法であり、EC-Council

のECIH v3カリキュラムのデジタルフォレンジックと電子メール分析のトピックで扱われています。

最新問題: **71**
インシデントハンドラーのシャリーは、フロリダ州に拠点を置くテキサス社（Texas Pvt.Ltd.）に勤務しています。彼女はインシデント対応計画の策定を依頼されました。計画の一環として、彼女は企業のセキュリティインフラを強化・改善することにしました。彼女は、セキュリティ担当者が情報システム全体に複数の保護レイヤーを使用できるセキュリティ戦略を導入しました。このセキュリティ戦略は、多層防御を採用しているため、組織の情報システムへの直接攻撃を防ぐのに役立ちます。なぜなら、あるレイヤーに侵入しても、攻撃者は次のレイヤーへと進むだけだからです。
Shall y がインシデント対応計画に組み込んでいるセキュリティ戦略を特定してください。
A. 指数バックオフアルゴリズム
B. 秘密チャンネル
C. 三者握手
D. 多層防御
Answer: D (メーッセージを残す**)**

最新問題: **72**
高速検出、構成監査、資産プロファイリング、機密データ検出、脆弱性分析などの機能を備えたアクティブ脆弱性スキャナーは、次のように呼ばれます。
A. サイバーコップ
B. ネッソス
C. イーサラップ
D. nmap
Answer: B (メーッセージを残す**)**

最新問題: **73**
インシデント処理および対応（IH&R）プロセスの以下のどの段階で、インシデント担当者はインシデントの根本原因、インシデントの背後にいる脅威アクター、脅威ベクトルなどを特定しようとしますか？
A. 事件の記録と割り当て
B. 証拠収集および法医学分析
C. 事件後の活動
D. インシデントトリアージ
Answer: (解答を表示する**)**

最新問題: **74**
Qual Tech Solutionsは、セキュリティサービスを提供する大手企業です。ディクソンはこの会社でインシデント対応担当者として勤務しています。彼は、自動化ツールを使用して

企業ネットワーク内のホスト、サービス、脆弱性を特定し、ネットワークのセキュリティ上の問題点を明らかにするための脆弱性評価を実施しています。
上記のシナリオに基づき、ディクソン社が実施した脆弱性評価の種類を特定してください。
A. 受動的評価
B. 内部評価
C. アクティブ評価
D. 外部評価
Answer: B (メーッセージを残す**)**

最新問題**: 75**
攻撃者は攻撃を実行した後、鑑識調査を回避するために、アーティファクト消去技術を用いて証拠を消去することにした。彼はデジタルメディア機器に磁場を印加し、その結果、以前保存されていたデータが完全に消去された状態になった。
攻撃者が使用したアーティファクト消去手法を特定する。
A. ファイル消去ユーティリティ
B. ディスクの消磁／破壊
C. ディスククリーニングユーティリティ
D. システムコールプロキシ
Answer: B (メーッセージを残す**)**
攻撃者がデジタルメディアデバイスに磁場を印加して、以前に保存されていたデータをすべて消去するこの手法は、ディスク消磁として知られています。消磁とは、ディスクやテープを強力な磁場にさらすことで磁気データ記憶機構を破壊し、デバイスからデータを完全に消去する方法です。このプロセスは、デジタル証拠を復元不可能な方法で消去するために効果的に使用され、フォレンジック対策として機能します。データを上書きまたは削除するファイル消去ユーティリティやディスククリーニングユーティリティとは異なり（復元可能な痕跡が残る可能性があります）、消磁は記憶媒体自体を物理的に変化させるため、データの復元は不可能になります。
参考文献 :ECIH v3認証プログラムでは、攻撃者が検出や調査を回避するために使用するフォレンジック対策方法を理解する一環として、消磁を含むさまざまなアーティファクト消去技術について説明しています。

最新問題**: 76**
ある国際物流企業は、ITシステムが倉庫自動化システムと連携し、プログラマブルユニットとダッシュボードを介して仕分け、配送ルート設定、コンベア調整などのタスクを実行するスマートハブを運営している。最近、第三者のリモートメンテナンス用トンネルが侵害されたことが原因で発生したサイバー攻撃により、バックエンドのスケジューリングアプリケーションと組み込み自動化ユニット間の通信が途絶え、処理ラインの停止や出荷遅延が発生した。

影響を受けたセグメントを隔離し、悪意のあるコンポーネントを削除し、重要なワークフローを復元した後、復旧チームは復旧した運用の検証を開始します。ログと構成をレビューする中で、内部認証サーバーと組み込み自動化モジュール間で過剰な権限が付与されていることを発見しました。
システムインターフェース間の通信を検証するために使用される認証トークンの異常も検出します。これには、元の構成と一致しない未確認のフィンガープリントなどが含まれます。安全な復旧計画の一環として、どの対策を優先すべきでしょうか？
A. SCADAデバイスを標的とするマルウェアの亜種を検出するために、新しいIDSシグネチャを適用する
B. レッドチームによるシミュレーションを実施し、OTセグメンテーション防御をテストする。
C. ファームウェアの安定動作を確認するため、すべてのシステムを再起動してください。
D. 制御システム全体にわたってきめ細かなロールベースのアクセス ポリシーを適用し、信頼できるデバイス証明書を検証する
Answer: D (メーッセージを残す**)**
EC-Councilのインシデントハンドラー（ECIH）カリキュラムでは、復旧は単に機能を回復させるだけでなく、再感染や継続的な侵害につながる可能性のある残存セキュリティ上の脆弱性を排除する必要があることを強調しています。運用技術（OT）および産業環境においては、相互接続されたシステム間のID検証、証明書の信頼性、および厳格なアクセス制御が不可欠です。
このシナリオは、認証サーバーと自動化モジュール間の過剰な権限設定と、認証トークンにおける未確認のフィンガープリントの異常という、2つの主要な問題点を浮き彫りにしています。これらの結果は、信頼関係の侵害と、過剰な権限を持つシステム通信を示しています。
ECIHの復旧ガイダンスでは、システムが完全に復旧したと宣言する前に、認証メカニズムの再検証、最小権限の原則の適用、信頼関係の見直し、証明書の完全性の確保を徹底するよう強調しています。きめ細かなロールベースアクセス制御（RBAC）の実装と信頼できるデバイス証明書の検証は、過剰な権限と認証異常の両方に直接対処します。
オプションAは検出精度を向上させますが、信頼設定の誤りを修正するものではありません。オプションB（レッドチームシミュレーション）は有用ですが、認証制御のセキュリティ確保に比べると二次的なものです。オプションC（システム再起動）は、権限や証明書の検証に関する問題を解決しません。
したがって、きめ細かな役割ベースのアクセス ポリシーを適用し、信頼できるデバイス証明書を検証することが、最も重要な安全な復旧対策となります。

最新問題: 77
共通の役割を除いて、IRT の役割は組織ごとに異なります。
IRTのインシデントコーディネーターが果たす役割は以下のとおりです。
A. インシデントに焦点を当て、管理面と技術面の両方から対処する。
B. 法務、人事、各種事業など、事件の影響を受けるグループをリンクします。
分野と管理
C. 適切な技術を事件に結び付け、財団のオフィスが復旧されるようにする
できるだけ早く通常の業務に戻る
D. 適切な技術を適用し、事件の根絶と復旧を試みる
Answer: B (メーッセージを残す)

最新問題: 78
インシデント対応チームの一員であるサミールは、複数の従業員が偽の社内通知を受け取った後、知らず知らずのうちに偽のログインページに認証情報を入力してしまったという警告を受けた。攻撃に使用されたドメイン名には、微妙な文字の変更が加えられていた。この攻撃はどのような不正アクセス事件から始まったのか？
A. DNSフットプリンティング
B. ポートスキャン
C. 社会工学
D. ARPスプーフィング
Answer: C (メーッセージを残す)
ECIHのインシデント対応入門モジュールでは、ソーシャルエンジニアリングは、攻撃者が技術的な脆弱性を悪用することなく不正アクセスを取得するために用いる主要な手法であると指摘している。
選択肢Cが正解です。この攻撃は、偽の通知や類似ドメインといった欺瞞的な手法を用いてユーザーを騙し、認証情報を漏洩させようとしています。これは典型的なソーシャルエンジニアリングの手法であり、最初の侵入経路としてよく用いられます。
選択肢A、B、Dは、技術的な偵察またはネットワーク攻撃であり、人間を対象とした欺瞞ではありません。
ソーシャルエンジニアリングを根本原因として認識することは、ECIHのガイダンスで強調されているユーザー意識向上トレーニング、フィッシング対策、多要素認証などの適切な対策を選択する上で不可欠です。

最新問題: 79
ある国際銀行において、ITセキュリティチームはマルウェア感染の可能性を示す異常なネットワークトラフィックを検出しました。さらに分析を進めた結果、複数の高価値トラ

ンザクションサーバーが外部のコマンド＆コントロールサーバーと通信していることが判明しました。チームは、このマルウェアインシデントのトリアージを最適に処理するために、直ちに取るべき行動を決定する必要があります。脅威を軽減し、機密データを効果的に保護するために、何を優先すべきでしょうか？
A. 影響を受けたサーバーをネットワークから切断し、さらなるデータ漏洩を防ぐ。
B. トランザクションサーバーの現在の状態を維持するために、制御されたシャットダウンを開始します。
C. すべてのネットワーク機器とサーバーのウイルス対策シグネチャを即座に更新します
D. 影響を受けたサーバーのメモリダンプを実行し、詳細なフォレンジック分析を行う
Answer: A (メーッセージを残す**)**
このシナリオは、コマンド＆コントロール（C2）通信が確認されたアクティブなマルウェア感染を描写しており、機密性の高い金融データに対する差し迫った深刻なリスクを示しています。EC-Council ECIHのマルウェアインシデント対応プロセスによれば、このような場合の最優先事項は封じ込めであり、具体的には進行中の悪意のある活動を停止し、さらなるデータ漏洩を防ぐことです。
選択肢Aが正解です。影響を受けたサーバーをネットワークから切断することで、攻撃者の制御チャネルが即座に遮断され、外部へのデータ漏洩が停止します。ECIHは、C2トラフィックが観測された場合、対応者は、より詳細なフォレンジック分析や修復を行う前に、侵害されたシステムを隔離するために断固とした行動を取らなければならないと強調しています。封じ込めによって被害を最小限に抑え、法的、経済的、そして評判への影響を軽減できます。
オプションBはシステムの状態を維持する可能性がありますが、シャットダウンが完了するまでデータの流出が継続するため、重要な銀行業務に支障をきたす可能性があります。
オプションCは予防措置であり、既に発生している感染を阻止するものではありません。
選択肢Dは調査には有益だが、封じ込め後に行うべきであり、封じ込め前に行うべきではない。
ECIHの指針は、重要な資産が危険にさらされている場合、証拠収集よりも被害の防止を常に優先する。
したがって、影響を受けたサーバーのネットワーク接続を直ちに切断することが、適切な緊急対応策である。

最新問題: **80**
定量的リスク分析について正しいのはどれか？
A. 主観的ではあるが、定性的なリスク分析よりも速い。
B. 定性的なリスク分析よりも優れている
C. レベルと描写表現を用いる
D. 簡単に自動化できる
Answer: D (メーッセージを残す**)**

最新問題: **81**

サーベンス・オクスリー法（SOX法）のタイトルを特定してください。このタイトルは1つのセクションのみで構成されており、証券アナリストの報告に対する投資家の信頼回復を支援するために設計された措置が含まれています。
A. タイトルV：アナリストの利益相反
B. 第7章：研究および報告
C. 第VIII編：企業および刑事詐欺の責任
D. タイトルIX：ホワイトカラー犯罪刑罰強化
Answer: A (メーッセージを残す)

最新問題: **82**
次の用語のうち、限られた時間内で最小限の調査コストでデジタル証拠を最適に活用する組織の能力を指すのはどれですか？
A. 脅威評価
B. データ分析
C. リスク評価
D. 鑑識準備
Answer: D (メーッセージを残す)
フォレンジック対応準備とは、調査のコストと業務への支障を最小限に抑えつつ、調査においてデジタル証拠を効果的に活用する組織の能力を最大限に高めることを指します。これには、デジタル証拠を効率的に収集、保存、分析するためのポリシー、手順、テクノロジーを整備し、インシデントが発生した際に、組織が迅速かつ最小限のコストで対応できるようにすることが含まれます。フォレンジック対応準備は、調査に費やす時間とリソースを削減するだけでなく、証拠の信頼性を確保し、必要に応じて法的手続きで使用できることを保証します。参考文献：フォレンジック対応準備の概念は、インシデントハンドラー（ECIH v3）カリキュラムの一部であり、証拠の保存や効果的かつ効率的な調査を実施する能力など、インシデントに事前に備えることの戦略的重要性を強調しています。

最新問題: **83**
ファイルを開いたときに実行可能プログラムをインストールし、被害者のシステムを他者が制御できるようにする、あらゆる有用なプログラムに偽装した悪意のあるセキュリティ侵害コードは、次のように呼ばれます。
A. ルートキット
B. ワーム
C. ウイルス
D. トロイの木馬
Answer: D (メーッセージを残す)

最新問題: **84**

同僚は、所属する組織が小規模であるため、セキュリティに関する責任を最小限に抑えたいと考えています。彼は、複数の形式で提供されている新しいアプリケーションを評価しています。同僚にとって最も責任が軽減される形式はどれでしょうか？
A. オンプロムインストール
B. saaS
C. IaaS
D. PaaS
Answer: (解答を表示する**)**
SaaS（Software as a Service）は、サービスプロバイダーが基盤となるインフラストラクチャ、ソフトウェアの保守、セキュリティパッチの適用、およびアップデートを管理するため、エンドユーザーや組織のセキュリティ責任を最小限に抑えることができます。SaaSアプリケーションを選択することで、同僚の所属組織は物理サーバー、オペレーティングシステム、またはアプリケーションのセキュリティ構成について責任を負う必要がなくなり、セキュリティ責任を最小限に抑えるための最良の選択肢となります。
参考資料：認定インシデントハンドラー（ECIH v3）コースの教材では、さまざまなクラウドサービスモデル（IaaS、PaaS、SaaS）について、セキュリティ責任と管理への影響に焦点を当てて解説しています。

最新問題: **85**
インシデント対応担当者であるアンドリューは、クライアント組織のリスク評価を実施している。
リスク評価プロセスの一環として、彼はITシステムの境界、およびシステムを構成するリソースと情報を特定した。
アンドリューが実施しているリスク評価の手順を特定してください。
A. 管理に関する推奨事項
B. システム特性評価
C. 制御分析
D. 可能性判定
Answer: B (メーッセージを残す**)**

最新問題: **86**
データ、アプリケーション、その他のリソースをパブリッククラウドまたは専用サービスプロバイダーに復元することを目的とした戦略とサービスの組み合わせを表す用語は、次のうちどれですか？
A. 緩和
B. 分析
C. 根絶
D. クラウドリカバリ
Answer: (解答を表示する**)**

データ、アプリケーション、その他のリソースをパブリッククラウドまたは専用サービスプロバイダーに復元することを目的とした戦略とサービスの組み合わせを表す用語は「クラウドリカバリ」です。この用語は、データ損失、システム障害、または災害が発生した場合に、組織のデジタル資産を迅速かつ効果的にクラウド環境に復元または移行できるようにするための災害復旧活動を包含しています。
クラウド復旧戦略は、より広範な災害復旧および事業継続計画の一部であり、クラウドコンピューティングのスケーラビリティと柔軟性を活用することで、ダウンタイムとデータ損失を最小限に抑えます。緩和、分析、および根絶は、インシデント対応とリスク管理の他の側面に関連する用語であり、クラウド環境へのリソース復旧に特化したものではありません。
参考資料 :インシデントハンドラー（ECIH v3）のカリキュラムには、災害復旧と事業継続計画に関する議論が含まれており、クラウド復旧が組織の混乱に対する回復力を確保するための重要な要素であることを強調しています。

最新問題**: 87**
悪意のあるユーザーのコンピュータ活動やキーボード入力を記録するために使用されるスパイウェアツールは、次のように呼ばれます。
A. ファイアウォール
B. アドウェア
C. キーロガー
D. ルートキット
Answer: C (メーッセージを残す**)**

最新問題**: 88**
ミコはXYZ社にインシデントハンドラーとして採用されました。彼の最初の仕事は、ネットワーク内で発生したPINGスイープ試行を特定することでした。この目的のために、彼はWiresharkを使用してトラフィックを分析しました。ICMP pingスイープ試行を特定するために、彼はどのようなフィルタを使用しましたか？
A. tcp.typec == icmp
B. icrrip.lype == icmp
C. icmp.type == 8 または icmp.type == 0
D. udp.lype - 7
Answer: (解答を表示する**)**
Wiresharkでは、ICMPピングスイープの試みを識別するために、icmp.type == 8またはicmp.type == 0というフィルタを使用します。このフィルタは、ピングコマンドを示すICMPエコー要求とエコー応答をキャプチャします。タイプ8は、送信元がピングを送信したときに使用されるエコー要求を表し、タイプ0は、ターゲットからの応答であるエコー応答を表します。これらのICMPタイプでフィルタリングすることで、Mikoはネットワーク全体でピング要求が急増していることを検出できます。これは、ピングスイープの試みを示している可能性があります。ピングスイープとは、攻撃者が複数のアドレスにピング要求

を送信してネットワーク上のアクティブなホストを発見するためによく使用する探索活動です。
参考資料 :インシデントハンドラー（ECIH v3）コースや学習ガイドには、Wiresharkなどのネットワーク分析ツールの使用方法に関するトレーニングがよく含まれており、特定の種類のネットワークアクティビティや潜在的な脅威を検出するためのフィルタの使用方法も含まれています。

最新問題: **89**
Future Tech Corpは、AIベースの予測システム内にマルウェアを発見した後、事業予測が歪んでいることに気づきました。このマルウェアはデータを改ざんするだけでなく、機械学習機能を備え、その手法を進化させていました。専用のAIセキュリティモジュールとデータベース復元ツールを利用できるようになった今、最初にとるべきステップは何でしょうか？
A. マルウェア侵入前の時点にデータベースを復元します。
B. AIセキュリティモジュールを展開して、進化したマルウェアに対抗し、削除します。
C. AI予測システムを無効にして、一時的に手動予測に頼る。
D. ビジネスパートナーに、予測が歪んでいる可能性があることを知らせる。
Answer: B (メーッセージを残す**)**
このインシデントは、AIシステムに組み込まれた適応型マルウェアによるもので、その動作は積極的に進化しています。ECIHのマルウェアインシデント対応手法では、復旧作業よりも脅威の封じ込めと根絶を優先します。マルウェアを削除せずにデータを復元すると、即座に再感染し、操作が継続されるリスクがあります。
選択肢Bが正解です。AIセキュリティモジュールを導入することで、マルウェアの適応メカニズムを直接的に標的にできるため、対応者はAI環境内の悪意のあるロジックを検出、封じ込め、駆除することができます。ECIHは、インシデントに関わるテクノロジースタックに合わせた、適切なコンテキスト認識型セキュリティ制御の使用を重視しています。AI駆動型環境では、従来の制御では検出できない脅威に対抗するために、専用のツールが必要となります。
オプションAは、根絶前に実施するには時期尚早で危険です。オプションCは、脅威を解決することなく事業運営を混乱させます。オプションDは、封じ込めと検証の後に実施すべきコミュニケーション手順です。
したがって、AIセキュリティモジュールを使用して進化したマルウェアを無力化することが、正しい最初のステップである。

最新問題: **90**
デジタルフォレンジック対応担当者のマイケルは、データ漏洩の疑いがあるサーバー室に入ります。彼は、調査に関係のない全員が退室していることを確認し、デバイスの設定変更を避け、サーバーの電源を切らずにネットワークから切り離します。マイケルの行動の主な目的は何でしょうか？

A. 保管管理記録の作成
B. 揮発性メモリの収集
C. 犯罪現場の確保と評価
D. 影響を受けたサーバーのクローン作成
Answer: (解答を表示する)
マイケルの行動は、ECIHの鑑識準備モジュールにおける基本的な初期対応原則である犯罪現場管理を反映している。現場を確保し、不正アクセスを防止し、システム変更を避けることで、証拠の完全性を保つことができる。
選択肢Cが正解です。なぜなら、彼の主な目的は、証拠収集を開始する前にデジタル犯罪現場を確保し、評価することだからです。ECIHは、現場管理によって汚染、改ざん、偶発的な証拠破壊を防ぐことができると強調しています。
選択肢A、B、Dは後続する可能性はあるものの、当面の目標ではない。

最新問題: **91**
OmegaTechは、競合他社に引き抜かれた内部関係者によって、主力製品に意図的に脆弱性が仕込まれたという被害に遭いました。OmegaTechは今後、このようなリスクを最小限に抑えたいと考えています。
その主な焦点は何であるべきか？
A. 6ヶ月ごとに職務を交代する。
B. サプライズロイヤルティテストを導入する。
C. すべてのソフトウェアリリースに対して厳格な審査プロセスを実施する。
D. 身元調査を強化し、従業員の行動を継続的に監視して異常がないか確認する。
Answer: D (メーッセージを残す)
包括的かつ詳細な説明（ECIH準拠）：
ECIHの内部脅威対策ガイドラインでは、悪意のある内部関係者に対する最も効果的な抑止策として、継続的な監視と行動分析を背景調査と組み合わせることを強調している。
選択肢Dが正解です。なぜなら、内部脅威は採用後に変化することが多いからです。継続的な監視によって、静的な審査では検出できない異常な行動パターンを検出できます。
オプションACは、高度な内部脅威に対して不十分または効果がない。

最新問題: **92**

以下のリスク軽減戦略のうち、リスク要因を低減して許容可能なレベルにするための対策を実行するもの、または潜在的なリスクを受け入れてITシステムの運用を継続するものはどれですか？
A. リスク想定
B. リスク移転
C. リスク計画
D. リスク回避
Answer: A (メーッセージを残す**)**

最新問題: **93**
イヴはABC社のインシデントハンドラーです。ある日、彼女は社内従業員の一人からメールハッキング事件に関する苦情を受けました。インシデント対応プロセスの一環として、彼女は業務継続性を維持するために、インシデントの影響から復旧するための多くの復旧手順に従わなければなりません。
彼女が従業員アカウントを安全に保護するために最初に行うべき手順は何ですか？
A. メールサービスを復元し、パスワードを変更してください。
B. 二段階認証を有効にする
C. すべてのメール内のリンクと添付ファイルのスキャンを有効にする
D. システム間の自動ファイル共有を無効にする
Answer: A (メーッセージを残す**)**
メールのハッキング事件発生後、従業員のアカウントを保護するための最初のステップは、必要に応じてメールサービスへのアクセスを復元し、不正アクセスを防ぐためにパスワードを直ちに変更することです。
この措置により、攻撃者がアカウントからできるだけ早く締め出されることが保証されます。二段階認証の有効化、リンクや添付ファイルのスキャン、自動ファイル共有の無効化は重要なセキュリティ対策ですが、これらは、侵害されたアカウントのパスワードを変更して不正アクセスを阻止し、アカウントを安全に保護した後に実施されるものです。
参考資料 :ECIH v3認定資料では、アカウント侵害に関するインシデントに対応する際に取るべき初期手順について説明しており、アカウントをさらなる不正アクセスから保護するためにパスワードを迅速に変更することの重要性を強調しています。

最新問題: **94**
ハッカーが組織を攻撃する他の方法を見つけられない場合、従業員や不満を抱えたスタッフに影響を与える可能性がある。
これはどのような脅威ですか？
A. 内部犯行
B. 足跡
C. t を識別する
D. フィッシング攻撃
Answer: A (メーッセージを残す**)**

最新問題: **95**
プラットフォーム・アズ・ア・サービス（PaaS）クラウドモデルを活用している地域医療機関が、患者記録への不正アクセスを含む不審な活動を検知した。調査中、インシデント対応チームは、侵害時に使用された仮想マシンからシステムログを取得しようと試みた。しかし、短時間しか稼働しなかったインスタンスが事件直後に自動的に終了したため、重要なログファイルが入手できないことが判明した。このため、完全な活動履歴を再構築し、攻撃者の動きを追跡することが困難になった。
この状況は、クラウドフォレンジックにおけるどの主要な課題を最も反映している可能性が高いでしょうか？
A. コンテナ化されたワークロードからのログアクセスが制限されます。
B. ログ正規化の不整合に起因するメタデータの不整合。
C. 揮発性物質の保管による丸太の蒸発。
D. 鍵管理の不備によりログ暗号化が妨げられる。
Answer: C (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
このシナリオは、ログの消失として知られるクラウドフォレンジックの課題を示しています。ログの消失とは、ログが揮発性または短命な環境に保存され、インスタンスが終了すると失われる現象です。ECIHクラウドセキュリティモジュールは、これをクラウド調査における主要な障害として強調しています。
選択肢Cが正解です。PaaSインスタンスの自動終了により重要なログが失われ、攻撃者の活動を再現することができなくなったためです。
オプションA、B、Dは、ここで取り上げていない異なるログ記録の問題について説明しています。
ECIHは、ログの消失を防ぐために、集中管理された永続的なログ記録の重要性を強調しています。このシナリオは、そのような制御を実装しなかった場合の結果を直接的に反映しているため、オプションCが正解となります。

最新問題: **96**
インシデント復旧手順の有効性を判断するために実施されるテストはどれですか？
A. 施設レベルの検査
B. 手順のライブウォークスルー
C. 学科レベルのテスト
D. シナリオテスト
Answer: B (メーッセージを残す**)**

最新問題: **97**
ジェームズはインシデント対応・対応（IH&R）チームのリーダーに任命され、社内の自身のチームと共にIH&R計画を策定するよう指示された。

ジェームズが現在取り組んでいるIH&Rプロセスのステップを特定してください。
A. 根絶
B. 回復
C. 準備
D. 通知
Answer: C (メーッセージを残す)
インシデント対応（IH&R）において、準備フェーズは、潜在的なセキュリティインシデントに効果的に対応できるよう、チームとリソースを編成する最初のステップです。このフェーズでは、IH&Rチームの構築、インシデント対応計画とポリシーの策定、コミュニケーションチャネルの設定、そしてチームが必要なツールと権限を持っていることの確認を行います。IH&R計画の策定とチームの編成を担当するジェームズは、インシデント対応プロセスの準備フェーズに取り組んでいます。この基礎となるステップは、インシデント発生時に連携のとれた効率的な対応を確保するために不可欠です。
参考文献 :インシデント対応ライフサイクルにおける準備段階の重要性は、さまざまなサイバーセキュリティフレームワークやガイドラインで強調されており、ECIH v3認証資料で取り上げられているものもその一つです。これらの資料では、効果的なインシデント対応能力を確立するために必要な役割、責任、計画が詳細に説明されています。

最新問題: **98**
正規ユーザーがネットワーク、システム、またはアプリケーションにアクセスできないようにするタイプの攻撃。
ネットワークリソースを枯渇させ、アプリケーションに不正なリクエストを送信する行為は、次のように呼ばれます。
A. 中間攻撃
B. サービス拒否攻撃
C. セッションハイジャック攻撃
D. SQLインジェクション攻撃
Answer: B (メーッセージを残す)

最新問題: **99**
チャンドラーは、Technote 組織を標的とするプロのハッカーです。彼は、異なる階層間でやり取りされている重要な組織情報を入手したいと考えています。その過程で、彼はネットワークを介して送信されるデータパケットを傍受し、ネットワーク、ポート、プロトコル、デバイス、ネットワーク伝送の問題、その他のネットワーク仕様などのパケットの詳細を収集するために分析します。チャンドラーがパケット分析を実行するために使用する必要があるツールは次のうちどれですか？
A. IDAPro
B. オムニピーク
C. シャープ
D. ビーフ

Answer: B (メーッセージを残す)

最新問題: **100**
オーティスはデルモント社でインシデント対応担当者として働いている。最近、同社は事業上の問題に直面し、収益が減少している。オーティスは事態の調査を任された。企業セキュリティの監査を行った結果、企業ネットワークから機密情報が盗まれ、競合他社に渡された攻撃の痕跡を発見した。
デルモント社が直面した情報セキュリティインシデントは次のうちどれですか？
A. 不正アクセス
B. スパイ活動
C. メールによる嫌がらせ
D. ネットワークとリソースの乱用
Answer: B (メーッセージを残す)

最新問題: **101**
攻撃者が曖昧な言葉遣いを用いてメッセージを理解しにくくするために用いる手法として、次のうちどれが挙げられますか？
A. ステガノグラフィー
B. なりすまし
C. 暗号化
D. 難読化
Answer: D (メーッセージを残す)
難読化とは、データやコードを理解しにくくするために使用される手法です。攻撃者は、コードや通信の真の意図を隠蔽するために難読化を用いることが多く、セキュリティ専門家や自動化ツールなどが悪意のある活動を分析・検出することを困難にします。難読化には、曖昧な表現や誤解を招く表現の使用に加え、エンコード、暗号化、ソースコード内の意味不明な変数名の使用など、より技術的な手法を用いて、コードの真の機能を隠蔽する方法があります。
参考文献：ECIH v3 プログラムでは、難読化など、攻撃者が検出を回避するために使用するさまざまなテクニックについて説明し、それが悪意のあるペイロードの分析と理解をいかに複雑にするかを強調しています。

最新問題: **102**
情報セキュリティ管理システム（ISMS）の導入、実装、または維持を行う組織に対し、情報セキュリティ対策の実装に関する推奨事項を提供する標準的なフレームワークは、次のうちどれですか？
A. ISO/IEC 27002
B. ISO/IEC 27035
C. PCI DSS
D. RFC 219G

Answer: A (メーッセージを残す)
ISO/IEC 27002は、情報セキュリティ管理システム（ISMS）の導入、実装、または維持を担当する者が使用する情報セキュリティ管理に関するベストプラクティス推奨事項を提供する規格です。リスク評価、人的資源セキュリティ、運用セキュリティ、通信セキュリティなどの分野を網羅し、ISMSの確立、実装、運用、監視、レビュー、維持、および改善のためのフレームワークを提供します。ISO/IEC 27035は情報セキュリティインシデント管理に関する規格であり、PCI DSS（Payment Card Industry Data Security Standard）はカード所有者データのセキュリティに関する規格であり、RFC 2196はコンピュータセキュリティインシデント対応チーム（CSIRT）向けのガイドであり、ISMSを実装するための規格ではありません。
参考文献：ECIH v3カリキュラムには、情報セキュリティ管理とガバナンスをサポートするさまざまな標準とフレームワークの研究が含まれており、ISO/IEC 27002もその一つです。これは、組織が効果的なセキュリティ制御を実装する際の指針となる役割を強調しています。

最新問題: **103**
内部脅威対応計画は、組織が悪意のある内部者によって引き起こされる損害を最小限に抑えるのに役立ちます。これらの脅威を軽減するためのアプローチの1つは、人事部による管理体制の構築です。人事部は、次のうちどのガイドラインを利用できますか？
A. 組織の物理的環境を監視し、安全を確保する。
B. バックアッププロセスと物理メディアを保護するために、個人間のルールを導入します。
C. ユーザーに付与されたアクセス権限は文書化され、監督者によって審査される必要があります。
D. 責任の所在を明確にするため、デフォルトの管理者アカウントを無効にします。
Answer: C (メーッセージを残す)

最新問題: **104**
アダムは、金銭的利益を目的として、チームと共に標的組織に対して複数の攻撃を仕掛けた攻撃者である。逮捕されることを恐れた彼は、身元を偽装することを決意した。そのため、彼は複数の被害者から情報を入手し、新たな身元を作り上げた。
アダムが行った個人情報窃盗の種類を特定してください。
A. ソーシャルアイデンティティの盗難
B. 医療情報窃盗
C. 合成身元窃盗
D. 税金関連の個人情報盗難
Answer: C (メーッセージを残す)

最新問題: **105**

次のインシデント復旧テスト方法のうち、火災などの模擬災害を起こして原因を特定する方法はどれですか？
こうした状況に対処するために実施される手順に対する反応は？
A. 設備検査
B. ライブウォークスルーテスト
C. 手順テスト
D. シナリオテスト
Answer: C (メーッセージを残す**)**

最新問題**: 106**
NITSによると、クラウドコンピューティングにおける主要な5つのプレーヤーは何ですか？
A. プロバイダー、キャリア、監査人、ブローカー、販売者
B. 消費者、プロバイダー、キャリア、監査人、ブローカー
C. 購入者、消費者、運送業者、監査人、およびブローカー
D. これらのどれでもない
Answer: B (メーッセージを残す**)**
クラウドコンピューティングの標準規格とガイドラインの主要な情報源である米国国立標準技術研究所（NIST）によると、クラウドコンピューティングにおける主要な5つの主体は、消費者、プロバイダー、キャリア、監査者、ブローカーです。これらの役割は次のように定義されています。
* 消費者 :クラウドコンピューティングサービスを利用する個人または組織。
* プロバイダー：消費者にクラウドサービスを提供する事業体。
* キャリア :クラウドプロバイダーと消費者に接続サービスと伝送サービスを提供する組織。
* 監査人 :クラウドサービス、セキュリティ管理、および運用を評価および検証する独立した機関。
* ブローカー :クラウドサービスの利用、パフォーマンス、および提供を管理し、クラウドプロバイダーと消費者の間の関係を交渉する主体。
これらの関係者はクラウドコンピューティングのエコシステムにおいて重要な役割を果たし、サービスが安全かつ効率的、効果的に提供および使用されることを保証します。参考資料 :NISTのクラウドコンピューティングに関するドキュメント（NISTクラウドコンピューティング標準ロードマップ、NISTクラウドコンピューティング参照アーキテクチャなど）では、これらの役割とクラウドコンピューティングフレームワークにおけるその重要性について詳しく説明しています。

最新問題: **107**
著名なIT企業であるZaimasoft社は、ハードウェアを直接標的とした攻撃を受け、ハードウェアに修復不可能な損傷を被りました。結果として、ハードウェアの交換または再インストールが唯一の解決策となりました。Zaimasoft社に対して行われたサービス拒否攻撃の種類を特定してください。
A. DDoS
B. PDoS
C. DRDoS
D. DoS
Answer: (解答を表示する**)**

最新問題: **108**
次のうち、クラウドアプリケーションをハッキングの危険にさらさないものはどれですか？
A. 設定エラー
B. クラウドサービスベンダーとの契約
C. 不適切な技術的問題
D. クラウドシステムの操作経験不足
Answer: (解答を表示する**)**

最新問題: **109**
ジェームズはCyberSol Inc.でインシデント対応担当者として働いている。経営陣はジェームズに、最近社内で発生したサイバーセキュリティインシデントの調査を指示した。調査の一環として、ジェームズはWindowsオペレーティングシステム上で稼働するシステムから揮発性情報の収集を開始した。
次のコマンドのうち、ジェームズが実行中のプロセスに必要なすべての実行可能ファイルを特定するのに役立つものはどれですか？
A. カテゴリーA &. 時間 、/t
B. netstat -ab
C. トップ
D. ドスキー/歴史
Answer: B (メーッセージを残す**)**
netstat -ab コマンドは、Windows オペレーティングシステムにおいて、すべての接続とリスニングポート、および各接続またはリスニングポートの作成に関与する実行可能ファイルを表示するのに便利です。これは、James のようなインシデント対応担当者が、システム

上でどのプロセスが実行されているか、またそれらがネットワーク上でどのように通信しているかを特定しようとする際に特に役立ちます。この情報は、悪意のあるプロセス、不正な接続、またはシステム上のその他の侵害の兆候を特定するのに役立ちます。netstat -ab は実行中のプロセスの実行可能ファイルだけを一覧表示するわけではありませんが、プロセスとネットワークアクティビティを関連付けます。これは、サイバーセキュリティインシデント調査中に不安定な情報を収集する上で重要な要素です。
参考資料 :EC-Council の認定インシデントハンドラー (ECIH v3) コースでは、インシデント対応活動の一環としてシステムから揮発性データを収集するために使用できるさまざまなコマンドとツールについて説明し、ネットワーク接続とそれらに関係するプロセスを理解することの重要性を強調しています。

最新問題: **110**
プログラムの実行中に広告バナーを表示するソフトウェアアプリケーション。
コンピュータ画面やブラウザに表示されるポップアップウィンドウやバーを表示する広告は、次のように呼ばれます。
A. ワーム
B. トロイの木馬
C. ルートキット
D. ウイルス
E. アドウェア（すべて小文字）
Answer: (解答を表示する**)**

最新問題: **111**
リスク軽減戦略とは、リスクを最小限に抑え、克服するためにどのような状況下で行動を起こす必要があるかを決定するものです。システムの脆弱性と適切な対策を探索することで、リスクと損失の発生確率を最小限に抑えることに焦点を当てたリスク軽減戦略を特定してください。
A. リスク制限
B. リスク想定
C. 研究と謝辞
D. リスク吸収
Answer: C (メーッセージを残す**)**

最新問題: **112**
システムからマルウェアが削除され、クリーンなスキャン結果が出た後、影響を受けたデバイスに対して以下のどの手順を実行すべきですか？
A. イメージを刷新すべきです
B. 箱に密封して90日間保管してください。
C. 更新情報を取得するために、イーサネット経由でドメインコントローラに接続する必要があります。

D. 本番環境に導入する前に、マルウェアが除去されていることを確認するために、監視環境に置いてレビューを行う必要があります。
Answer: D (メーッセージを残す)

最新問題: **113**
ネットワークセキュリティアナリストのローガンは、社内サブネット内の広範囲のIPアドレスに対して、ICMPエコー要求が繰り返し送信されているパターンに気づいた。偵察活動の可能性を疑うローガンは、Wiresharkを起動し、異常なスキャン動作がないかトラフィックの分析を開始した。
攻撃者はどのような手法を用いている可能性が最も高いですか？
A. DNSポイズニング
B. ピングスイープ
C. ポートスキャン
D. SYNフラッディング
Answer: B (メーッセージを残す)
包括的かつ詳細な説明（ECIH準拠）：
今回説明した活動（多数のIPアドレスに対してICMPエコー要求を順次送信する）は、ネットワーク上の稼働中のホストを特定するために使用される偵察手法である、典型的なピングスイープです。ECIHのネットワークインシデント対応では、偵察は攻撃の初期段階の活動であり、多くの場合、悪用につながると認識されています。
正解はBです。なぜなら、ピングスキャンはICMPエコー要求を使用して応答するホストを特定し、攻撃者がネットワークをマッピングできるようにするからです。これは観測されたトラフィックと完全に一致します。
オプションAはDNS操作を伴う。オプションCはICMPではなくTCP/UDPポートのプローブを伴う。オプションDは偵察ではなく、サービス拒否攻撃の手法を説明する。
偵察活動を早期に認識することで、防御側は悪用される前に対策を講じることができ、ECIHの検出および防止に関する指針に沿った対応が可能となる。

最新問題: **114**
CSIRTが提供するサービスは次のうちどれですか？
A. セキュリティツールの開発
B. テクノロジーウォッチ
C. 脆弱性への対応
D. 上記すべて
Answer: D (メーッセージを残す)

最新問題: **115**
アリスはインシデントハンドラーであり、上司から、インシデント対応プロセス中にデータが破損した場合に復元できるよう、影響を受けたシステムのデータをバックアップする必要があると伝えられています。また、システムのバックアップは、インシデントのさらな

る調査にも使用できるとも伝えられています。アリスは、インシデント処理および対応（IH&R）プロセスの次のどの段階で、感染したシステムの完全なバックアップを行う必要がありますか？
A. 封じ込め
B. 事件記録
C. インシデントトリアージ
D. 根絶
Answer: A (メーッセージを残す**)**
インシデント処理および対応（IH&R）プロセスにおいて、影響を受けたシステムのデータをバックアップすることは、通常、封じ込めフェーズに含まれる重要なステップです。封じ込めフェーズは、インシデントの範囲と深刻度を制限し、インシデントがさらに拡大したり、他のシステムに影響を与えたりしないようにするために不可欠です。封じ込めフェーズ中に影響を受けたシステムをバックアップすることは、いくつかの理由から不可欠です。
フォレンジック分析のためにシステムの現在の状態のスナップショットを保存し、対応プロセス中にシステムを消去または変更する必要がある場合にデータが失われないようにし、データが破損または失われた場合の復旧プロセスを支援します。
封じ込めフェーズ中に感染システムの完全なバックアップを実行することで、Aliceは、駆除やより詳細なフォレンジック分析といった主要な措置を講じる前に、すべてのデータとシステム状態の信頼できるコピーが確実に存在するようにします。この手順は、インシデントの発生状況の分析や、インシデント解決後のシステム機能の復旧において、バックアップを将来的に活用するための準備でもあります。
参考資料：EC-Councilの認定インシデントハンドラー（ECIH v3）コースと学習ガイドでは、IH&Rプロセスにおける封じ込めフェーズの重要性が強調されており、データ損失を防ぎ、調査と復旧プロセスを支援するために影響を受けたシステムをバックアップする実践も含まれています。

最新問題: **116**
スミス氏は、オーストラリアに数店舗の支店を持つ小規模金融機関の主任インシデント対応担当者です。最近、同社は銀行間システムを通じて500万米ドルの損失を被る大規模な攻撃を受けました。事件の詳細な調査の結果、6か月前に攻撃者が軽微な脆弱性を利用してネットワークに侵入し、ユーザーに気づかれることなくアクセスを維持していたことが原因であることが判明しました。その後、攻撃者はユーザーの指紋を削除しようとし、銀行間システムで権限を持つ人物のコンピュータに横方向の移動を実行しました。
最終的に、攻撃者はアクセス権を取得し、不正な取引を行った。
上記のシナリオに基づいて、最も正確な攻撃の種類を特定してください。
A. フィッシング
B. ランサムウェア攻撃
C. サービス拒否攻撃
D. APT攻撃
Answer: (解答を表示する**)**

最新問題: **117**
マットは、マルウェアの被害を受けた大手ソーシャルネットワーク企業のインシデント対応担当者です。同社の報告期限に関するガイドラインによると、マルウェアの感染は、社内に拡散した後、発見・検出から1時間以内に報告する必要があります。
この事件はどのカテゴリーに属しますか？
A. CAT 1
B. CAT 4
C. CAT 2
D. CAT 3
Answer: D (メーッセージを残す**)**

最新問題: **118**
以下の鑑識捜査段階のうち、最初に実施すべき段階はどれですか？
A. 予備的な証拠を収集する。
B. 証拠の2ビットストリームコピーを作成します。
C. 応急処置を実施してください。
D. 証拠品を鑑識研究所へ搬送する。
Answer: C (メーッセージを残す**)**

最新問題: **119**
次のうち、常時電源供給が必要で、電源供給が中断されると削除されるデジタル機器に一時的に保存されるデジタル証拠はどれですか？
A. スワップファイル
B. イベントログ
C. スラックスペース
D. プロセスメモリ
Answer: D (メーッセージを残す**)**
プロセス メモリ、または揮発性メモリ (RAM) は、データを保持するために常時電源供給が必要であり、電源供給が中断されると削除または失われるデジタル証拠です。これには、システムの進行中のプロセスと操作に関する情報が含まれています。この種の証拠は、インシデント発生時のユーザー操作、システム イベント、アプリケーションとサービスの状態に関する情報が含まれている可能性があるため、フォレンジック調査にとって非常に重要になることがあります。常時電源供給なしで情報を保持できるスワップ ファイル、イベント ログ、スラック スペースとは異なり、プロセス メモリは本質的に揮発性であり、デバイスの電源がオフになったり再起動したりすると内容が失われます。参考資料: ECIH v3 認証プログラムには、インシデント対応と調査のコンテキストにおける、揮発性メモリと不揮発性メモリを含むさまざまな種類のデジタル証拠の重要性とデジタル フォレンジックに関する議論が含まれています。

最新問題: **120**
Ikeo Corp. は、企業セキュリティを評価するためにインシデント対応チームを雇用しました。インシデント処理および対応プロセスの一環として、IR チームは企業が現在実施しているセキュリティ ポリシーをレビューしています。IR チームは、組織の従業員がインターネット アクセスに制限を受けていないことを発見しました。つまり、従業員は任意のサイトにアクセスしたり、任意のアプリケーションをダウンロードしたり、リモートの場所からコンピュータやネットワークにアクセスしたりすることが許可されています。IR チームはこれを主要なセキュリティ 脅威とみなし、攻撃者によって容易に悪用される可能性があるため、このポリシーを変更することを計画しています。IR チームが変更を計画しているセキュリティ ポリシーを特定してください。
A. 乱交的なポリシー
B. 偏執的な方針
C. 寛容な方針
D. 慎重な方針
Answer: A (メーッセージを残す**)**

最新問題: **121**
ウェブサーバーの内容を変更すること、偽のIDを使用してワークステーションにアクセスすること、許可なく機密データをコピーすることは、以下の例です。
A. マルウェア攻撃
B. DDoS攻撃
C. ソーシャルエンジニアリング攻撃
D. 不正アクセス攻撃
Answer: D (メーッセージを残す**)**

最新問題: **122**
監査証跡ポリシーは、オペレーティングシステム、アプリケーション、またはユーザーアクティビティに関する一連のコンピュータイベントの記録など、すべての監査証跡を収集します。監査証跡ポリシーに関して、次の記述のうち正しくないものはどれですか。
A. インシデントによる組織の無形損失の計算に役立ちます
B. 個々の行動を追跡し、ユーザーが自身の行動に責任を持つことを可能にします。

C. さまざまな規制法、規則、ガイドラインへの準拠に役立ちます
D. 問題発生後の出来事を再構築するのに役立ちます
Answer: (解答を表示する**)**

最新問題**: 123**
インシデント対応担当者であるエリックは、インシデント対応計画と手順の策定に取り組んでいます。このプロセスの一環として、彼は組織ネットワークの分析を行い、レポートを作成するとともに、得られた結果に基づいてポリシーを策定しています。
ネットワークとその関連トラフィックを分析する際に、彼が役立つツールは次のうちどれですか？
A. Wireshark
B. FaceNiff
C. Burp Suite
D. Whois
Answer: A (メッセージを残す**)**

最新問題**: 124**
一見無害なプログラムを装い、攻撃者にユーザーの情報やシステムへの無制限のアクセス権限を与える悪意のあるプログラムを特定してください。これらのプログラムは、ユーザーのディスクを消去したり、被害者のクレジットカード番号やパスワードを第三者に送信したりする危険なプログラムを実行する可能性があります。
A. ワーム
B. アドウェア
C. ウイルス
D. トロイの木馬
Answer: D (メッセージを残す**)**
トロイの木馬（トロイの木馬）は、正規の無害なプログラムやファイルに偽装してユーザーを騙し、ダウンロードやインストールを促すマルウェアの一種です。一度起動すると、トロイの木馬は感染したシステムへの不正アクセスなど、さまざまな悪質な活動を実行します。これにより、クレジットカード番号やパスワードなどの機密情報が盗まれるだけでなく、攻撃者がさらにマルウェアをインストールし、データの消去など、さらなる被害を引き起こす可能性があります。ウイルスやワームとは異なり、トロイの木馬は自己複製せず、ユーザーを欺くことで拡散します。
参考資料 :インシデントハンドラー（ECIH v3）コースの教材では、トロイの木馬を含む様々な種類のマルウェアとその特性について解説しています。カリキュラムでは、様々な種類の悪意のあるソフトウェアがどのように動作するかを理解することの重要性を強調し、そのような脅威に関連するセキュリティインシデントを効果的に管理し、対応できるようにしています。

最新問題**: 125**

次のうち、揮発性データと呼ばれないものはどれですか？
A. ソケットまたはポートを開放する
B. システムのライムがないデール
C. ファイルの作成日
D. ネットワークインターフェースの状態
Answer: C (メーッセージを残す**)**
揮発性データとは、一時的に保存され、コンピュータの電源を切ったり再起動したりすると失われる情報のことです。例えば、RAMの内容（開いているソケットやポートを含む）、システムの日時、ネットワークインターフェースの状態などが挙げられます。ただし、ファイルの作成日は、ハードドライブに保存され、システムの再起動や電源オフ後も利用できるため、不揮発性データとみなされます。
不揮発性データは、ハードディスクドライブ、SSD、磁気テープなどの永続的な記憶媒体に保存され、削除または上書きされるまでそこに保持されます。
参考資料:インシデントハンドラー（ECIH v3）認定では、デジタルフォレンジックとインシデント対応の文脈における揮発性データと非揮発性データの区別を強調し、システムシャットダウン時に失われる可能性のあるデータと残存するデータを理解することの重要性を強調しています。

最新問題**: 126**
ある国立研究機関が最近、包括的なサイバーセキュリティコンプライアンス監査を受けた。
監査において、審査員は、調査中に機関のインシデント対応部門が有害なコードサンプルをどのように管理しているかを評価した。評価の結果、チームメンバーが、一般業務で使用されるエンタープライズ接続システム上で、危険なファイルペイロードに直接アクセスしているケースが頻繁に発生していることが明らかになった。さらに、偶発的なトリガーを防ぐための予防的なファイル名変更は行われておらず、機密資料は専門知識を持たない職員がアクセスできる場所に置かれていた。監査員は、これらの慣行が安全なサンプル処理プロトコルに著しく違反していると指摘し、業務への影響や偶発的な発生を防ぐために早急な改善を勧告した。
この事例において、悪意のあるコードを安全に取り扱うためのベストプラクティスのうち、どれが最も明確に無視されていたか？
A. マルウェアのサンプルを非実行可能ファイル拡張子で隔離された環境に保存する。
B. 対称暗号化を使用してすべてのマルウェアサンプルファイルを暗号化します。
C. 脅威プロファイリングとアーカイブをサポートするために、各マルウェアサンプルの脆弱性ドキュメントを作成します。
D. マルウェアのサンプルファイルにプラットフォーム固有の動作指標をタグ付けして、分類を改善します。
Answer: (解答を表示する**)**
包括的かつ詳細な説明（ECIH準拠）：

このシナリオは、フォレンジック対応と安全なマルウェア処理に関する違反を浮き彫りにしています。これらは、ECIHの「ファーストレスポンス」および「マルウェア分析」モジュールで明確に説明されています。ECIHは、マルウェアサンプルを本番環境や企業ネットワークに接続されたシステムで処理してはならないことを強調しています。これは、誤実行、横方向感染、組織への影響といった重大なリスクを生み出すためです。
選択肢Aが正解です。ECIHでは、悪意のあるコードサンプルは隔離された非ネットワーク環境に保存し、誤って実行されるのを防ぐために、実行不可能な拡張子（例.malware、.bin、.txt）を付けて名前を変更することが義務付けられています。この手順により、運用上の安全性が確保され、フォレンジックの完全性が維持されます。
オプションBは機密性を向上させますが、偶発的な実行を防ぐことはできません。オプションCは文書化を支援しますが、実行リスクを軽減するものではありません。オプションDは分類を支援しますが、安全な取り扱いについては対応していません。
企業システム上でマルウェアを隔離や名前変更せずに処理するという、前述の動作は、ECIHのベストプラクティスに真っ向から反します。調査中に二次的なインシデントを防ぐためには、適切なサンプルの隔離、名前変更、およびアクセス制限が必須の対策であり、したがってオプションAが正解です。

最新問題: **127**
インシデント処理および対応（IH&R）プロセスの以下のどの段階で、特定されたセキュリティインシデントの分析、検証、分類、および優先順位付けが行われますか？
A. 事件の記録と割り当て
B. 封じ込め
C. 通知
D. インシデントトリアージ
Answer: (解答を表示する**)**
インシデントトリアージとは、インシデント処理および対応プロセスにおいて、特定されたセキュリティインシデントを分析、検証、分類、優先順位付けする段階です。このステップは、インシデントの深刻度を判断し、効果的な対応のためのリソース配分を決定する上で非常に重要です。インシデントの性質、影響、緊急性を理解するための初期分析が行われ、その後の対応策の指針となります。
参考文献 :インシデントトリアージフェーズは、ECIH v3カリキュラムの基礎概念であり、セキュリティインシデントへの対応における構造化されたアプローチの重要性を強調し、リソースが最も必要とされる場所に集中することを保証します。

最新問題: **128**
内部脅威は、内部関係者が示す懸念すべき行動、例えば、
上司や同僚、業績の低下、遅刻、または説明のつかない欠勤。
内部脅威の検出に役立つ技術：
A. 疑わしい行動や悪意のある行動の既知のパターンを関連付ける

B. 適切な制御を実装してコンピュータシステムを保護する
C. 従業員に秘密保持契約書への署名を義務付ける
D. 情報の機密性とアクセス権限に基づいて情報を分類する
Answer: A (メーッセージを残す**)**
説明

最新問題**: 129**
従業員監視ツールは、主に雇用主が以下のどれを見つけるために使用しますか？
A. レジストリキーが失われた
B. 陰謀
C. 悪意のある内部脅威
D. 盗まれた認証情報
Answer: C (メーッセージを残す**)**
従業員監視ツールは、主に雇用主が悪意のある内部脅威を検知 -防止するために使用されます。
これらのツールは、データアクセス、データ漏洩の試み、不正な操作、その他悪意を示唆したり組織のセキュリティにリスクをもたらす可能性のある行動など、様々な活動を追跡できます。こうしたツールは、レジストリキーの紛失、陰謀、認証情報の盗難といった問題を偶然発見することもあります。しかし、その主な目的は、組織に損害を与えたり、データを盗んだり、システムを妨害したり、スパイ行為を行ったりするためにアクセス権を悪用する可能性のある内部関係者から組織を守ることです。
参考資料 :ECIH v3の学習資料では、組織が内部脅威から保護するために使用できるさまざまなセキュリティ対策とツールについて説明しており、内部者による悪意のある活動を検出して対応する上での監視の役割を強調しています。

最新問題**: 130**
インサイダーは企業の業務機能を理解している。インサイダーが会社の資産を損害するために行う正しい一連の行動は何か？
A. 特権アクセス権を取得し、マルウェアを有効化してインストールする
B. マルウェアをインストールし、特権アクセスを取得してから、アクティベートする
C. 特権アクセスを取得し、マルウェアをインストールして有効化する
D. マルウェアをアクティブ化し、特権アクセスを取得してからマルウェアをインストールする
Answer: C (メーッセージを残す**)**

最新問題**: 131**
イケオ株式会社は、企業セキュリティを評価するためにインシデント対応チームを編成しました。インシデント対応プロセスの一環として、インシデント対応チームは企業が現在実施しているセキュリティポリシーを検証しています。

IRチームの調査によると、当該組織の従業員はインターネットへのアクセスに関して何の制限も受けておらず、あらゆるサイトにアクセスしたり、あらゆるアプリケーションをダウンロードしたり、遠隔地からコンピュータやネットワークにアクセスしたりすることが許可されていることが判明した。
これを主なセキュリティ上の脅威とみなし、IRチームはこのポリシーが攻撃者によって容易に悪用される可能性があるため、変更を計画しています。IRチームが変更を計画しているセキュリティポリシーは次のうちどれですか？
A. 偏執的な政策
B. 慎重な方針
C. 乱交ポリシー
D. 寛容な方針
Answer: (解答を表示する**)**
寛容なセキュリティポリシーとは、従業員がインターネットアクセス、アプリケーションのダウンロード、リモートアクセス機能に関して幅広い自由度を持つポリシーのことです。本稿で述べたシナリオでは、インシデント対応チームが、制限の欠如が攻撃者に悪用される可能性のある重大なセキュリティ上の脅威であると認識し、現在のポリシーが寛容であると判断しました。このポリシーを変更するには、アクセス可能なサイト、ダウンロード可能なアプリケーション、リモートアクセスの許可方法などについて、より厳格な制御を導入し、より管理された安全な環境へと移行する必要があります。このアプローチは、それぞれに特徴とサイバーセキュリティフレームワークにおける適用方法を持つ、偏執的、慎重、無秩序なポリシーとは対照的です。
参考資料 :ECIH v3 認証資料では、組織のセキュリティ態勢という文脈でセキュリティ ポリシーについて議論することが多く、さまざまな制限の度合いがセキュリティとリスクにどのように影響するかを強調しています。

最新問題**: 132**
グローバル企業のサイバーセキュリティ対応チームは、上級幹部からのメールと思われる不審なメールについて、従業員から警告を受けました。調査の結果、チームはメールヘッダーを分析し、送信元のIPアドレスが組織とは一切関係のない外国のものであることに気づきました。WHOIS検索の結果、そのIPアドレスは不明な組織に登録されていることが確認されました。不審な活動を特定する上で、どのような重要な要素が役立ったでしょうか？
A. 反発分析
B. スパムフィルターのログ
C. DKIM認証
D. 発信元IPトレース
Answer: D (メーッセージを残す**)**
ECIHのメールセキュリティインシデント対応モジュールでは、なりすましメールや悪意のあるメールを特定するための主要な方法として、メールヘッダーの分析を重視しています。最も重要なヘッダー要素の一つは送信元IPアドレスであり、これによりメールの実際の送信元が明らかになります。

選択肢Dが正解です。発信元IPアドレスを追跡し、WHOISで検証することで、そのメールが正規の組織からのものではないという明確な証拠が得られました。この手法により、担当者は正規の役員からの連絡となりすましを区別することができます。
オプションAは事後対応型で信頼性に欠ける。オプションBは検出コンテキストを提供するが、原因特定はできない。オプションCはドメイン認証を検証するが、認証情報が漏洩した場合になりすましを必ずしも明らかにするとは限らない。
ECIHは、IPアドレス追跡とWHOIS分析を組み合わせることは、役員なりすまし捜査において強力な検証方法であると強調しており、選択肢Dが正解である。

最新問題: **133**
IDSとIPSを回避するために使用された方法は次のうちどれですか？
A. SNMP
B. HTTP
C. 断片化
D. TNP
Answer: C (メーッセージを残す**)**

最新問題: **134**
ジョンはプロのハッカーで、標的組織に対して攻撃を仕掛けています。彼は、IPアドレスと標的サーバー間の接続をリダイレクトすることで、ユーザーがインターネットアドレスを入力すると、元のウェブサイトに酷似した偽のウェブサイトにリダイレクトされるようにしようとしています。彼はキャッシュポイズニングの手法を用いてこの攻撃を試みています。ジョンが標的組織に対して行っている攻撃の種類を特定してください。
A. 戦争運転
B. ファーミング
C. スキミング
D. 言い訳
Answer: B (メーッセージを残す**)**
ファーミングは、ウェブサイトのトラフィックを別の偽のウェブサイトにリダイレクトすることを目的としたサイバー攻撃です。DNSサーバーのキャッシュを汚染することで、攻撃者はユーザーが意図したサイトから悪意のあるサイトにリダイレクトできます。これは、ユーザーが知らないうちに、またはユーザーが不正なリンクをクリックするなどの操作を行うことなく行われます。この手法は、ブラウザに正しいURLを入力したにもかかわらずリダイレクトされてしまう善意のユーザーにも影響を与える可能性があるため、特に悪質です。ウォードライビングは、走行中の車両から無線ネットワークを検索するもので、スキミングは、ATMやPOS端末に設置された装置を使用してクレジットカード情報を盗むもので、プリテキスティングは、攻撃者が特権データを取得するために嘘をつくソーシャルエンジニアリングの一種です。

参考資料 :インシデントハンドラー（ECIH v3）認定プログラムでは、DNSポイズニングやファーミングなど、さまざまなサイバー攻撃とテクニックを取り上げ、攻撃者が脆弱性を悪用してユーザーを不正なサイトにリダイレクトする方法を説明しています。

最新問題: **135**
世界的な環境研究機関であるEnviroTechは、過去6か月間の衛星気象データに異常が見られた。
ログに、ごくわずかな痕跡しか残らないマイクロバーストで発生した、不正なデータ改ざんの記録が見つかった。
意図は不明瞭だが、その影響は重大だ。最適な対応策は何だろうか？
A. データ相互検証を促す公式声明を直ちに発表する。
B. 国家の関与を推測し、国際的なサイバーセキュリティ機関にアプローチする。
C. 影響を受けたシステムを隔離し、徹底的なフォレンジック調査を開始し、最新の変更されていないバックアップに戻します。
D. 違反を露呈することなく、矛盾点を特定するためにグローバルな機関と協力する。
Answer: C (メーッセージを残す)
包括的かつ詳細な説明（ECIH準拠）：
このシナリオでは、ECIHのインシデント対応ライフサイクルで定義されているように、封じ込め、分析、復旧の各段階において断固とした行動が求められます。
選択肢Cが正解です。影響を受けたシステムを隔離することで、それ以上の操作を防ぐことができ、フォレンジック調査によって範囲と手法を特定でき、検証済みのクリーンなバックアップから復元することでデータの整合性を確保できます。ECIHは、調査開始後にのみ検証済みの復元を行うことを重視しています。
選択肢A、B、Dは時期尚早または憶測に基づくものであり、誤った情報をもたらす恐れがある。

最新問題: **136**
AlphaTechは最近、自社のインフラストラクチャにおいて高度な持続的脅威（APT）の兆候を発見しました。インシデント対応チームは、包括的な対応戦略を策定するために、脅威に関するより多くの情報を収集しようとしています。脅威インテリジェンスプラットフォームを活用するにあたり、APTに関する詳細かつ実用的な情報を収集する上で、次のうちどの方法が最も効果的でしょうか？
A. 既知のAPTキャンペーンに関連するIOCを検索し、観測されたパターンと比較します。
B. 業界の同業者と協力して、同様の脅威や観察されたTTP（戦術 技術、手順）を理解する。
C. 一般的なサイバー脅威に関する過去のデータを取得し、将来の動きを予測する。
D. オープンソースフォーラムから情報を収集し、内部に統合する。
Answer: B (メーッセージを残す)
包括的かつ詳細な説明（ECIH準拠）：

ECIHは、高度な持続的脅威（APT）に対処するには、静的な指標だけでは不十分であり、それ以上の情報が必要であると強調している。IOC（侵害指標）は有用ではあるものの、変化が激しく、提供される情報も限られている。
選択肢Bが正解です。業界の仲間との連携により、戦術、技術、手順（TTP）を共有することが可能になり、これらはIOC（侵害指標）よりも安定性が高く、実行可能性も高いからです。ECIHは、APT（高度標的型攻撃）に対する状況認識を向上させるため、情報共有コミュニティ、ISAC（情報共有諮問委員会）、信頼できる仲間との連携を強く推進しています。
選択肢A、C、Dは、部分的または時代遅れの知見しか提供しておらず、運用面での深みに欠ける。
したがって、攻撃者の行動に焦点を当てたピアコラボレーションが最も効果的なアプローチである。

最新問題: **137**
ジョンはプロのハッカーで、標的組織に対して攻撃を仕掛けています。彼は、IPアドレスと標的サーバー間の接続をリダイレクトすることで、ユーザーがインターネットアドレスを入力すると、元のウェブサイトに酷似した偽のウェブサイトにリダイレクトされるようにしようとしています。彼はキャッシュポイズニングの手法を用いてこの攻撃を試みています。ジョンが標的組織に対して行っている攻撃の種類を特定してください。
A. 戦争運転
B. ファーミング
C. スキミング
D. 言い訳
Answer: (解答を表示する)
ファーミングは、ウェブサイトのトラフィックを別の偽のウェブサイトにリダイレクトすることを目的としたサイバー攻撃です。DNS サーバーのキャッシュを汚染することで、攻撃者は、ユーザーが意図したサイトから、ユーザーが知らないうちに、またはユーザーが不正なリンクをクリックするなどの操作を行うことなく、悪意のあるサイトにリダイレクトすることができます。この手法は、ブラウザに正しい URL を入力したにもかかわらずリダイレクトされてしまう善意のユーザーにも影響を与える可能性があるため、特に悪質です。ウォー ドライビングは、移動中の車両から無線ネットワークを検索するもので、スキミングは、ATM や販売時点情報管理端末に設置されたデバイスを使用してクレジットカード

情報を盗むもので、プリテキスティングは、攻撃者が特権データを取得するために嘘をつくソーシャル エンジニアリングの一種です。参考資料:インシデント ハンドラー (ECIH v3) 認定プログラムでは、DNS ポイズニングやファーミングなど、さまざまなサイバー攻撃と手法を取り上げ、攻撃者が脆弱性を悪用してユーザーを不正なサイトにリダイレクトする方法を説明しています。

最新問題: **138**
特権アクセス権限を持つ正規ユーザーが企業の情報資産を不正使用し、資産の機密性、完全性、可用性に直接影響を与える場合、以下のように呼ばれます。
A. 内部脅威
B. ゾンビ
C. 外部からの脅威
D. ソーシャルエンジニア
Answer: A (メーッセージを残す**)**

最新問題: **139**
攻撃者または内部関係者は、ファイアウォール内にセキュリティ対策が施されていないアクセスポイントを設置することで、信頼できるネットワークへのバックドアを作成します。そして、任意のソフトウェアまたはハードウェアのアクセスポイントを使用して攻撃を実行します。次のうち、このタイプの攻撃はどれですか？
A. パスワードベースの攻撃
B. マルウェア攻撃
C. メール感染
D. 不正アクセスポイント攻撃
Answer: D (メーッセージを残す**)**

最新問題: **140**
オープンソースのTCP/IPネットワーク侵入防止・検知システム（IDS/IPS）は、ルール駆動型言語を使用し、リアルタイムのトラフィック分析とパケットログ記録を実行します。これは次のように呼ばれます。
A. 聖人
B. 鼻を鳴らす
C. ネッソス
D. Wireshark
Answer: B (メーッセージを残す**)**

最新問題: **141**
システム分析においては、ブラウザデータを利用して様々な認証情報にアクセスできる。Microsoft Edgeブラウザの履歴データファイルを分析するために使用されるツールは次のうちどれですか？

A. Chrome履歴ビュー
B. 閲覧履歴表示
C. MZCacheView
D. MZHistoryView
Answer: B (メーッセージを残す)
BrowsingHistoryView は、Microsoft Edge を含むさまざまな Web ブラウザーから履歴データを収集および分析するように設計されたツールです。ユーザーは、ブラウザーに保存されている閲覧履歴を 1 つの統合インターフェイスで表示できます。これには、アクセスした URL、ページ タイトル、アクセス時間、および各ページへのアクセス回数が含まれます。ChromeHistoryView は Google Chrome に特化していますが、BrowsingHistoryView は複数のブラウザーをサポートしているため、さまざまなプラットフォームで履歴データを分析するのに汎用性があります。MZCacheView および MZHistoryView は、Microsoft Edge またはその他のブラウザー履歴分析のコンテキストでこの目的のために認識されているツールとしては存在しません。参考資料:インシデント ハンドラー (ECIH v3) コースおよび学習ガイドでは、調査中に Web ブラウザー データを分析するために BrowsingHistoryView などのデジタル フォレンジック ツールを使用することの重要性が強調されています。

最新問題: **142**
最近のアップデート後、Trend Spotのユーザーからウェブサイトの読み込み速度が遅くなるという報告がありました。分析の結果、攻撃者が偽の検索リクエストを大量にアプリケーションに送信し、アプリケーション層でDoS攻撃が発生していることが判明しました。Trend Spotはまずどのように対応すべきでしょうか？
A. 定期的にサーバーキャッシュをクリアしてください。
B. より堅牢なホスティングプロバイダーに移行する。
C. 検索リクエスト機能にレート制限を導入します。
D. 不審なトラフィックに対してIPアドレスベースのブロックを実装します。
Answer: (解答を表示する)
今回の事案は、帯域幅ではなく特定の機能を標的としたアプリケーション層のDoS攻撃です。ECIHは、このようなシナリオにおいて機能レベルの保護を重視しています。
選択肢Cが正解です。レート制限は、正当な利用を許可しつつ、不正なリクエストの頻度を制限するからです。
これは、サービスの可用性を損なうことなく、悪用された機能に直接対処するものです。
オプションDは、共有IPアドレスを使用している正当なユーザーをブロックする可能性があります。オプションAとBは、攻撃経路を軽減しません。
レート制限は、レイヤー7攻撃時の可用性を維持するためのECIHのガイドラインに沿ったものです。

最新問題: **143**

ジェームズはプロのハッカーであり、ある組織に雇われてクラウドサービスを悪用する任務を遂行している。この任務を遂行するため、ジェームズはクラウドサービスへの匿名アクセスを確立し、パスワードや鍵のクラッキング、悪意のあるデータのホスティング、DDoS攻撃など、様々な攻撃を実行した。
彼はクラウドプラットフォームに対して、次のうちどの脅威をもたらしているでしょうか？
A. デューデリジェンスの不備
B. データ漏洩／データ損失
C. 安全性の低いインターフェースとAPI
D. クラウドサービスの悪用および不正利用
Answer: D (メーッセージを残す**)**

最新問題**: 144**
事業継続性とは、冗長なハードウェアとソフトウェアの導入、耐障害性システムの利用、そして確実なバックアップと復旧戦略によって、組織が災害発生後も機能を継続できる能力と定義されます。事業継続計画において必須となる計画を特定してください。
A. 販売 ･マーケティング計画
B. 鑑識手順計画
C. 事業復旧計画
D. 新規事業戦略計画
Answer: (解答を表示する**)**

最新問題**: 145**
最も一般的な知的財産の種類は以下のとおりです。
A. 著作権と商標
B. 特許
C. 工業デザイン権および企業秘密
D. 上記すべて
Answer: D (メーッセージを残す**)**
説明／参考資料：

最新問題**: 146**
スタンリーはシンガポールに拠点を置く大手多国籍企業でインシデント対応担当者として働いています。彼は最近社内で発生したサイバーセキュリティインシデントの調査を依頼されました。インシデント調査中に、彼は被害を受けたシステムから証拠を収集しました。彼は、この証拠を陪審員に明確かつ分かりやすい方法で提示し、証拠が事実を明らかにし、さらに調査プロセスを確認するためにインシデントに関する専門家の意見を得るのに役立つようにする必要があります。上記のシナリオにおいて、スタンリーはデジタル証拠の以下のどの特性を保存しようとしましたか？
A. 完全性

B. 受諾可能性
C. 信憑性
D. 真正性
Answer: B (メーッセージを残す**)**
前述のシナリオにおいて、スタンレーが事実関係を明確にし、専門家の意見を得るのに役立てる目的で、陪審員に証拠を明確かつ分かりやすく提示しようとした努力は、証拠能力の特性に合致する。デジタル証拠の証拠能力とは、法廷における証拠の受容性に関わるものであり、証拠が法的基準と手続きに準拠した方法で収集、処理、提示されるかどうかにかかっている。これには、証拠が関連性があり、信頼性が高く、過度に偏見を招くものでないことを保証することが含まれる。スタンレーは、陪審員が理解し、捜査過程を確認するために利用できる方法で証拠を提示する準備をすることで、証拠が法的手続きにおける証拠能力の基準を満たすことを確実にすることに重点を置いている。完全性、信憑性、真正性もデジタル証拠の重要な特性ですが、提供されたコンテキストは、スタンレーの主な焦点が、証拠が法廷で有効とみなされるための法的要件を満たすことにあることを示しています。参考文献 :インシデントハンドラー（ECIH v3）認定資料は、インシデント対応の法的側面をカバーしており、証拠収集および提示プロセスの基本的な目的として、法的手続きにおける証拠の許容性を確保することの重要性も含まれています。

最新問題**: 147**
マイケルはサイバーテック・ソリューションズのインシデントハンドラーです。彼はクラウドセキュリティインシデントの検出と分析を行っています。ストレージユニットのファイルシステム、スラック領域、メタデータを分析し、隠れたマルウェアや悪意のある行為の証拠を探しています。
マイケルが対応したクラウドセキュリティインシデントを特定してください。
A. ネットワーク関連のインシデント
B. 保管関連のインシデント
C. アプリケーション関連のインシデント
D. サーバー関連のインシデント
Answer: B (メーッセージを残す**)**
マイケルの活動内容は、ファイルシステム、スラック領域、ストレージユニットのメタデータを分析して、隠れたマルウェアや悪意の証拠を探し出すことであり、彼がストレージ関連のクラウドセキュリティインシデントに対応していることを示している。
この種のインシデントは、クラウド環境に保存されているデータへの不正アクセス、改ざん、またはデータ漏洩に関係します。マイケルは、ファイルシステムやメタデータなどのストレージの側面に着目することで、クラウドにおけるストレージ関連のセキュリティインシデントを示す、データの保存に特に影響を与える侵害の兆候を探しています。参考資料：インシデントハンドラー（ECIH v3）認定資料では、さまざまな種類のクラウドセキュリティインシデントについて説明し、機密データが標的になったり侵害されたりする可能性

のあるストレージ関連のインシデントを含め、それらを検出して対応する方法を詳しく説明しています。

最新問題: **148**
ネットワーク担当のネッドは、ある会社のセキュリティ管理者です。彼は会社の新しいウェブサーバーを本番環境に導入しようとしています。
会社のネットワークを最大限に保護するために、サーバーを以下のどのゾーンに設置すべきでしょうか？
A. DMZ
B. イントラネット
C. サンドボックス
D. ハニーポット
Answer: B (メーッセージを残す**)**

最新問題: **149**
_____ ユーザーの入力内容を記録します。
A. マルウェア
B. ウイルス
C. スパイウェア
D. アドウェア
Answer: C (メーッセージを残す**)**

最新問題: **150**
脅威対応担当者のリナは、Nuix Adaptive Securityツールを使用して、不審なファイルアップロードのアラートを分析しています。彼女は、内部関係者が勤務時間外にOutlookを使用して未知のメールアドレスに添付ファイルを送信したことを特定しました。このツールは、スクリーンショット、ファイルメタデータ、キーストロークログをキャプチャします。
リナは主にどのような種類の証拠に依拠しているのでしょうか？
A. ユーザー行動分析とエンドポイント監視
B. SIEMイベント相関
C. ネットワークフォレンジックログ
D. ホストベースの侵入防止ログ
Answer: A (メーッセージを残す**)**
EC-Councilのインシデントハンドラー（ECIH）カリキュラムでは、内部脅威の調査はエンドポイント監視とユーザー行動分析（UBA/UEBA）に大きく依存すると説明されています。今回のケースでは、Nuix Adaptive Securityツールがスクリーンショット、ファイルメタデータ、キーストロークログをキャプチャしました。これらは、エンドポイント上でのユーザーアクティビティを直接監視するホストレベルの監視手法です。
ユーザー行動分析は、営業時間外に未知の外部アドレスに添付ファイルを送信するなど、通常のパターンからの逸脱を検出することに重点を置いています。ECIHはこれを、潜在的

なデータ漏洩を示す異常な内部行動として識別します。エンドポイント監視ツールは、画面キャプチャ、アプリケーション使用ログ、キーストローク記録、ファイル転送メタデータなど、詳細なアーティファクトを提供します。これらは、フォレンジック分析と証拠保全にとって非常に重要です。
オプションB（SIEMイベント相関）は複数のシステムからログを集約しますが、通常はスクリーンショットやキーストロークレベルのデータは取得しません。オプションC（ネットワークフォレンジック）は、ユーザーレベルの操作証拠ではなく、パケットキャプチャとトラフィック分析に重点を置いています。オプションD（ホストベースの侵入防御システム）は主に悪意のあるアクティビティをブロックまたは検出しますが、スクリーンショットやキーストロークログなどの包括的な動作監視データは提供しません。
ECIHは、内部脅威の事例において、意図と範囲を特定するために、行動指標、デジタル活動の再構築、エンドポイントのテレメトリに大きく依存していることを強調しています。Linaがユーザー活動の再構築とエンドポイントレベルのアーティファクトに依存していることは、ユーザー行動分析とエンドポイント監視の考え方と明確に一致しています。
したがって、正解はユーザー行動分析とエンドポイント監視です。

最新問題: **151**
デジタルフォレンジック調査官が、被害を受けたコンピュータ上のすべてのIPアドレスとその関連付けられたMACアドレスのリストを表示し、そのコンピュータと通信していたマシンを特定するために使用するコマンドは何ですか？
A. "ifconfig" コマンド
B. "dd" コマンド
C. "arp"コマンド
D. 「netstat -an」コマンド
Answer: C (メーッセージを残す**)**

最新問題: **152**
アレクシスはXYZ組織でインシデント対応担当者として働いています。彼女は最近発生した攻撃の背後にいる人物を特定し、その責任を帰属させるよう依頼されました。そのため、彼女は脅威帰属分析を行っています。脅威帰属分析とは、標的への綿密に計画され実行され

た侵入や攻撃を支援している特定の人物、組織、または国家を特定する分析です。アレクシスが行った脅威帰属分析の種類は次のうちどれですか？
A. 侵入セットの帰属
B. 真の帰属
C. 国民国家帰属
D. キャンペーンアトリビューション
Answer: A (メーッセージを残す**)**

最新問題**: 153**
次のどの手法が、偽装されたAPが元のAPと類似したIPアドレスとMACアドレスを持っている場合でも、新しいAPを見つけて既に確立されているチャネルに接続しようとすることで、中間者攻撃を検出するのに役立ちますか？
A. 一般的な無線トラフィック監視
B. アクセスポイント監視
C. ワイヤレスクライアント監視
D. ネットワークトラフィック監視
Answer: (解答を表示する**)**

最新問題**: 154**
ウイルスとワームの主な違いは次のとおりです。
A. ワームは増殖するためにホストファイルが必要ですが、ウイルスはホストファイルを必要としません。
B. ウイルスとワームは同じマルウェアの一般的な名称です
C. ウイルスは増殖するためにホストファイルが必要ですが、ワームは必要ありません
D. ウイルスはユーザーの操作を必要とせず、自己複製するマルウェアです。
Answer: (解答を表示する**)**

最新問題**: 155**
ジェイコブはドルフィン -インベストメントという会社に勤務しています。勤務中に、彼のコンピューターに何らかの問題が発生していることに気づき、社内の担当者にその問題を伝えたいと考えました。しかし、この会社には現在、このような問題に対処するためのチケットシステムがありません。上記の状況において、ジェイコブが担当チームにこの件を知らせるために、ドルフィン -インベストメントが利用できるチケットシステムは次のうちどれでしょうか？
A. ThreatConnect
B. IBM XForco Exchange
C. MISP
D. ManageEngine ServiceDesk Plus
Answer: D (メーッセージを残す**)**

最新問題: **156**
以下の手順は、鑑識準備計画における主要な活動を説明するものです。
1. 職員に事件への対処方法と証拠保全方法を訓練する。
2. 手順を文書化するための特別なプロセスを作成する
3. 事件に必要な潜在的な証拠を特定する
4. 証拠の出所を特定する
5. 調査プロセスを指導するための法律諮問委員会を設置する
6. 事件が本格的な調査を必要とするかどうかを判断する
7. 収集した証拠を安全に取り扱い、保管するための方針を策定する。
8. 最小限の混乱で電子証拠を合法的に抽出するための手順を決定するポリシーを定義する。フォレンジック準備計画に含まれる正しい手順の順序を特定する。
A. 2-->3-->1-->4-->6-->5-->7-->8
B. 3-->4-->8-->7-->6-->1-->2-->5
C. 3-->1-->4-->5-->8-->2-->6-->7
D. 1-->2-->3-->4-->5-->6-->7-->8
Answer: (解答を表示する**)**
前述の活動に基づくと、鑑識準備計画における正しい手順は以下のとおりです。
* 事件に必要な証拠を特定する。
証拠の出所を特定する。
* 最小限の混乱で電子証拠を合法的に抽出するための手順を定めるポリシーを定義する。
収集した証拠を安全に取り扱い、保管するためのポリシーを確立する。
* 当該事案が本格的な調査を必要とするかどうかを判断する。
* 職員に対し、事件への対処方法と証拠保全方法について研修を実施する。
手順を文書化するための特別なプロセスを作成する。
参考資料 :インシデントハンドラー（ECIH v3）コースと学習ガイドには、フォレンジック対応計画に関する議論が含まれており、組織がインシデントを効果的に法的および技術的に処理できるように準備することの重要性が強調されています。

最新問題: **157**
フィンは、システムにインストールされているWindowsオペレーティングシステムで発生したインシデントの根本原因を取り除く、駆除フェーズに取り組んでいます。彼は、不足しているセキュリティパッチを検出し、システムとネットワークに最新のパッチをインストールできるツールを実行しました。不足しているセキュリティパッチを検出するために、彼は次のうちどのツールを使用しましたか？
A. Microsoft Cloud App Security
B. Offico360 アドバンスドスロートプロテクション
C. マイクロソフトアドバンストスレットアナリティクス
D. Microsoft Baseline Security Analyzer
Answer: D (メーッセージを残す**)**

Microsoft Baseline Security Analyzer (MBSA) は、セキュリティ更新プログラムの不足や一般的なセキュリティ設定ミスをチェックすることで、コンピュータやネットワークのセキュリティ状態を評価するために設計されたツールです。インシデント対応プロセスの根絶フェーズで作業しているフィンの場合、MBSA の使用は理にかなっています。このツールが不足しているセキュリティパッチを検出し、最新のパッチのインストールを推奨する機能は、インシデントの根本原因となりうる Windows オペレーティングシステムの脆弱性を排除する上で非常に重要です。
MBSAは、セキュリティアップデートの不足、設定ミス、その他の脆弱性をシステム上でスキャンし、詳細なレポートと修復に関する推奨事項を提供します。このステップは、インシデントの根本原因を取り除き、将来の攻撃からシステムを保護することを目的とする駆除フェーズにおいて非常に重要です。必要なパッチがすべて適用されていることを確認することで、Finnは攻撃者に悪用される可能性のあるセキュリティ上のギャップに対処しています。
参考資料 :EC-CouncilのECIH v3プログラムでは、システムとネットワークを保護するためのさまざまなツールとテクニックについて説明しています。これには、パッチ管理の重要性や、インシデント対応プロセスの一環として必要なセキュリティ更新プログラムを特定して適用するためのMicrosoft Baseline Security Analyzerなどのツールの使用が含まれます。

最新問題**: 158**
サーベンス -オクスリー法 $OX法）の該当箇所を特定する。この条項は1つのセクションのみで構成されており、証券アナリストの報告に対する投資家の信頼回復を支援するために設計された措置が含まれている。
A. タイトルV :アナリストの利益相反
B. 第7章：研究および報告
C. タイトルIX :ホワイトカラー犯罪刑罰強化
D. 第VIII編：企業および刑事詐欺の責任
Answer: (解答を表示する**)**

最新問題**: 159**
将来起こりうる出来事の兆候は、次のように呼ばれます。
A. 兆候
B. 積極的な
C. 反応性
D. 前駆者
Answer: D (メーッセージを残す**)**

最新問題**: 160**
次のうち、揮発性データと呼ばれないものはどれですか？
A. ソケットまたはポートを開放する

B. システムのライムがないデール
C. ファイルの作成日
D. ネットワークインターフェースの状態
Answer: C (メーッセージを残す**)**
揮発性データとは、一時的に保存され、コンピュータの電源を切ったり再起動したりすると失われる情報のことです。例えば、RAMの内容（開いているソケットやポートを含む）、システムの日時、ネットワークインターフェースの状態などが挙げられます。ただし、ファイルの作成日は、ハードドライブに保存され、システムの再起動や電源オフ後も利用できるため、不揮発性データとみなされます。
不揮発性データは、ハードドライブ、SSD、磁気テープなどの永続ストレージ媒体に保存され、削除または上書きされるまでそこに残ります。参考資料:インシデントハンドラー（ECIH v3）認定では、デジタルフォレンジックとインシデント対応のコンテキストで揮発性データと不揮発性データの区別を強調し、システムシャットダウン時に失われる可能性のあるデータと、永続するデータを理解することの重要性を強調しています。

最新問題**: 161**
スタンレーは、米国に拠点を置くTexaCorp.に勤務するインシデントハンドラーです。組織外からのメールが増加していることへの懸念が高まる中、スタンレーは組織のセキュリティを維持するために適切な措置を講じるよう求められました。悪意のあるメールを検出して封じ込める過程で、スタンレーは従業員が受信したメールの正当性を確認するよう指示されました。スタンレーがこのタスクを実行するために使用できるツールを特定してください。
A. メールフォルダ
B. イベントログアナライザー
C. 郵便物の発送
D. 丁寧なメール
Answer: C (メーッセージを残す**)**

最新問題**: 162**
ファーヒーンは、フロリダに拠点を置く評判の高いIT企業のインシデント対応担当者です。ファーヒーンは、組織が最近直面したサイバー犯罪の調査を依頼されました。このプロセスの一環として、彼女は被害者のシステムから静的データを収集しました。彼女はコマンドラインツールであるddを使用してフォレンジック複製を実行し、元のディスクのNTFSイメージを取得しました。彼女はディスクのセクターごとのミラーイメージを作成し、出力イメージファイルをimage.ddとして保存しました。ファーヒーンが静的データを収集する際に実行した静的データ収集プロセスの手順を特定してください。
A. 比較
B. 物理的なプレゼンテーション
C. システム保存
D. 行政上の考慮事項

Answer: C (メーッセージを残す)

最新問題: **163**
リチャードは企業ネットワークを分析しています。ネットワークのIPSでアラートが発生した後、彼はすべてのサーバーがウェブサイトabc.xyzに大量のトラフィックを送信していることを特定しました。このネットワークに影響を与えた情報セキュリティ攻撃ベクトルはどのようなものですか？
A. ボットネット
B. 前進持続三は
C. ランサムウェア
D. IoTの脅威
Answer: (解答を表示する)
企業ネットワークのサーバーが特定の Web サイトに対して大量のトラフィックを送信していることが、ネットワークの侵入防止システム (IPS) によって検出された場合、この動作はボットネット攻撃を示唆しています。ボットネットとは、侵害されたコンピューターのネットワークであり、多くの場合「ボット」と呼ばれ、通常はコンピューターの所有者の知らないうちに攻撃者によって遠隔操作されます。攻撃者はこれらのボットに、分散型サービス拒否 (DDoS) 攻撃を実行させたり、スパムを送信したり、その他の悪意のある活動を実行させたりすることができます。このシナリオでは、サーバーがボットとして動作し、大量のトラフィックで Web サイトを標的にしていることから、Web サイト abc.xyz に対して DDoS 攻撃を実行するためにボットネットに組み込まれた可能性が示唆されます。参考資料:インシデント ハンドラー (ECIH v3) コースと学習ガイドでは、ボットネットや分散型サイバー攻撃におけるその役割など、さまざまな種類のサイバー脅威と攻撃ベクトルについて説明しています。

最新問題: **164**
OBC組織でインシデント対応担当者として働くエリザベスは、組織のセキュリティに対するリスクを評価しています。評価プロセスの一環として、彼女は脅威発生源が既存のシステム脆弱性を悪用する確率を計算しています。エリザベスは現在、以下のリスク評価のどの段階にいるでしょうか？
A. 脆弱性の特定
B. 尤度分析
C. 影響分析
D. システム特性評価
Answer: B (メーッセージを残す)

最新問題: **165**
機関が情報技術資産を保護するための計画に関する要件と指示を文書で示した、生きた高レベルの文書は、次のように呼ばれます。
A. 情報セキュリティ手順

B. 情報セキュリティポリシー
C. 情報セキュリティ基準
D. 情報セキュリティ基準
Answer: (解答を表示する**)**

最新問題**: 166**
ブランは組織のネットワークを評価しているインシデントハンドラーです。彼はWiresharkを使用してネットワーク上でのpingスイープ試行を検出したいと考えています。ブランはこのタスクを実行するために、次のどのWiresharkフィルタを使用するでしょうか？
A. icmp.lype==8
B. icmp.scq
C. icmp.redir_gw
D. icmp.ident
Answer: A (メーッセージを残す**)**

最新問題**: 167**
グローバル企業のサイバーセキュリティ対応チームは、上級幹部からのメールと思われる不審なメールについて、従業員から警告を受けました。調査の結果、チームはメールヘッダーを分析し、送信元のIPアドレスが組織とは一切関係のない外国のものであることに気づきました。WHOIS検索の結果、そのIPアドレスは不明な組織に登録されていることが確認されました。不審な活動を特定する上で、どのような重要な要素が役立ったでしょうか？
A. 反発分析
B. スパムフィルターのログ
C. DKIM認証
D. 発信元IPトレース
Answer: D (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
ECIHのメールセキュリティインシデント対応モジュールでは、なりすましメールや悪意のあるメールを特定するための主要な方法として、メールヘッダーの分析を重視しています。最も重要なヘッダー要素の一つは送信元IPアドレスであり、これによりメールの実際の送信元が明らかになります。

選択肢Dが正解です。発信元IPアドレスを追跡し、WHOISで検証することで、そのメールが正規の組織からのものではないという明確な証拠が得られました。この手法により、担当者は正規の役員からの連絡となりすましを区別することができます。
オプションAは事後対応型で信頼性に欠ける。オプションBは検出コンテキストを提供するが、原因特定はできない。オプションCはドメイン認証を検証するが、認証情報が漏洩した場合になりすましを必ずしも明らかにするとは限らない。
ECIHは、IPアドレス追跡とWHOIS分析を組み合わせることは、役員なりすまし捜査において強力な検証方法であると強調しており、選択肢Dが正解である。

最新問題: **168**
ファーヒーンは、フロリダに拠点を置く評判の高いIT企業でインシデント対応担当者として働いています。ファーヒーンは、最近組織が直面したサイバー犯罪の調査を依頼されました。調査の一環として、彼女は被害を受けたシステムから静的データを収集しました。彼女はDDツールコマンドを使用してフォレンジック複製を実行し、元のディスクのNTFSイメージを取得しました。彼女はディスクのセクターごとのミラーイメージを作成し、出力イメージファイルをimage.ddとして保存しました。
Farheenが静的データを収集する際に実行した静的データ収集プロセスの手順を特定してください。
A. 比較
B. 行政上の考慮事項
C. システム保存
D. 物理的なプレゼンテーション
Answer: (解答を表示する**)**
ファーヒーンがDDツールを使用して元のディスクのセクターごとのミラーイメージを作成したことは、システム保存の一例です。このプロセスは、ストレージデバイスの正確なコピーを作成し、調査中に元のデータが変更されないようにするために、デジタルフォレンジックにおいて非常に重要です。ディスクのフォレンジック複製、つまりイメージを作成することで、ファーヒーンはディスク上の静的データが元の証拠を変更することなく、徹底的な分析のために現在の状態で保存されることを保証します。この手順により、捜査官はデータの正確な複製を扱うことができ、元の証拠の完全性を保護することができます。
参考資料：インシデントハンドラー（ECIH v3）認定資料では、データ取得と保存のためのさまざまな方法とツールについて説明し、フォレンジック分析の初期段階におけるシステム保存の重要性を強調しています。

最新問題: **169**
スミス氏は、オーストラリアに数店舗の支店を持つ小規模金融機関の主任インシデント対応担当者です。最近、同社は銀行間システムを介した大規模なサイバー攻撃を受け、500万ドルの損失を被りました。

詳細な調査の結果、今回の事件は、6か月前に攻撃者が軽微な脆弱性を悪用してネットワークに侵入し、ユーザーに気づかれることなくアクセスを維持していたことが原因であることが判明した。攻撃者はその後、ユーザーの指紋を削除しようと試み、銀行間システムで権限を持つ人物のコンピュータへの横方向の移動を行った。最終的に攻撃者はアクセス権を取得し、不正取引を実行した。
上記のシナリオに基づいて、最も正確な攻撃の種類を特定してください。
A. APT攻撃
B. フィッシング
C. サービス拒否攻撃
D. ランサムウェア攻撃
Answer: (解答を表示する**)**

最新問題**: 170**
脆弱性評価フェーズでは、インシデント対応担当者は以下のような様々な手順を実行します。
1. ツールを使用して脆弱性スキャンを実行する
2. 脆弱性を特定し、優先順位を付ける
3. 物理的セキュリティを調査および評価する
4. OSINT情報収集を実施して脆弱性を検証する
5. スキャナーの結果にビジネスとテクノロジーのコンテキストを適用する
6. 設定ミスや人為的ミスがないか確認する
7. 脆弱性スキャンレポートを作成する
インシデント対応担当者が実施する脆弱性評価手順の正しい順序を特定する。
A. 3-->6-->1-->2-->5-->4-->7
B. 1-->3-->2-->4-->5-->6-->7
C. 4-->1-->2-->3-->6-->5-->7
D. 2-->1-->4-->7-->5-->6-->3
Answer: C (メーッセージを残す**)**
インシデント対応担当者が脆弱性評価フェーズで実行すべき正しい手順は以下のとおりです。
* OSINT情報収集を実行して脆弱性を検証する 4）まず、オープンソースインテリジェンス（OSINT）を使用して、組織のデジタルフットプリントと潜在的な脆弱性に関する情報を収集します。
* ツールを使用して脆弱性スキャンを実行する (1):次に、組織のネットワークとシステムをスキャンして脆弱性を検出するための専用ツールが使用されます。
* 脆弱性の特定と優先順位付け 2）：特定された脆弱性は、その深刻度と組織への潜在的な影響に基づいて分析され、優先順位が付けられます。
* 物理的セキュリティの調査と評価 3）：物理的セキュリティの評価は、全体的なセキュリティ体制とデジタル資産の保護に影響を与える可能性があるため、非常に重要です。

* 設定ミスや人的ミスをチェックする (6):このステップでは、システムやネットワークの設定ミス、および脆弱性につながる可能性のある人的ミスを探します。
* スキャナーの結果にビジネスとテクノロジーのコンテキストを適用する (5):スキャンの結果は、リスクを正確に評価するために、ビジネスとそのテクノロジー環境のコンテキスト内で評価されます。
* 脆弱性スキャンレポートの作成 (7):最後に、脆弱性、その深刻度、推奨される緩和戦略を詳細に記述した包括的なレポートが作成されます。
この手順により、徹底的な評価が保証され、最もリスクの高い脆弱性を優先的に特定し、軽減策のための実用的な知見が得られます。
参考資料:ECIH v3のコースと学習ガイドでは、脆弱性評価プロセスについて詳しく解説しており、組織のITインフラストラクチャ内のセキュリティ脆弱性を特定、評価、対処するために必要な手順を詳細に説明しています。

最新問題: **171**
SOCアナリストのララは、IDSによって生成された複数のアラートを調査しています。このアラートは、特定のワークステーションから内部アプリケーションへのログインが繰り返し失敗していることを示しています。Windowsイベントビューアーのログを確認したところ、勤務時間外にユーザーが繰り返しログインを試みていることが判明しました。さらに調査を進めた結果、ユーザーが不正なリモートデスクトップツールをインストールしていたことが明らかになりました。この状況を最もよく表しているのは次のうちどれですか？
A. 方針に基づき実施されたリモートワークの試み
B. 第三者による不正アクセス事件
C. ポリシー違反およびソフトウェアのインストールによる不適切な使用
D. 内部アプリケーションに対するDoS攻撃
Answer: C (メーッセージを残す**)**
EC-Councilのインシデントハンドラー（ECIH）カリキュラムでは、不正なソフトウェアのインストールやポリシー違反などのインシデントを不適切な使用インシデントに分類しています。このシナリオでは、アクティビティは外部の第三者ではなく、正当な社内ワークステーションとユーザーアカウントから発生したものです。
営業時間外における度重なるログイン失敗と、許可されていないリモートデスクトップツールのインストールは、利用規約違反および悪意のある意図を示唆しています。しかしながら、重要な点は、これらの行為が有効なアクセス認証情報を使用した内部ユーザーによって行われたことであり、これは外部からの不正アクセス攻撃ではなく、内部関係者によるポリシー違反であるということです。
オプションAは、ポリシーの範囲内での正当なリモートワークを示唆していますが、これは不正なソフトウェアのインストールによって矛盾しています。オプションBは第三者による侵害を示唆していますが、ログには内部ユーザーアカウントからのアクティビティが示されています。オプションD（DoS攻撃）は、トラフィックの大量流入によるサービス妨害を伴いますが、ここでは説明しません。

ECIHは、内部関係者による不正使用を軽減するために、適切な利用ポリシーの遵守、ユーザー行動の監視、不正なソフトウェアインストールの制限、最小権限の原則の適用を重視しています。したがって、このシナリオは、ポリシー違反や不正なソフトウェアインストールによる不適切な利用に最も適しています。

最新問題: **172**
以下の内部脅威のうち、潜在的なセキュリティ脅威について知識のない内部関係者、あるいは職場の効率性を高めるために一般的なセキュリティ手順を単に無視する内部関係者が関与する脅威はどれですか？
A. 過失のある内部関係者
B. 情報漏洩した内部関係者
C. プロのインサイダー
D. 悪意のある内部関係者
Answer: (解答を表示する**)**

最新問題: **173**
インシデント対応担当者が、進化し続けるメールの脅威から組織を守るために使用できるメールセキュリティツールは次のうちどれですか？
A. メールヘッダーアナライザー
B. Gpg4win
C. G Suite Toolbox
D. Mx Toolbox
Answer: B (メーッセージを残す**)**

最新問題: **174**
イヴはABC社のインシデントハンドラーです。ある日、彼女は社内従業員の一人からメールハッキング事件に関する苦情を受けました。インシデント対応プロセスの一環として、彼女は業務継続性を維持するために、インシデントの影響から復旧するための多くの復旧手順に従わなければなりません。
彼女が従業員アカウントを安全に保護するために最初に行うべき手順は何ですか？
A. すべてのメール内のリンクと添付ファイルのスキャンを有効にする
B. システム間の自動ファイル共有を無効にする
C. メールサービスを復元し、パスワードを変更する
D. 二段階認証を有効にする
Answer: (解答を表示する**)**

最新問題: **175**
受信されたメッセージで、緊急の対応が必要であり、受信者に特定のファイルを削除したり、他の人に転送したりするよう促すメッセージは、次のように呼ばれます。
A. 郵便爆弾

B. アドウェア
C. ウイルス詐欺
D. スピアフィッシング
Answer: (解答を表示する**)**

最新問題**: 176**
インシデントの影響を受けたコンピュータシステムを再構築し、正常な運用状態に復旧させるプロセス
すべてのプロセス、ポリシー、ツールを含む段階は、次のように呼ばれます。
A. インシデント管理
B. インシデント対応
C. インシデント復旧
D. インシデント対応
Answer: C (メーッセージを残す**)**
説明／参考資料：

最新問題**: 177**
SOCアナリストのダニエルは、組織のメールサーバーに対して、異なるIPアドレスから複数のTCPリクエストが届いていることを検出しました。しかし、いずれのリクエストもハンドシェイクを完了していません。彼はサーバーリソースを枯渇させようとしている可能性を疑い、netstatログでそれを確認しました。ダニエルが特定しているのは、どのタイプのプロトコルレベルのインシデントでしょうか？
A. TCPセッションハイジャック
B. UDPリフレクション
C. DNSキャッシュポイズニング
D. SYN洪水攻撃
Answer: D (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
このシナリオでは、ECIHのネットワークセキュリティインシデントモジュールで解説されている、プロトコルレベルのサービス拒否攻撃の典型的な手法であるSYNフラッド攻撃について説明します。SYNフラッド攻撃では、攻撃者は大量のTCP SYNパケットを送信しますが、3ウェイハンドシェイクを完了させないため、サーバーは応答を待たされ、接続リソースが枯渇します。
選択肢Dが正解です。なぜなら、不完全なTCPハンドシェイク、半開きの接続、リソース枯渇はSYNフラッド攻撃の特徴だからです。複数の送信元IPアドレスが存在することは、分散型攻撃であることをさらに示唆しています。
オプションAは、既存のセッションを乗っ取るものであり、リソースを枯渇させるものではありません。オプションBは、UDPベースの増幅攻撃に適用されます。オプションCは、TCPハンドシェイクではなく、DNS解決に影響を与えます。

ECIHは、SYNフラッド攻撃を早期に特定することで、防御側はSYNクッキー、レート制限、およびアップストリームフィルタリングを展開できると強調しています。したがって、ハンドシェイクの異常を認識することは、サービスの可用性を保護する上で非常に重要です。

最新問題: **178**
コンピュータフォレンジック調査官は、デジタル証拠を保護するために適切な調査を実施する必要があります。
調査では、調査員は自動化されたツールと分析ツールを組み合わせて大量のデータを処理する必要があります。
手動による方法。関連するコンピュータフォレンジックプロセスを特定する。
A. 分析
B. 試験
C. 準備
D. コレクション
Answer: B (メーッセージを残す**)**

最新問題: **179**
以下のリスク軽減戦略のうち、リスク要因を低減して許容レベルまで下げるための対策を実行するもの、または潜在的なリスクを受け入れてITシステムの運用を継続するものはどれですか？
A. リスク想定
B. リスク回避
C. リスク計画
D. リスク移転
Answer: A (メーッセージを残す**)**
リスクの受容とは、潜在的なリスクを受け入れ、リスクを許容可能なレベルまで低減するための対策を実施しながら、ITシステムの運用を継続することを意味します。この戦略は、ある程度のリスクは避けられないことを認識し、リスクを完全に排除するのではなく、軽減策を通じてリスクを管理することに重点を置いています。
リスク回避とは、リスクを完全に回避するための行動をとることであり、リスク計画とは、潜在的なリスクに備えることであり、リスク移転とは、通常は保険やアウトソーシングを通じて、リスクを他者に移転することである。
リスク想定は、業務継続の必要性とリスク管理の必要性のバランスを取る実用的なアプローチです。参考文献 :ECIH v3 認証プログラムでは、さまざまなリスク軽減戦略を取り上げ、組織のリスク許容度と脅威の特定の状況に基づいて適切なアプローチを選択することを強調しています。

最新問題: **180**
メールによるインシデントを防止するための最良の方法はどれですか？

A. メール本文フィールドでのHTMLの無効化
B. Webプロキシフィルタリング
C. エンドユーザー向けトレーニング
D. ウイルス対策ルールの更新をインストールしています
Answer: (解答を表示する**)**

最新問題**: 181**
ジョンはマルウェアの痕跡を見つけるために、メモリダンプ分析を行っている。
彼は目的を達成するために、ボラティリティツールを利用した。
メモリダンプから実行中のプロセスを分析するために、彼は以下のVolatility Frameworkコマンドのうちどれを使用するでしょうか？
A. python vol.py svcscan --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem | more
B. python vol.py pslist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem
C. python vol.py hivelist --profile=Win2008SP1x86 -f /root/Desktop/memdump.mem
D. python vol.py imageinfo -f /root/Desktop/memdump.mem
Answer: B (メーッセージを残す**)**
Volatilityフレームワークは、揮発性メモリ（RAM）ダンプの分析に広く用いられているツールです。特にデジタルフォレンジックやマルウェア分析において有用です。メモリ分析における基本的なタスクの一つは、メモリダンプ取得時にシステム上で実行されていたプロセスを一覧表示することです。Volatilityフレームワークのpslistコマンドは、メモリ内のプロセスリストから全てのプロセスを一覧表示することでこの目的を果たします。これにより、悪意のあるプロセスの存在を含め、システム上で何が起こっていたのかについての貴重な情報を得ることができます。
回答オプションに示されている構文は、Volatilityツールでpslistコマンドを使用する際の構文に対応しており、分析対象のメモリダンプファイル（-f /root/Desktop/memdump.mem）と、ダンプが取得されたシステムのプロファイル（--profile=Win2008SP1x86）を指定します。プロファイルはVolatilityがメモリ構造を正しく解釈するのに役立つため、この情報は正確な分析に不可欠です。
参考資料: Volatility フレームワーク内で pslist コマンドを使用してメモリ ダンプから実行中のプロセスを分析する方法は、公式の Volatility ドキュメントに記載されており、インシデント対応活動の一環としてメモリ フォレンジックの分野における基本的な手法です。

最新問題: **182**
OBC組織でインシデント対応担当者として働くエリザベスは、組織のセキュリティに対するリスクを評価している。評価プロセスの一環として、彼女は脅威の発生源が既存のシステム脆弱性を悪用する確率を計算している。
エリザベスは現在、以下のリスク評価のどの段階にいますか？
A. 影響分析
B. 脆弱性の特定
C. システム特性
D. 尤度分析
Answer: (解答を表示する)

最新問題: **183**
アランはレッドチーム活動の一環として、社内ネットワークに対して偵察攻撃を行った。彼はIPアドレス範囲をスキャンして、稼働中のホストIPアドレスを特定した。彼はネットワークを悪用するためにどのような手法を用いたのか？
A. ポートスキャン
B. ピン掃討
C. DNSフットプリント
D. 社会工学
Answer: B (メーッセージを残す)

最新問題: **184**
IDSとIPSを回避するために使用された方法は次のうちどれですか？
A. 断片化
B. TNP
C. HTTP
D. SNMP
Answer: (解答を表示する)
フラグメンテーションは、攻撃者が侵入検知システム（IDS）や侵入防御システム（IPS）による検知を回避するために用いる手法です。パケットをより小さな断片に分割することで、攻撃者はこれらのセキュリティシステムが悪意のあるペイロードや既知の攻撃に関連付けられたシグネチャベースのパターンを検知することをより困難にすることができます。この手法は、一部のIDS/IPSソリューションが分析のためにパケット断片を適切に再構成できないという事実を悪用し、悪意のある断片が検知されずに通過することを可能にしています。

参考資料: ECIH v3 認証では、ネットワーク セキュリティ メカニズムと回避技術に関する説明の中で、攻撃者がパケット断片化の使用を含め、IDS および IPS システムの実装における脆弱性をどのように悪用するかを詳しく説明しています。

最新問題: **185**
SWA Cloud Servicesは、クラウドセキュリティ対策の一つとしてPKIを追加しました。PKIとは何でしょうか？
A. 公開鍵情報
B. 私のライオンのためのプライベートキー
C. 秘密鍵インフラストラクチャ
D. 公開鍵基盤
Answer: D (メーッセージを残す**)**

最新問題: **186**
グローバルeコマース企業であるDeltaCorpは、CEOを名乗る人物から緊急の資金送金を求めるメールを財務部門に受け取った。この潜在的に詐欺的なメールの正当性を判断するために、調査の主な焦点となるべき事項は次のうちどれか？
A. メールヘッダーを調べて、なりすましや送信者のIPアドレスの異常がないか確認してください。
B. メールに記載されているベンダーに連絡してください。
C. 過去のメールをレビューして、類似の表現を探します。
D. メールサーバーをマルウェアスキャンします。
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
ECIHのメールインシデント対応ガイドラインでは、なりすましやなりすまし攻撃が疑われる場合の主要な検証手法として、メールヘッダー分析を重視しています。
選択肢Aが正解です。ヘッダーには送信者のIPアドレス、ルーティングパス、認証結果（SPF、DKIM、DMARC）が記録されているため、メールが正当な送信元から送信されたものかどうかを直接確認できます。
選択肢B、C、Dは補足的な措置であり、正式な検証を提供するものではありません。

最新問題: **187**
世界的な医療サービスプロバイダーであるメガヘルス社は、MRI装置に突然の不具合が発生した。
調査の結果、MRI検査結果を改ざんし、外部のコマンド＆コントロールサーバーと通信するマルウェアが発見された。高度なエンドポイント保護システムやネットワークモニターといったツールを活用する場合、最初にとるべき対策は何だろうか？
A. 患者にデータ侵害の可能性について知らせる。
B. ネットワークモニターを使用して、C&Cサーバーとの通信を特定し、ブロックします。
C. MRI装置のファームウェアとソフトウェアを更新します。

D. MRI装置にエンドポイント保護を導入して、マルウェアを検出して停止します。
Answer: (解答を表示する**)**
今回の事案は、医療機器にマルウェアが積極的に影響を与え、患者の安全を脅かす事態です。ECIHのマルウェア事案対応原則によれば、最優先事項はエンドポイントレベルでの封じ込めと駆除です。
選択肢Dが正解です。エンドポイント保護を導入することで、MRI装置上でマルウェアの実行を直接検知して停止させることができ、結果の改ざんやさらなる悪意のある活動を阻止できます。ネットワークレベルや復旧措置の前に、エンドポイントの封じ込めは不可欠です。
オプションBは通信に関する事項を扱いますが、ローカル操作を阻止するものではありません。オプションCは、封じ込め措置なしにシステム状態を変更します。オプションAは、バリデーションに続く規制上のステップです。
ECIHは、重要インフラおよび医療環境においては、安全性とデータ完全性を保護するために、エンドポイントの即時封じ込めが不可欠であることを強調している。

最新問題**: 188**
無線ネットワーク管理者であるエラは、複数の認証失敗と、ユーザーが社内Wi-Fiネットワークから切断されたという報告に気づきました。調査の結果、正規のネットワークと同じSSIDをブロードキャストしている不正なアクセスポイントを特定しました。エラが直面している可能性が最も高い問題は何でしょうか？
A. 邪悪な双子の攻撃
B. ネットワーク設定ミス
C. MACアドレスの偽装
D. 不正なDHCPサーバー
Answer: A (メーッセージを残す**)**
包括的かつ詳細な説明（ECIH準拠）：
このシナリオでは、ECIHのネットワークセキュリティインシデントモジュールで取り上げられている、よく知られた無線ネットワークの脅威である「イービルツイン攻撃」について説明します。イービルツイン攻撃は、攻撃者が正規のネットワークのSSIDを模倣した不正な無線アクセスポイントを設置することで発生します。何も知らないユーザーは、より強力な信号やアクセスしやすい信号に接続してしまうため、攻撃者は認証情報を傍受したり、マルウェアを注入したり、中間者攻撃を実行したりすることが可能になります。
選択肢Aが正解です。なぜなら、同じSSIDを発信する不正なアクセスポイントが存在し、認証エラーを引き起こすことは、悪意のあるツイン攻撃の決定的な兆候だからです。ユーザーは知らず知らずのうちに悪意のあるアクセスポイントに接続してしまい、正規のネットワークから繰り返し切断される可能性があります。
オプションBは不正アクセスポイントとは関係ありません。オプションCはMAC層でのIDなりすましに焦点を当てていますが、SSIDの重複については説明していません。オプショ

ンDはIPアドレス割り当ての問題に関するもので、SSIDのなりすましとは関係ありません。
ECIHは、不正な無線インフラを迅速に特定することが、被害拡大の封じ込めに不可欠であることを強調しています。悪意のあるツイン攻撃を検出することで、対応者は不正デバイスを隔離し、認証情報を保護し、安全な無線運用を復旧させることができます。

最新問題: **189**
大量のトラフィックをネットワークに送り込み、既存のネットワークリソースをすべて消費させることで、本来のユーザーまたは承認されたユーザーがシステム、ネットワーク、またはアプリケーションを使用できなくなるようなネットワークセキュリティインシデントを特定する。
A. XSS攻撃
B. サービス拒否
C. URL操作
D. SQLインジェクション
Answer: B (メーッセージを残す**)**
サービス拒否（DoS）攻撃は、大量のトラフィックをネットワークに送り込み、利用可能なネットワークリソースをすべて消費することで、本来アクセス権限を持つユーザーや正規ユーザーがシステム、ネットワーク、アプリケーションにアクセスできないようにする攻撃です。この種の攻撃は、ターゲットの受信リクエスト処理能力を圧倒し、正規ユーザーのアクセスを拒否することを目的としています。Webアプリケーションの脆弱性を悪用して不正なデータアクセスやデータ操作を行うXSS（クロスサイトスクリプティング）攻撃、URL操作、SQLインジェクションとは異なり、DoS攻撃はサービスの可用性を標的としています。
参考資料 :インシデントハンドラー（ECIH v3）コースと学習ガイドでは、サービス拒否攻撃を含むさまざまな種類のネットワークセキュリティインシデントを取り上げ、ネットワークリソースとサービスへの影響を詳しく説明しています。

最新問題: **190**
次のエンコード技術のうち、通常とは異なるASCII文字を
「%」の後に、その文字の2桁のASCIIコードを16進数で表したものが続きますか？
A. Base64エンコーディング
B. Unicodeエンコーディング
C. HTMLエンコーディング
D. URLエンコーディング
Answer: D (メーッセージを残す**)**

最新問題: **191**
オーティスはデルモントという組織でインシデント対応担当者として働いています。最近、デルモントは事業上のいくつかの問題に直面し、収益が減少しています。オーティスは

この問題の調査を任されました。彼は企業セキュリティの監査中に、企業ネットワークから機密情報が盗まれ、競合他社に渡された攻撃の痕跡を発見しました。デルモントが直面した情報セキュリティインシデントは次のうちどれでしょうか？
A. ネットワークとリソースの乱用
B. スパイ活動
C. メールによる嫌がらせ
D. 不正アクセス
Answer: B (メーッセージを残す**)**
情報セキュリティインシデントの文脈におけるスパイ行為とは、競争上の優位性を得るために、機密情報への不正アクセスや窃盗を行うことを指します。今回説明したシナリオでは、デルモント社の企業ネットワークから機密情報が盗まれ、競合他社に渡されたため、これはまさにスパイ行為の定義に合致しています。このインシデントは、機密性の高いビジネス情報を意図的に標的にして抽出したものであり、競合他社はそれを市場優位性を得るために利用しています。このような行為は、ビジネス上重要な情報の機密性を損なうだけでなく、被害を受けた組織の財務安定性や競争力にも重大な影響を与える可能性があります。
参考資料：EC-Councilによる認定インシデントハンドラー（ECIH v3）カリキュラムでは、スパイ行為を含むさまざまな情報セキュリティインシデントについて議論し、そのような脅威から保護し対応するための包括的なセキュリティ対策、インシデント検出機能、効果的な対応戦略の必要性を強調しています。