

EC-COUNCIL.212-89.v2024-05-16.q153

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:	153
バージョン:	v2024-05-16
アクセス数:	866
ページビュー数:	1530
https://www.jpnpdf.com/EC-COUNCIL.212-89.v2024-05-16.q153-mondaishu.html	

最新問題: 1

悪意のある内部アクターまたは侵害されたアクターを検出するために使用される一般的なツールは次のうちどれですか？

- A. SOC2 準拠レポート
- B. ユーザー行動分析
- C. ログ転送
- D. Syslog 設定

Answer: B ([メッセージを残す](#))

最新問題: 2

多くの業界や教育機関で利用できる、無料のオープンソースの TCP/IP プロトコル アナライザー、スニファー、パケット キャプチャ ユーティリティ標準は、次のように知られています。

- A. 鼻を鳴らす
- B. Wireshark
- C. nmap
- D. カインとアベル

Answer: ([解答を表示する](#))

最新問題: 3

ホストは、脆弱なサービスを通じて伝播するワームに感染します。ワームの存在の兆候には次のようなものがあります。

- A. ネットワーク使用量の減少
- B. 上記すべて
- C. システムが不安定になるかクラッシュする
- D. 脆弱なサービスを対象とした確立された接続試行

Answer: ([解答を表示する](#))

最新問題: 4

オープンソースの TCP/IP ネットワーク侵入防御および検出システム (IDS/IPS) は、ルール駆動型の

言語を使用してリアルタイムのトラフィック分析を実行し、パケット ロギングは次のように知られています。

- A. 鼻息
- B. Wireshark
- C. ネスス
- D. 聖人

Answer: A ([メッセージを残す](#))

説明

最新問題: 5

フレデリックは、担当している事件の 1 つで撲滅プロセスを進めています。

根絶プロセスではないものは次のうちどれですか？

- A. クラウド プロバイダー インターフェイスのセキュリティ モデルを分析します。
- B. 脆弱性スキャンと構成監査を実施します。
- C. CC は、クラウドを安全に使用できるように数人の従業員をトレーニングする必要があります。
- D. クライアントのトラフィックを監視して、悪意のあるアクティビティがないか確認します。

Answer: C ([メッセージを残す](#))

最新問題: 6

内部関係者は企業のビジネス機能を理解しています。によって実行されるアクティビティの正しい順序は何ですか？

内部関係者による会社資産への損害:

- A. 特権アクセスを取得し、マルウェアをインストールしてアクティブ化します
- B. 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します
- C. 特権アクセスを取得し、マルウェアをアクティブ化してインストールします
- D. マルウェアをインストールし、特権アクセスを取得してアクティブ化します

Answer: ([解答を表示する](#))

最新問題: 7

インシデント発生後にコンピュータ システムを回復する手順は次のとおりです。

- A. システムの検証、復旧、運用および監視
- B. システムの監視、検証、操作、および復元
- C. システムの復元、検証、運用および監視

D. システムの復元、運用、検証、監視

Answer: C ([メッセージを残す](#))

最新問題: 8

チャンドラーは、Technote と呼ばれる組織をターゲットとするプロのハッカーです。彼は、異なる階層間で送信され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、ネットワークを介して送信されたデータ パケットを傍受し、それらを分析して、ネットワーク、ポート、プロトコル、デバイス、ネットワーク送信の問題、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できるツールは次のうちどれですか？

A. BeEf

B. IDA プロ

C. オムニ ピーク

D. シャープ

Answer: D ([メッセージを残す](#))

最新問題: 9

リスク管理は、リスク評価、リスク軽減、評価の 3 つのプロセスから構成されます。リスク評価では、SDLC を通じて IT システムに関連する潜在的な脅威とリスクの範囲を決定します。NIST のリスク評価方法論には、主なステップがいくつ含まれていますか？

A. 9

B. 12

C. 4

D. 6

Answer: A ([メッセージを残す](#))

最新問題: 10

インシデント管理チームは、脅威または攻撃の影響を受ける組織内のすべてのユーザーにサポートを提供します。組織の内部監査人はインシデント対応チームの一員です。インシデント対応チームの一員としての内部監査人の責任の 1 つを特定します。

A. 情報セキュリティ担当者とインシデント封じ込め活動を調整します。

B. セキュリティの抜け穴を特定し、必要な措置を講じるため管理者に報告します。

C. 情報セキュリティ管理の構成

D. 侵入者と思われる者からのネットワーク トラフィックをブロックするために必要なアクションを実行します。

Answer: B ([メッセージを残す](#))

最新問題: 11

組織リソースの保護と追跡のための制御を推奨するポリシーは次のとおりです。

A. アクセス制御ポリシー

- B. 管理セキュリティ ポリシー
- C. 利用規約
- D. 資産管理ポリシー

Answer: ([解答を表示する](#))

説明/参照:

最新問題: 12

商業的価値があり、著作権と商標を含む知的成果物は次のように呼ばれます。

- A. ロゴ
- B. 営業秘密
- C. 特許
- D. 知的財産

Answer: D ([メッセージを残す](#))

最新問題: 13

James はプロのハッカーで、クラウド サービスを悪用するために組織に雇われています。これを達成するために、James はクラウド サービスへの匿名アクセスを作成し、パスワードやキーのクラッキング、悪意のあるデータのホスト、DDoS 攻撃などの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与えている脅威は次のうちどれですか？

- A. デューデリジェンスが不十分です
- B. クラウド サービスの悪用および不正使用
- C. データ侵害/損失
- D. 安全でないインターフェースと API

Answer: ([解答を表示する](#))

最新問題: 14

アリスは不満を持った従業員です。彼女は、経済的利益を得るために、組織から重要な情報を入手することにしました。

これを達成するために、アリスは被害者の仮想マシンと同じ物理ホスト上で仮想マシンの実行を開始し、共有物理リソース (プロセッサ キャッシュ) を利用して被害者マシンからデータ (暗号キー/平文の秘密) を盗みました。上記のシナリオでアリスが実行している攻撃の種類を特定します。

- A. サイドチャネル攻撃
- B. クラウド内マン攻撃
- C. SQL インジェクション攻撃
- D. サービスハイジャック

Answer: A ([メッセージを残す](#))

最新問題: 15

適切なテクノロジーを適用し、インシデントの根絶と回復を試みる役割は、次のように呼ばれます。

- A. インシデント マネージャー
- B. インシデント分析者
- C. インシデントコーディネーター
- D. インシデントハンドラー

Answer: B ([メッセージを残す](#))

最新問題: 16

ユーザーが正しくログアウトできなかったときにブラウザーがセッションを期限切れにしない場合、次の OWASP トップ 10 Web 脆弱性のどれが原因ですか？

- A. A2: 認証が失敗しました
- B. A3: 機密データの漏洩
- C. A5: アクセス制御が壊れています
- D. A7: クロスサイト スクリプティング

Answer: ([解答を表示する](#)**)**

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード:

Freepdfdumps)

最新問題: 17

デジタル フォレンジック分析ツールではないものは次のうちどれですか:

- A. アクセス データ FTK
- B. EAR/ピラール
- C. らせん
- D. ガイダンス ソフトウェア EnCase Forensic

Answer: B ([メッセージを残す](#))

最新問題: 18

非常によく知られた無料のオープン ソース ポート、OS、サービス スキャナー、およびネットワーク検出ユーティリティは次のように呼ばれます。

- A. 聖人
- B. Wireshark
- C. 鼻息

D. Nmap (ネットワーク マッパー)

Answer: D ([メッセージを残す](#))

最新問題: 19

コンピュータ フォレンジックのタイプではないものは次のうちどれですか:

- A. 画像フォレンジック
- B. USB フォレンジック
- C. 電子メールフォレンジック
- D. 法医学考古学

Answer: D ([メッセージを残す](#))

最新問題: 20

コンピュータ ファイルに感染し、ファイル内のデータを破損または削除し、ホスト ファイルを必要とするマルウェア コード。

伝播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

Answer: D ([メッセージを残す](#))

最新問題: 21

電子メールを使用した悪意のあるコード攻撃は次のようにみなされます。

- A. 不適切な使用事件
- B. 複数コンポーネント攻撃
- C. マルウェアベースの攻撃
- D. 電子メール攻撃

Answer: ([解答を表示する](#))

最新問題: 22

IDS および IPS を回避するために使用されたものは次のうちどれですか?

- A. TNP
- B. SNMP
- C. 断片化
- D. HTTP

Answer: C ([メッセージを残す](#))

最新問題: 23

IDS および IPS システム ログは、典型的なネットワーク トラフィック フローからの異常な逸脱を示します。これは次のように呼ばれます:

- A. プロアクティブ
- B. 前駆体
- C. リアクティブ
- D. 指示

Answer: ([解答を表示する](#))

最新問題: 24

ライアンは、ファイルを分析しているときに、攻撃者が画像ファイル内に隠しメッセージを埋め込むというアンチフォレンジック手法を使用していることを発見しました。これはどのような種類の方法ですか？

- A. パスワード保護
- B. ステガノグラフィー
- C. ゴールデン チケット
- D. プログラムパッカー

Answer: ([解答を表示する](#))

最新問題: 25

インサイダー リスク マトリックスは、技術リテラシーとビジネス プロセスの知識ベクトルで構成されます。マトリックスを考慮すると、次のように結論付けることができます。

- A. 内部関係者の技術リテラシーが低く、プロセスに関する知識が高い場合、脅威によってもたらされるリスクはわずかです。
- B. 内部関係者の技術リテラシーとプロセス知識が高い場合、脅威によってもたらされるリスクはわずかです。
- C. 内部関係者の技術リテラシーが高く、プロセスの知識が低い場合、脅威によってもたらされるリスクは高くなります。
- D. 内部関係者の技術リテラシーとプロセス知識が高い場合、脅威によってもたらされるリスクは高くなります。

Answer: D ([メッセージを残す](#))

最新問題: 26

同僚は、小規模な組織に所属しているため、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。彼らは、さまざまな形で提供される新しいアプリケーションを評価しています。

どのような形で同僚に対する責任が最も少なくなるのでしょうか？

- A. オンプレミスのインストール
- B. SaaS
- C. PaaS
- D. IaaS

Answer: B ([メッセージを残す](#))

最新問題: 27

アダムは、10,000 ドル相当のデータを保護するための制御の総コストを 20,000 ドルと計算しました。アダムに何をするようにアドバイスしますか？

- A. コントロールを適用します
- B. 代わりに半定性的なリスク評価を使用します
- C. コントロールを適用しない
- D. 定性的リスク評価を使用する

Answer: C ([メッセージを残す](#))

最新問題: 28

証拠袋に含まれる詳細は次のうちどれですか？

- A. 機密ディレクトリ、個人および組織の電子メール アドレス
- B. ソフトウェアのバージョン情報と Web アプリケーションのソース コード
- C. 機密情報を含むエラー メッセージとパスワードを含むファイル
- D. 押収日時、証拠番号、事件対応者の名前

Answer: D ([メッセージを残す](#))

最新問題: 29

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. クラウド回復
- B. 軽減策
- C. 分析
- D. 根絶

Answer: A ([メッセージを残す](#))

最新問題: 30

オーティスは、デルモントの組織で働くインシデントハンドラーです。最近、この組織は事業でいくつかの挫折に直面しており、それにより収益が減少しています。オーティスは責任をとってこの問題を調査するよう頼まれた。企業のセキュリティを監査しているときに、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。

デルモントの組織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. ネットワークとリソースの不正使用
- B. 電子メールベースの不正行為
- C. 不正アクセス
- D. スパイ活動

Answer: D ([メッセージを残す](#))

最新問題: 31

マルウェアがシステムから削除され、クリーンなスキャンが返された後、影響を受けるデバイスに対して次のどの手順を実行する必要がありますか？

- A. 箱に密封し、90 日間保管する必要があります。
- B. 再イメージ化する必要があります
- C. 運用環境に配置する前に、マルウェアが確実に削除されるように、レビューのために監視環境に配置する必要があります。
- D. 更新された情報を取得するには、イーサネット経由でドメイン コントローラーに接続する必要があります

Answer: C ([メッセージを残す](#))

有効な 212-89 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の 212-89 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (30530%OFF問題集溶と正解付きで 30%w 特別割引コード:

Freepdfdumps)

最新問題: 32

最近の電子メール攻撃の後、ハリーは重要な情報を入手するために事件を分析しています。彼は事件を調査する際に、送信者の身元、メール サーバー、送信者の IP アドレス、場所などの情報を抽出しようとしています。

ハリーがこのタスクを実行するには、次のツールのうちどれを使用する必要がありますか？

- A. クラムウィン
- B. シャープ
- C. ログリー
- D. はい、わかります

Answer: D ([メッセージを残す](#))

最新問題: 33

オーティスはデルモントという組織で働くインシデントハンドラーです。最近、この組織は事業面でいくつかの挫折に直面し、それにより収益が減少しています。オーティスは責任をとってこの問題を調査するよう頼まれた。企業のセキュリティを監査しているときに、彼は企業ネットワークから機密情報が盗まれ、競合他社に渡される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関連の事件は次のうちどれですか？

- A. スパイ活動
- B. 電子メールベースの不正行為

- C. 不正アクセス
- D. ネットワークとリソースの不正使用

Answer: A ([メッセージを残す](#))

最新問題: 34

NIST のリスク評価手法の統制分析段階では、技術的管理手法と非技術的管理手法が 2 つのカテゴリに分類されます。これら 2 つのコントロール カテゴリとは何ですか？

- A. 予防および予測制御
- B. 探偵および偽装コントロール
- C. 予測および検出コントロール
- D. 予防および検出制御

Answer: D ([メッセージを残す](#))

最新問題: 35

地域社会で緊急事態に対応できるよう人々を訓練するプログラムは、次のように知られています。

- A. インシデント対応チーム (IRT)
- B. セキュリティ インシデント対応チーム (SIRT)
- C. 上記すべて
- D. コミュニティ緊急対応チーム (CERT)

Answer: ([解答を表示する](#))

最新問題: 36

現在の従業員の専門知識が非常に低い場合、インシデント対応チームに最適な人員配置モデルは何ですか？

- A. 上記すべて
- B. 完全に内製化
- C. 完全にアウトソーシング
- D. 部分的に外部委託

Answer: ([解答を表示する](#))

最新問題: 37

静的データ収集プロセスの一部ではないものは次のうちどれですか？

- A. 証拠の取得
- B. パスワード保護
- C. システムの保存
- D. 証拠調べ

Answer: B ([メッセージを残す](#))

最新問題: 38

Tibs on は、シンガポールに拠点を置く多国籍企業のインシデント対応者として働いています。彼は、会社が最近直面した Web アプリケーションのセキュリティ インシデントを調査しています。この攻撃は、同社がホストする MSSQL サーバー上で実行されます。検出および分析フェーズでは、正規表現を使用して、SQL インジェクション攻撃につながる SQL メタキャラクターを分析および検出しました。MSSQL サーバーに対する SQL インジェクション攻撃を検出するために Tibs によって使用される正規表現を特定します。

- A. ((\AW)(\AV))
- B. ((\.1%2E)\.1%2E)(V%2FN|%5C))
- C. ((\%3C) <) (\%2F) /) *(スクリプト) (\%3E) >)
- D. /exec(\s|\\+) +(s|x) p\\w+/ix

Answer: ([解答を表示する](#))

最新問題: 39

脆弱性評価フェーズでは、インシデント対応者は次のようなさまざま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. 脆弱性を特定して優先順位を付ける
3. 物理的セキュリティの調査と評価
4. OSINT 情報収集を実行して脆弱性を検証します。
5. ビジネスおよびテクノロジーのコンテキストをスキャナーの結果に適用する
6. 設定ミスや人的エラーがないか確認する
7. 脆弱性スキャンレポートを作成する

インシデント対応者が実行する脆弱性評価手順の正しい順序を特定します。

- A. 1-->3-->2->4->5->6-->7
- B. 2-->1-->4->7->5->6-->3
- C. 4-->1-->2->3->6->5-->7
- D. 3-->6-->1->2->5->4-->7

Answer: D ([メッセージを残す](#))

最新問題: 40

ジェイソンはコンピューターフォレンジックラボを立ち上げており、次の手順を実行する必要があります。

1. 物理的な位置と構造設計の考慮事項。
2. 計画と予算編成。
3. 作業エリアに関する考慮事項。
4. 物理的セキュリティに関する推奨事項。
5. 法医学研究所のライセンス;
6. 人的資源の考慮事項。

これらのステップを実行順序に並べてください。

- A. 5->2->1->3->4->6

B. 2->1->3->6->4->5

C. 3->2->1->4->6->5

D. 2->3->1->4->6->5

Answer: B ([メッセージを残す](#))

最新問題: 41

インシデント対応プロセス中に、インシデント対応担当者がファイル システムの表示、削除されたデータの取得、タイムライン分析、Web アートの事実などを実行するのに役立つツールは次のどれですか？

A. netstat

B. プロセス エクスプローラー

C. nbtstat

D. 解剖

Answer: D ([メッセージを残す](#))

最新問題: 42

あなたの会社は SaaS を販売しており、会社自体はクラウドでホストされています (PaaS として使用)。

顧客のデータベースでマルウェア インシデントが発生した場合、悪意のあるソフトウェアを根絶する責任は誰にありますか？

A. 顧客

B. ビル管理

C. PaaS プロバイダー

D. あなたの会社

Answer: ([解答を表示する](#))

最新問題: 43

受信した、緊急のアクションが必要で、受信者に特定のファイルを削除するか、他のファイルに転送するように促すメッセージは、次のように呼ばれます。

A. スピアフィッシング

B. メール爆弾

C. アドウェア

D. ウイルスのデマ

Answer: D ([メッセージを残す](#))

最新問題: 44

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、および入力として raw ディスク デバイスが与えられた場合にディスク イメージング ツールとして使用される Linux コマンドは次のとおりです。

A. 検索」コマンド

- B. `fiestat` コマンド
- C. `fslookup` コマンド
- D. `fd` コマンド

Answer: D ([メッセージを残す](#))

最新問題: 45

スミス氏は、オーストラリアにいくつかの支店を持つ小規模金融企業の主任インシデント対応担当者です。最近、同社は大規模な攻撃を受け、銀行間システムを通じて 500 万ドルの損失を被りました。詳細な調査の結果、攻撃者が 6 か月前に軽微な脆弱性を介してネットワークに侵入し、アクセスを維持したために事件が発生したことが判明しました。任意のユーザーによって検出されます。次に、彼らはユーザーの指紋を削除しようとし、銀行間システムで特権を持つ人物のコンピュータへの横移動を実行しました。攻撃者は最終的にアクセスを獲得し、不正な取引を実行しました。

上記のシナリオで、攻撃の種類を最も正確に説明しているものは次のうちどれですか？

- A. サービス拒否攻撃
- B. ランサムウェア攻撃
- C. フィッシング
- D. APT 攻撃

Answer: D ([メッセージを残す](#))

最新問題: 46

コンピュータに感染し、コンピュータ上のデータを破壊または削除する悪意のあるソフトウェア プログラムは次のうちどれですか？

- A. スパイウェア
- B. ウイルス
- C. トロイの木馬
- D. ワーム

Answer: B ([メッセージを残す](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 47

インシデントの優先順位付けは、以下に基づいて行う必要があります。

- A. 潜在的な影響
- B. 影響を受けるシステムの重要度
- C. 現在のダメージ
- D. 上記すべて

Answer: ([解答を表示する](#))

最新問題: 48

NIST のリスク評価/方法論において、IT システムの境界を特定するプロセス。
システムを構成するリソースと情報は次のように呼ばれます。

- A. 資産評価
- B. 資産の識別
- C. システム分類
- D. システムの特性評価

Answer: ([解答を表示する](#))

最新問題: 49

デジタル証拠は、サイバー犯罪者の訴追において重要な役割を果たします。ジョンはサイバー犯罪捜査官で、児童ポルノ事件の捜査を依頼されました。問題の犯人のパソコンは郡警察によって押収された。次の証拠のうちどれがジョンの捜査を導くものでしょうか？

- A. Web ブラウザの履歴
- B. Web サーバーのログ
- C. ルーティング テーブルのリスト
- D. SAM ファイル

Answer: A ([メッセージを残す](#))

最新問題: 50

スミス氏は、オーストラリアにいくつかの支店を持つ小規模金融企業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大規模な攻撃を受け、500 万ドルを失いました。

詳細な調査の結果、このインシデントは、6 か月前に攻撃者が軽微な脆弱性を介してネットワークに侵入し、ユーザーが気づかないうちにアクセスを維持したために発生したことが判明しました。次に、彼らはユーザーの指紋を削除しようとし、銀行間システムで特権を持つ人物のコンピュータへの横移動を実行しました。攻撃者は最終的にアクセスを取得し、不正な取引を実行しました。

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ます。

- A. フィッシング
- B. APT 攻撃
- C. サービス拒否攻撃
- D. ランサムウェア攻撃

Answer: B ([メッセージを残す](#))

最新問題: 51

ネットワークフォレンジックツールではないものは次のうちどれですか？

- A. ワイヤーシャーク
- B. Tcpdump
- C. 高度な NTFS ジャーナリング パーサー
- D. ネットワーク アナライザを制限します

Answer: C ([メッセージを残す](#))

最新問題: 52

プログラムの実行中に広告バナーが表示され、以下の内容を提供するソフトウェア アプリケーション。

コンピュータ画面またはブラウザ上に表示されるポップアップ ウィンドウまたは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 (すべて小文字で綴られます)

Answer: E ([メッセージを残す](#))

最新問題: 53

コンピューター ファイルに感染し、ファイル内のデータを破損または削除し、伝播するにはホスト ファイルを必要とするマルウェア コードは次のように呼ばれます。

- A. トロイの木馬
- B. ルートキット
- C. ワーム
- D. ウイルス

Answer: ([解答を表示する](#))

最新問題: 54

Rose はインシデントハンドラーであり、悪意のある攻撃者によるネットワーク上のあらゆる種類のスキャンの試みを検出して排除する責任があります。ローズは Wire shark を使用してネットワークを盗聴し、進行中の悪意のあるアクティビティを検出します。

次の Wireshark フィルタのうち、攻撃者による TCP クリスマス スキャンの試みを検出するために使用できるものはどれですか？

- A. tcp.dstport== 7
- B. tcp.flags.reset== 1
- C. tcp.flags==0X 000
- D. tcp.flags==0X 029

Answer: D ([メッセージを残す](#))

最新問題: 55

セキュリティ インシデントを効果的に説明するには、共通の用語セットを採用し、インシデントを分類する必要があります。

ECIH の文書によると、疑わしいユーザーまたは未知のユーザーによる違法なファイルのダウンロードに関わるインシデントはどのカテゴリに分類されますか？

- A. 高レベル
- B. 超高レベル
- C. 低レベル
- D. 中レベル

Answer: A ([メッセージを残す](#))

最新問題: 56

インシデント対応の目標は、被害を最小限に抑え、復旧時間とコストを削減する方法でインシデントに対処することです。インシデント対応の目標を構成しないものは次のうちどれですか？

- A. インシデント処理中に収集した情報を使用して、将来のインシデントをより適切に処理するための準備をし、システムとデータをより強力に保護します。
- B. 個人がセキュリティ インシデントから迅速かつ効率的に回復できるように支援し、紛失や盗難、サービスの中断を最小限に抑えます。
- C. 事件中に発生する可能性のある法的問題に適切に対処します。
- D. 人事部門および従業員のさまざまな対立行動に対処します。

Answer: ([解答を表示する](#))

最新問題: 57

Darwin は組織内の攻撃者であり、システムをプロミスキャス モードで実行してネットワーク スニффイングを実行しています。彼は、組織内で送信されるすべてのネットワーク パケットをキャプチャして表示しています。エドウィンは同じ組織のインシデントハンדרラーです。

上記の状況で、プロミスキャス モードで実行されている Darwin のシステムを検出するために Edwin が使用する必要がある Nmap コマンドは次のうちどれですか？

- A. nmap --script=sniffer-detect [ターゲット IP アドレス/IP アドレスの範囲]
- B. nmap -sU -p 500
- C. nmap --script ホスト マップ
- D. nmap -sV -T4 -O -F -version-light

Answer: A ([メッセージを残す](#))

最新問題: 58

プロのハッカーであるクラークは、フォームとパラメータ値を改ざんすることで、ターゲット組織の Web アプリケーションを悪用することに成功しました。その結果、クラークは組織の情報資産にアクセスできるようになりました。

攻撃者によって悪用された Web アプリケーションの脆弱性は次のうちどれですか？

- A. 壊れたアクセス制御
- B. 機密データの漏洩
- C. セキュリティの構成ミス
- D. SQL インジェクション

Answer: D (メッセージを残す)

最新問題: 59

アリスはインシデントハンドラーであり、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回復できるように、影響を受けるシステム上のデータをバックアップする必要があると彼女のリーダーから知らされました。また、システムのバックアップは事件のさらなる調査にも使用できるとも言われました。

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、Alice は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. 根絶
- B. 封じ込め
- C. 事件の記録
- D. インシデントのトリアージ

Answer: C (メッセージを残す)

最新問題: 60

本物の無害なプログラムとして隠蔽され、攻撃者にユーザー情報とシステムへの無制限のアクセスを与える悪意のあるプログラムを特定します。これらのプログラムは、無防備なユーザーのディスクを消去し、被害者のクレジットカード番号とパスワードを見知らぬ人に送信する危険なプログラムを実行する可能性があります。

- A. ウイルス
- B. ワーム
- C. アドウェア
- D. トロイの木馬

Answer: D (メッセージを残す)

最新問題: 61

インシデント対応に関する最新の NIST 標準は何ですか？

- A. 800-53r3
- B. 800-171r2
- C. 800-61r2
- D. 800-61r3

Answer: ([解答を表示する](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 62

複数コンポーネントのインシデントは、システム内の 2 つ以上の攻撃の組み合わせで構成されます。

次のうち、複数の要素が関係するインシデントではないものはどれですか？

- A. 悪意のあるコードを含む電子メールを使用して内部ワークステーションに感染する攻撃者
- B. 攻撃者がマシンに感染して DDoS 攻撃を開始する
- C. 攻撃者はユーザーを悪意のある Web サイトにリダイレクトし、ユーザーのシステムをトロイの木馬に感染させます。
- D. 内部関係者がワークステーションからファイルを意図的に削除

Answer: D ([メッセージを残す](#))

最新問題: 63

マットは、マルウェアの影響を受けた最大手のソーシャル ネットワーク会社の 1 つで働くインシデント ハンドラーです。同社の報告期間ガイドラインによれば、マルウェア インシデント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. カテゴリー 2
- B. カテゴリー 1
- C. カテゴリー 4
- D. カテゴリー 3

Answer: D ([メッセージを残す](#))

最新問題: 64

複数コンポーネントのインシデントは、システム内の 2 つ以上の攻撃の組み合わせで構成されます。次のうち、複数の要素が関係するインシデントではないものはどれですか？

- A. 攻撃者がマシンに感染して DDoS 攻撃を開始する
- B. 攻撃者はユーザーを悪意のある Web サイトにリダイレクトし、ユーザーのシステムをトロイの木馬に感染させます。

C. 悪意のあるコードを含む電子メールを使用して内部ワークステーションに感染する攻撃者

D. 内部関係者がワークステーションからファイルを意図的に削除

Answer: D ([メッセージを残す](#))

最新問題: 65

インシデント対応における各段階の流れの正しい順序は次のうちどれですか:

A. 根絶 - 封じ込め - 特定 - 準備 - 回収 - フォローアップ

B. 封じ込め - 特定 - 準備 - 回収 - フォローアップ - 根絶

C. 特定 - 準備 - 封じ込め - 回収 - 追跡調査 - 根絶

D. 準備 - 特定 - 封じ込め - 根絶 - 回収 - 追跡調査

Answer: D ([メッセージを残す](#))

最新問題: 66

多国籍企業の従業員である ADAM は、会社のアカウントを使用して、なりすましたメールアドレスを使用して第三者に電子メールを送信します。このタイプのアカウントをどのように分類できますか?

A. ネットワーク侵入インシデント

B. 不正アクセス事件

C. サービス拒否インシデント

D. 不適切な使用事件

Answer: ([解答を表示する](#))

最新問題: 67

PGP Desktop Email が提供する主な機能は次のとおりです。

A. インシデント時の電子メール サービス

B. 上記のどれもでない

C. エンドツーエンドの安全な電子メール サービス

D. エンドツーエンドの電子メール通信

Answer: C ([メッセージを残す](#))

最新問題: 68

インシデント管理プロセスの正しい順序は次のとおりです。

A. 準備、保護、トリアージ、検出、対応

B. 準備、検出、保護、優先順位付け、対応

C. 準備、保護、検出、優先順位付け、対応

D. 準備、保護、検出、対応、優先順位付け

Answer: C ([メッセージを残す](#))

最新問題: 69

Sam Morson Inc. という組織は、メンテナンスのコストを削減するためにクラウドベースのサービスを使用することにしました。彼らはまず、クラウド サービスの導入と重要なビジネス データのサードパーティ システムへの移行に関連するさまざまなリスクと脅威を特定しました。そこで組織は、今後の脅威を防ぐためにクラウドベースのセキュリティ ツールを導入することにしました。

組織がクラウド リソースとサービスを保護するのに役立つツールは次のうちどれですか？

- A. ワイヤーシャーケ
- B. Nmap
- C. げっぷスイート
- D. アラートロジック

Answer: D ([メッセージを残す](#))

最新問題: 70

コンピューティング機器、さまざまな記憶装置、デジタル メディアから証拠を収集し、一貫した意味のある形式で法廷に提出するための系統的な一連の技術と手順は、次のように呼ばれます。

- A. フォレンジック分析
- B. フォレンジック対応
- C. コンピューターフォレンジック
- D. ステガナリシス

Answer: C ([メッセージを残す](#))

最新問題: 71

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処理担当者です。彼は、Wire shark を使用してネットワーク上の ping スイープの試行を検出したいと考えています。Bran がこのタスクを達成するために使用するのは、次の W re shark フィルターのうちどれですか？

- A. icmp.seq
- B. icmp.ident
- C. icmp.type== 8
- D. icmp.redir_gw

Answer: ([解答を表示する](#))

最新問題: 72

ジョンソンはインシデントハンドラーであり、彼の組織が最近直面した Web アプリケーション攻撃に取り組んでいます。このプロセスの一環として、彼は水飲み場攻撃を分析して検出するためにデータの前処理を実行しました。Johnson は、ファイアウォールとプロキシ サーバーから収集した送信ネットワーク トラフィック データを前処理しました。次に、特定の期間内のユーザー アクティビティの分析を開始し、時系列のドメイン シーケン

スを作成し、連続パターンについてさらに分析を実行しました。Johnson によって実行されたデータ前処理ステップを特定します。

- A. 無効なホスト名のフィルタリング
- B. ホスト名の正規化
- C. ユーザー固有のセッション化
- D. 人気のないドメインの特定

Answer: C ([メッセージを残す](#))

最新問題: 73

次のプロセスのうち、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呼ばれるものはどれですか？

- A. 脅威の評価
- B. 脆弱性管理
- C. インシデント対応オーケストレーション
- D. リスク評価

Answer: C ([メッセージを残す](#))

最新問題: 74

コンピューターフォレンジックは、あらゆるコンピューターまたはデジタルメディアデバイスから法的証拠を発見する法医学の一分野です。次のうち、取得した証拠を調査し、有用な証拠を分離する責任は誰にありますか？

- A. 証拠調査官/捜査官
- B. 証拠監督者
- C. 証拠マネージャー
- D. 証拠書類作成者

Answer: A ([メッセージを残す](#))

最新問題: 75

2001 年米国愛国者法の修正第 4 条による。検索がプライバシーに対する個人の「合理的」または「正当な」期待に違反しない場合、検索は次のようにみなされます。

- A. 合憲/合法
- B. 上記のどれもでない
- C. 非倫理的
- D. 違法/違法

Answer: A ([メッセージを残す](#))

最新問題: 76

事業継続性は、壊滅的な災害が発生した後でも組織が機能し続ける能力として定義されます。

イベントは、冗長ハードウェアとソフトウェアの導入、フォールトトレラントの使用を通じて実現されます。

システムだけでなく、確実なバックアップとリカバリ戦略も必要です。必須の部分である計画を特定する

事業継続計画？

A. 事業回復計画

B. フォレンジック手順計画

C. 販売およびマーケティング計画

D. 新規事業戦略計画

Answer: ([解答を表示する](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w**特別割引コード:

Freepdfdumps)

最新問題: 77

ドルフィン投資会社のジャコビさん社員。彼は勤務中に、自分のコンピュータがいくつかの問題に直面していることに気づき、その問題を組織内の各当局に伝えたいと考えていました。

しかし現在、この組織にはそのような種類の問題に対処する発券システムがありません。上記のシナリオでは、ドルフィン投資会社が次の発券システムのどれを使用すれば、ジェイコブが問題を提起してそれぞれのチームにインシデントについて伝えることができるでしょうか？

A. IBM XForce Exchange

B. ManageEngine ServiceDesk Plus

C. ThreatConnect

D. MISP

Answer: ([解答を表示する](#))

最新問題: 78

電子メール経由で配信されるウイルスに感染したホスト上に悪意のあるコードが存在する兆候が見られる場合、
なれ：

A. 送受信メール数の増加

B. ウイルス対策ソフトウェアが感染ファイルを検出しました

- C. システム ファイルにアクセスできなくなります
- D. 上記すべて

Answer: D ([メッセージを残す](#))

最新問題: 79

悲惨な出来事が起こった後でも機能を継続できる政府機関の能力。

冗長ハードウェアとソフトウェアの導入、フォールトトレラントシステムの使用、および
確実なバックアップ

回復戦略は次のように知られています。

- A. ビジネスの継続性
- B. 災害計画
- C. 緊急時対応計画
- D. 事業継続計画

Answer: A ([メッセージを残す](#))

最新問題: 80

キーロガー対策スキャナーに関する誤った記述はどれですか？

- A. ソフトウェア ツール
- B. ステルス モードで実行し、被害者のオンライン アクティビティを記録します。
- C. 被害者のマシンにすでにインストールされているキーロガーを検出します

Answer: ([解答を表示する](#))

最新問題: 81

内部関係者の脅威に対する次のテクニックのうち、不審なアクティビティに関連するイベントを特定するものはどれですか？

- A. パターンの検出
- B. 異常検出
- C. 相関関係
- D. 正規化

Answer: B ([メッセージを残す](#))

最新問題: 82

Khai は、Linux 電子メール サーバーからのログを調査する任務を負っていました。サーバーは Sendmail を使用してコマンドを実行して電子メールを送信し、Syslog を使用してログを維持します。

電子メール ヘッダー内のデータを検証するには、Khai は次のどのディレクトリで送信元と宛先の IP アドレス、日付、タイムスタンプなどの情報を確認する必要がありますか？

- A. /var/log/maillog
- B. /var/log/sendmail
- C. /var/log/sendmail/maillog

D. /var/log/maillog

Answer: A ([メッセージを残す](#))

最新問題: 83

SWA Cloud Services は、クラウド セキュリティ コントロールの 1 つとして PK を追加しました。

PKI とは何の略ですか？

A. 公開鍵インフラストラクチャ

B. 公開鍵情報

C. 秘密鍵インフラストラクチャ

D. 秘密鍵情報

Answer: ([解答を表示する](#)**)**

最新問題: 84

リスクは、インシデントが発生する確率として定義されます。リスクの定式化は一般に、イベントの発生の可能性、それが引き起こす可能性のある危害から始まり、通常、 $\text{リスク} = \sum(\text{イベント}) \times (\text{発生確率}) \times ?$ として表されます。

A. 結果

B. 大きさ

C. 確率

D. 重要性

Answer: B ([メッセージを残す](#))

最新問題: 85

攻撃者は攻撃を実行した後、フォレンジック調査を回避するためにアーティファクト消去技術を使用して証拠を消去することを決定しました。彼はデジタル メディア デバイスに磁場を適用し、その結果、デバイスから以前に保存されていたデータが完全に消去されました。

攻撃者が使用したアーティファクト消去手法を特定します。

A. ファイル ワイプ ユーティリティ

B. ディスク クリーニング ユーティリティ

C. Syscall プロキシ

D. ディスクの消磁/破壊

Answer: D ([メッセージを残す](#))

最新問題: 86

内部関係者による脅威は、上司や同僚との衝突、パフォーマンスの低下、遅刻や原因不明の欠勤など、内部関係者が示す行動を観察することで検出できます。内部関係者の脅威の検出に役立つ手法を選択してください。

A. 機密性とアクセス権に従って情報を分類します。

- B. 疑わしい動作と悪意のある動作の既知のパターンを相関させる
- C. 従業員は非開示契約に署名することが義務付けられています
- D. 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

Answer: B ([メッセージを残す](#))

最新問題: 87

重要なイベントをキャプチャして確認するために、どのイベント セットをログに記録する必要があるかを定義するポリシー。

タイムリーなデータは次のように知られています。

- A. 監査証跡ポリシー
- B. ロギングポリシー
- C. 証拠収集ポリシー
- D. 文書化ポリシー

Answer: ([解答を表示する](#))

最新問題: 88

企業情報資産を悪用し、資産の機密性、完全性、可用性に直接影響を与える、特権アクセスを持つ許可されたユーザーは、次のように呼ばれます。

- A. ゾンビ
- B. ソーシャル エンジニア
- C. 内部関係者の脅威
- D. 外部からの脅威

Answer: ([解答を表示する](#))

最新問題: 89

給与システムには、現在のテクノロジーでは悪用できない脆弱性があります。このシナリオについて正しいのは次のうちどれですか。

- A. リスクを早急に軽減する必要があります
- B. リスクは直ちに移転される必要があります
- C. リスクは受け入れられます
- D. 現時点ではリスクは存在しません

Answer: D ([メッセージを残す](#))

最新問題: 90

悪意のあるオフィス文書が操作されることによって引き起こされる悪意のあるダウンロードは、次のどれによって引き起こされますか？

- A. クリック ジャッキング
- B. マクロの不正使用
- C. なりすまし
- D. レジストリ キーの操作

Answer: B ([メッセージを残す](#))

最新問題: 91

曖昧な言語を使用してメッセージを理解しにくくするために攻撃者が使用するテクニックは次のうちどれですか？

- A. 難読化
- B. 暗号化
- C. ステガノグラフィー
- D. スプーフィング

Answer: A ([メッセージを残す](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 92

次のリスク軽減戦略には、リスク要因を低減して許容レベルにするための制御の実行が含まれますか、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必要がありますか？

- A. リスク計画
- B. リスク移転
- C. リスク回避
- D. リスクの想定

Answer: ([解答を表示する](#)**)**

最新問題: 93

著名な IT 組織である Zaimasoft が、ハードウェアを直接標的とした加害者による攻撃を受け、ハードウェアに回復不能な損害を与えました。結果的に、ハードウェアを交換または再インストールすることが唯一の解決策でした。Zaimasoft に対して実行されたサービス拒否攻撃の種類を特定します。

- A. DDoS
- B. DoS
- C. DRDoS
- D. PDoS

Answer: D ([メッセージを残す](#))

最新問題: 94

次のタイプの内部関係者の脅威には、潜在的なセキュリティの脅威について教育を受けていない内部関係者が関与しているもの、または職場の効率性を満たすために一般的なセキュリティ手順を単に回避しているものはどれですか？

- A. 専門の内部関係者
- B. 悪意のある内部関係者
- C. 過失のある内部関係者
- D. 侵害された内部関係者

Answer: C ([メッセージを残す](#))

最新問題: 95

最も一般的な知的財産の種類は次のとおりです。

- A. 著作権と商標
- B. 特許
- C. 工業意匠権および営業秘密
- D. 上記すべて

Answer: D ([メッセージを残す](#))

説明/参照:

最新問題: 96

デジタル証拠のビット ストリーム イメージ コピーは、次の目的で実行する必要があります。

- A. 上記すべて
- B. スラックスペースを含むすべてのディスクセクターをコピーします
- C. FAT テーブルをコピーします
- D. 元のディスクへの変更を禁止します

Answer: ([解答を表示する](#))

最新問題: 97

患者の電子的に保護された医療情報の完全性、機密性、可用性を確保することは、次のように知られています。

- A. 医療保険の相互運用性およびプライバシー法
- B. グラム ・リーチ ・ブライリー法
- C. 社会保障法
- D. サーベンス ・オクスリー法

Answer: ([解答を表示する](#))

最新問題: 98

リスク軽減戦略は、リスクを最小限に抑えて克服するために行動をとるべき状況を決定します。システム内の脆弱性と適切な制御を検索することで、リスクと損失の可能性を最小限に抑えることに重点を置いたリスク軽減戦略を特定します。

- A. 研究と承認
- B. リスク吸収
- C. リスク想定
- D. リスク制限

Answer: A ([メッセージを残す](#))

最新問題: 99

ネットワークに対する攻撃は、次のどれを使用してブロックするのが最も効果的ですか？

- A. Web プロキシ
- B. ヒップ
- C. IPS デバイス インライン
- D. ロードバランサ

Answer: C ([メッセージを残す](#))

最新問題: 100

コンピューター犯罪中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、次のように呼ばれます。

- A. デジタル調査
- B. コンピュータメール
- C. デジタル フォレンジック検査官
- D. デジタル証拠

Answer: D ([メッセージを残す](#))

最新問題: 101

既存のネットワーク リソースをすべて消費する大量のトラフィックでネットワークをフラディンングすることにより、意図したユーザーまたは許可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ネットワーク セキュリティ インシデントを特定します。

- A. サービス拒否攻撃
- B. XSS 攻撃
- C. SQL インジェクション
- D. URL 操作

Answer: ([解答を表示する](#)**)**

最新問題: 102

デジタル フォレンジック検査者は、被害者のコンピュータ上のすべての IP アドレスとそれに関連する MAC アドレスのリストを表示し、通信していたコンピュータを特定するために使用するコマンドは次のとおりです。

- A. `netstat -an` コマンド
- B. `nslookup` コマンド
- C. `arp` コマンド
- D. `ifconfig` コマンド

Answer: [\(解答を表示する\)](#)

最新問題: 103

監査証跡ポリシーは、オペレーティング システムに関するコンピュータ イベントの一連の記録など、すべての監査証跡を収集します。

システム、アプリケーション、またはユーザーのアクティビティ。監査証跡ポリシーに当てはまらないのは次のどれですか:

- A. 問題が発生した後にイベントを再構築するのに役立ちます。
- B. 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
- C. インシデントによる組織への無形の損失の計算に役立ちます
- D. 個々のアクションの追跡に役立ち、ユーザーが自分のアクションに対して個人的に責任を持つことができます。

Answer: [C \(メッセージを残す\)](#)

最新問題: 104

次の CERT のうち、オランダの高等教育機関やその他のさまざまな研究機関へのインターネット プロバイダーであり、顧客が被害者または容疑者として関与するコンピューター セキュリティ インシデントに関連するすべての事件を扱っているのはどれですか?

- A. DFN-CERT
- B. NET-CERT
- C. Funet CERT
- D. SURFnet-CERT

Answer: [D \(メッセージを残す\)](#)

最新問題: 105

James は、インシデント処理および対応 (IH&R) チームのリーダーに任命され、社内で IH&R 計画と彼自身のチームを構築するよう割り当てられました。James が現在取り組んでいる IH&R プロセス ステップを特定します。

- A. 準備
- B. 根絶
- C. 通知
- D. 回復

Answer: [A \(メッセージを残す\)](#)

最新問題: 106

インシデント後に予想される損失の推定は、組織が優先順位を付けて策定するのに役立ちます。

インシデント対応。インシデントのコストは、有形コストと無形コストに分類できます。特定する

ウィルスの発生に伴う具体的なコストは？

- A. のれんの喪失
- B. 精神的ダメージ
- C. 企業の評判への損害
- D. 生産性の損失によるダメージ

Answer: D ([メッセージを残す](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード:

Freepdfdumps)

最新問題: 107

US-CERT によると; 政府機関が DOS 攻撃を軽減できなかった場合は、以下の範囲内で報告する必要があります。

- A. 成功した攻撃がまだ進行中の場合、1 時間の検出/検出
- B. 成功した攻撃がまだ進行中の場合、4 時間の発見/検出
- C. 成功した攻撃がまだ進行中の場合、発見/検出に 2 時間かかります
- D. 成功した攻撃がまだ進行中の場合、3 時間の発見/検出

Answer: ([解答を表示する](#))

最新問題: 108

サムは、電子メール監視ツールを通じて、会社がフィッシング攻撃の標的になったことを示すアラートを受け取りました。事件を分析した後、サムは攻撃のターゲットのほとんどが会社の高名な幹部であることを特定しました。

これはどのような種類のフィッシング攻撃ですか？

- A. 捕鯨
- B. スピアフィッシング
- C. パドルフィッシング
- D. ファーミング

Answer: ([解答を表示する](#))

最新問題: 109

Linux コマンドは、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、生のファイルが与えられた場合はディスク イメージング ツールとして使用されます。入力としてのディスクデバイスは次のとおりです。

- A. `dd` コマンド
- B. `fiestat` コマンド
- C. `fslookup` コマンド
- D. 検索 コマンド

Answer: A ([メッセージを残す](#))

説明/参照:

最新問題: 110

システムまたはサイトの情報保証 (IA) およびセキュリティ体制を維持するシステムを認証および認定するための、一連の活動、一般的なタスク、および管理構造を確立する標準的な国内プロセスを特定します。

- A. NIACAP
- B. ニアサップ
- C. NIPACP
- D. NIAAAP

Answer: A ([メッセージを残す](#))

最新問題: 111

悲惨な出来事が発生した後でも政府機関が機能を継続できることは、冗長ハードウェアとソフトウェアの導入、フォールトトレラントシステムの使用、堅固なバックアップと回復戦略によって実現されます。これは次のように知られています。

- A. ビジネスの継続性
- B. 緊急時対応計画
- C. 事業継続計画
- D. 災害計画

Answer: A ([メッセージを残す](#))

最新問題: 112

ジェームスは、Cyber Sol Inc. でインシデント対応者として働いています。経営陣は、最近社内で発生したサイバーセキュリティ インシデントに対処するようにジェームスに指示しました。調査プロセスの一環として、James は Windows オペレーティング システムで実行されているシステムから揮発性情報の収集を開始しました。

James がプロセスを実行するためのすべての実行可能ファイルを判断するのに役立つコマンドは次のうちどれですか？

- A. dos キー/履歴
- B. 日付/t&時刻/t
- C. netstat-ab
- D. トップ

Answer: ([解答を表示する](#))

最新問題: 113

Smith は、さまざまなマルウェア検出技術を採用して、ネットワークとそのシステムに疑わしい悪意のあるマルウェア ファイルがないか徹底的に検査します。

すべての技術の中で、メモリ ダンプまたはマルウェアの痕跡のバイナリ コードを分析する技術はどれですか？

- A. 侵入分析
- B. 動的分析
- C. ライブ システム
- D. 静的解析

Answer: ([解答を表示する](#))

最新問題: 114

Raven は IH&R チームの一員であり、マネージャーから、インシデントの根本原因を処理および除去し、将来の同様のインシデントを防ぐためにすべての攻撃ベクトルを遮断するよう指示を受けました。Raven は、影響を受けるリソースをサービス プロバイダーと開発者に通知します。

インシデントの根本原因を取り除くために、Raven が実装する必要があるインシデント処理および対応プロセスの次のステップはどれですか？

- A. 根絶
- B. インシデントのトリアージ
- C. 証拠の収集とフォレンジック分析
- D. 封じ込め

Answer: A ([メッセージを残す](#))

最新問題: 115

既存のネットワーク リソースをすべて消費する大量のトラフィックでネットワークをフラディンングすることにより、意図した許可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ネットワーク セキュリティ インシデントを特定します。

- A. XSS 攻撃
- B. サービス拒否攻撃
- C. URL 操作
- D. SQL インジェクション

Answer: ([解答を表示する](#))

最新問題: 116

ネットワーク境界は、すべての送受信トラフィックを拒否するように構成する必要があります。

必要のないサービス。以下のサービスがブロックされている場合、サービス拒否の防止に役立つのはどれですか

攻撃？

- A. SAM サービス
- B. エコー サービス
- C. SMTP サービス
- D. POP3 サービス

Answer: B ([メッセージを残す](#))

最新問題: 117

US-CERT および連邦民間機関は、連邦機関の報告分類における報告期間基準を使用します。CAT 4 連邦政府機関カテゴリに基づいてインシデントを報告するにはどのくらいの時間がかかりますか？

- A. 成功した攻撃がまだ進行中であり、政府機関が活動をうまく緩和できない場合は、発見/検出から 4 時間以内
- B. 毎週
- C. 毎月
- D. 発見/検出から 2 時間以内

Answer: ([解答を表示する](#)**)**

最新問題: 118

学内ネットワークに接続された端末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いうのでしょうか？

- A. アクセスを許可する
- B. 不適切な使用法
- C. ネットワークアクセス
- D. アクセスを許可しない

Answer: C ([メッセージを残す](#))

最新問題: 119

DDoS 攻撃に対応するため。次の戦略のいずれかを使用できます。

- A. 追加の容量を使用して攻撃を吸収します
- B. 重要ではないサービスを特定し、それらを停止します
- C. 攻撃が収まるまで一部のサービスをシャットダウンします。
- D. 上記すべて

Answer: D ([メッセージを残す](#))

最新問題: 120

組織の顧客は、ネットワーク通信が遅くなったり、サービスが利用できなくなったりしています。さらに、ネットワーク管理者は、IDS/IPS やファイアウォールなどのセキュリティツールから、DoS/DDoS 攻撃の可能性に関する警告を受信しています。その結果、組織はインシデント処理および対応 (IH&R) チームにインシデントのさらなる調査を要求します。IH&R チームは、手動手法を使用して DoS/DDoS 攻撃を検出することにしました。IH&R チームが DoS/DDoS 攻撃を手動で検出するのに役立つコマンドは次のうちどれですか？

- A. nbtstat /c
- B. netstat -an
- C. nbtstat /S
- D. netstat -r

Answer: B ([メッセージを残す](#))

最新問題: 121

内部関係者は企業のビジネス機能を理解しています。企業資産に損害を与えるために内部関係者が実行する活動の正しい順序は次のとおりです。

- A. 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します
- B. 特権アクセスを取得し、マルウェアをインストールしてアクティブ化します
- C. マルウェアをインストールし、特権アクセスを取得してアクティブ化します
- D. 特権アクセスを取得し、マルウェアをアクティブ化してインストールします

Answer: B ([メッセージを残す](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (30530%OFF問題集溶と正解付きで 30%w 特別割引コード:

Freepdfdumps)

最新問題: 122

クラウド環境では、認定されたセキュリティ専門家が、認定されたユーティリティを使用して認定された衛生手順を実行し、クラウド内の汚染された情報システムやアプリケーションから流出したデータを永久に削除します。

これは次のどれの一例ですか？

- A. クラウド監査人

- B. クラウド コンピューティング
- C. クラウド ブローカー
- D. クラウドの撲滅

Answer: A ([メッセージを残す](#))

最新問題: 123

情報セキュリティ管理システム (ISMS) を開始、実装、または維持する組織に情報セキュリティ管理を実装するための推奨事項を提供する標準フレームワークは次のうちどれですか？

- A. RFC 2196
- B. ISO/IEC27035
- C. PCI DSS
- D. ISO/IEC27002

Answer: ([解答を表示する](#))

最新問題: 124

OBC 組織でインシデント対応者として働いているエリザベスは、組織のセキュリティが直面しているリスクを評価しています。評価プロセス中に、彼女は脅威源が既存のシステムの脆弱性を悪用する確率を計算します。

エリザベスが現在行っているリスク評価ステップを特定します。

- A. 影響分析
- B. システムの特性評価
- C. 尤度分析
- D. 脆弱性の特定

Answer: ([解答を表示する](#))

最新問題: 125

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、通常の動作状態に復元するプロセス

すべてのプロセス、ポリシー、ツールを含むステージは次のように知られています。

- A. インシデント管理
- B. インシデント対応
- C. インシデントの回復
- D. インシデント処理

Answer: C ([メッセージを残す](#))

説明/参照:

最新問題: 126

特定の脅威源に対して実行される可能性のある脆弱性がない場合、脅威源はリスクを示しません。さまざまな脅威ソースが定義されているステップを特定します。



- A. 制御分析
- B. 脅威の特定
- C. 識別の脆弱性
- D. システムの特性評価

Answer: B ([メッセージを残す](#))

最新問題: 127

パスワードクラッキングツールのインストール、ポルノコンテンツのダウンロード、同僚への電子メールの送信。

会社のコンピュータ上で無許可の Web サイトをホスティングすることは、次のような理由で彼らを苛立たせると考えられます。

- A. 不正アクセス攻撃
- B. マルウェア攻撃
- C. ネットワークベースの攻撃
- D. 不適切な使用事件

Answer: D ([メッセージを残す](#))

最新問題: 128

クアル テック ソリューションズは、大手セキュリティ サービス企業です。ディクソンはこの会社でインシデント対応者として働いています。彼は、エンタープライズ ネットワークに存在するホスト、サービス、および脆弱性を特定する自動ツールを使用して、ネットワーク内のセキュリティ問題を特定するために脆弱性評価を実行しています。

上記のシナリオに基づいて、Dickson が実行する脆弱性評価の種類を特定します。

- A. 内部評価
- B. 外部評価
- C. 受動的評価
- D. アクティブな評価

Answer: A ([メッセージを残す](#))

最新問題: 129

ホストは、脆弱なサービスを通じて伝播するワームに感染します。の存在の兆候ワームには次のものが含まれます。

- A. 上記すべて
- B. 脆弱なサービスを対象とした確立された接続試行
- C. ネットワーク使用量の減少
- D. システムが不安定になるかクラッシュする

Answer: ([解答を表示する](#))

最新問題: 130

次の技術のうち、インシデント処理プロセスを妨げたり誤解を与えたり、フォレンジック調査プロセスの収集、保存、特定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. フットプリント
- B. 列挙型
- C. スキャン中
- D. アンチフォレンジック

Answer: ([解答を表示する](#))

最新問題: 131

デジタル証拠は次のことを行う必要があります。

- A. 本物、完全、信頼できるものであること
- B. 揮発性であること
- C. 証拠の信頼性と真実性に疑問を投げかける
- D. 攻撃者の行動を証明しない

Answer: ([解答を表示する](#))

最新問題: 132

インシデント処理担当者である Shelly は、フロリダに拠点を置く Texas Pvt.Ltd. という会社で働いています。彼女はインシデント対応計画に取り組むよう依頼されました。計画の一環として、彼女は企業のセキュリティ インフラストラクチャを強化および改善することを決定しました。彼女は、セキュリティ専門家が情報システム全体で複数の保護層を使用できるようにするセキュリティ戦略を組み込みました。このセキュリティ戦略は、複数層の保護により、1つの層を突破しても攻撃者を次の層に誘導するだけなので、組織の情報システムに対する直接攻撃を防ぐのに役立ちます。

次のセキュリティ戦略のうち、インシデント対応計画に組み込んだものはどれですか？

- A. 多層防御
- B. 秘密チャネル
- C. 指数バックオフ アルゴリズム
- D. スリーウェイ ハンドシェイク

Answer: A ([メッセージを残す](#))

最新問題: 133

攻撃者は、標的となる個人が頻繁にスリングを訪問していた Web サイトを発見しました。次に、攻撃者はこれらの特定の Web サイトをテストして、潜在的な脆弱性を特定しました。Web サイト内の脆弱性を検出した後、攻撃者は、Web ページをリダイレクトしてマルウェアを被害者のマシンにダウンロードする悪意のあるスクリプト/コードを Web アプリケーションに挿入し始めました。脆弱な Web アプリケーションに感染した後、攻撃者は被

被害者が感染した Web アプリケーションにアクセスするのを待ちました。攻撃者が実行した攻撃の種類を特定します。

- A. Cookie/セッションポイズニング
- B. 水飲み場
- C. ディレクトリ トラバーサル
- D. 難読化アプリケーション

Answer: A ([メッセージを残す](#))

最新問題: 134

インシデントの処理と対応の手順は、インシデントの検出、特定、対応、管理に役立ちます。どれ

次の手順は、インシデントの範囲と範囲を制限することに重点を置いていますか？

- A. データ収集
- B. 封じ込め
- C. 根絶
- D. 識別

Answer: B ([メッセージを残す](#))

最新問題: 135

ロッシさんは組織のインシデント マネージャー (IM) であり、彼のチームは組織内のすべてのユーザーにサポートを提供しています。

脅威や攻撃の影響を受ける組織。組織の内部監査人であるデビッドは、ロスのインシデント対応チームの一員でもあります。

デビッドの責任は次のうちどれですか？

- A. 侵入者と思われる者からのネットワーク トラフィックをブロックするために必要なアクションを実行します。
- B. 情報セキュリティ責任者 (ISO) とインシデント封じ込め活動を調整します。
- C. セキュリティの抜け穴を特定し、必要な措置を講じるため管理者に報告します。
- D. 情報セキュリティ制御を構成します。

Answer: ([解答を表示する](#)**)**

最新問題: 136

オープン ソースの TCP/IP ネットワーク侵入防止および検出システム (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 ログを実行し、次のように呼ばれます。

- A. ネスス
- B. 鼻息
- C. 聖人
- D. Wireshark

Answer: B ([メッセージを残す](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 137

緊急時対応計画により、組織は緊急事態に対処するための効果的な方法を開発および維持できます。すべての組織には、計画で対処する必要がある独自の要件があります。IT 緊急時対応計画には、サポート情報、通知のアクティブ化、復旧と再構成、および計画の付録という 5 つの主要なコンポーネントがあります。再建計画の主な目的は何ですか？

- A. 通知手順、損害評価を定義し、計画のアクティブ化を提案するため
- B. 元のサイトを復元するには、インシデントを防ぐためにシステムをテストし、運用を終了します。
- C. 回復手順を利用して一連の回復アクティビティを提供します。
- D. 緊急時対応計画の概要と詳細な概念を提供します。

Answer: B ([メッセージを残す](#))

最新問題: 138

マネージャーはあなたにいくつかのデジタル証拠を渡し、変動性の高い順に調査するように求めます。

最も不安定なものは次のうちどれですか？

- A. 電子メール
- B. キャッシュ
- C. ディスク
- D. 一時ファイル

Answer: B ([メッセージを残す](#))

最新問題: 139

インシデント処理担当者である Shall y は、フロリダに拠点を置く Texas Pvt.Ltd. という会社で働いています。彼女はインシデント対応計画に取り組むよう依頼されました。計画の一環として、彼女は企業のセキュリティ インフラストラクチャを強化および改善することを決定しました。彼女は、セキュリティ専門家が情報システム全体にわたって複数の保護層を使用できるようにするセキュリティ戦略を組み込みました。このセキュリティ戦略は、複数層の保護により、1 つの層を突破しても攻撃者を次の層に誘導するだけであるため、組織の情報システムに対する直接攻撃の防止に役立ちます。

インシデント対応計画に組み込んだセキュリティ戦略を特定します。

- A. スリーウェイ ハンドシェイク
- B. 多層防御
- C. 指数バックオフ アルゴリズム
- D. 秘密チャネル

Answer: B ([メッセージを残す](#))

最新問題: 140

インシデント処理および対応 (IH&R) プロセスの段階の流れとして正しいのは次のうちどれですか？

- A. 封じ込め インシデントの記録 インシデントのトリアージ 準備 回復 根絶 インシデント後の活動
- B. インシデントの追跡 根絶の封じ込め インシデントの記録 準備 回復 インシデント後の活動
- C. 準備 インシデントの記録 インシデントのトリアージ 封じ込め根絶 回復 インシデント後の活動
- D. インシデントの記録 準備 封じ込め インシデントのトリアージ 回復 根絶 インシデント後の活動

Answer: C ([メッセージを残す](#))

最新問題: 141

次のフォレンジック調査フェーズのうちどれを最初に実行する必要がありますか？

- A. 予備証拠を収集します。
- B. 証拠を法医学研究所に輸送します。
- C. 証拠の 2 つのビットストリームのコピーを作成します。
- D. ファーストレスポンド手順を実行します。

Answer: D ([メッセージを残す](#))

最新問題: 142

あらゆるユーザー、企業、政府機関、または組織に年中無休のコンピューター セキュリティ インシデント対応サービスを提供するサービス組織は、次のように知られています。

- A. セキュリティ オペレーション センター SOC
- B. コンピュータ セキュリティ インシデント対応チーム CSIRT
- C. デジタル フォレンジック検査官
- D. 脆弱性評価者

Answer: B ([メッセージを残す](#))

最新問題: 143

政府機関が情報セキュリティ インシデントを報告しない理由は次のとおりです。

- A. 上記すべて

- B. 悪評が怖い
- C. 内部で攻撃を処理する方法について十分な知識を持っている
- D. インシデントの報告に追加コストを支払いたくない

Answer: B ([メッセージを残す](#))

最新問題: 144

いくつかの統計に基づいて、典型的なナンバーワンの事件は何ですか？

- A. ポリシー違反
- B. 不正アクセス
- C. マルウェア
- D. フィッシング

Answer: D ([メッセージを残す](#))

最新問題: 145

異常なログイン、職務上使用されていない機密情報へのアクセス、会社資産での個人用外部ストレージドライブの使用はすべて、次のどれに該当する兆候ですか？

- A. セキュリティ侵害
- B. インサイダーの脅威
- C. 働きすぎ
- D. ジョブローテーションの欠如

Answer: B ([メッセージを残す](#))

最新問題: 146

OBC 組織でインシデント対応者として働いているエリザベスは、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、彼女は脅威源が既存のシステムの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、次のリスク評価ステップのうちどれを行っていますか？

- A. 脆弱性の特定
- B. 影響分析
- C. 尤度分析
- D. システムの特性評価

Answer: ([解答を表示する](#))

最新問題: 147

不適切な使用事件は次のうちどれですか？

- A. 偵察攻撃
- B. アクセス制御攻撃
- C. 内部関係者の脅威
- D. サービス拒否攻撃

Answer: C ([メッセージを残す](#))

最新問題: 148

定性的リスク分析では、リスクは次の観点から計算されます。

- A. (攻撃成功 + クリティカル) - (対策)
- B. (対策 + 影響の大きさ) - (事前のリスク評価からのレポート)
- C. 資産の重要性評価 - (リスクおよび関連するリスク レベル)
- D. 損失の確率 × 損失

Answer: D ([メッセージを残す](#))

最新問題: 149

コンピュータフォレンジックは、コンピューティングから証拠を収集するための体系的な一連の技術と手順です

一貫した法律の授業で提示できる機器、さまざまな記憶装置、デジタルメディアそして意味のある形式。コンピュータフォレンジックの手順の流れとして適切なのは次のうちどれですか。

プロセス :

- A. 準備 > 分析 > 収集 > 検査 > 報告
- B. 検査 > 分析 > 準備 > 収集 > 報告
- C. 準備 > 収集 > 検査 > 分析 > レポート
- D. 分析 > 準備 > 収集 > 報告 > 検査

Answer: ([解答を表示する](#)**)**

最新問題: 150

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、すべてのサーバーが Web 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。

どのような種類の情報セキュリティ攻撃ベクトルがネットワークに影響を与えていますか？

- A. IoT の脅威
- B. ランサムウェア
- C. 高度で持続的な脅威
- D. ボットネット

Answer: ([解答を表示する](#)**)**

最新問題: 151

ネットワーク リソースを使い果たし、アプリケーションに不正なリクエストを送信することで、許可された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することを妨げるタイプの攻撃は、次のように知られています。

- A. セッションハイジャック攻撃
- B. 中間者攻撃

C. サービス拒否攻撃

D. SQL インジェクション攻撃

Answer: ([解答を表示する](#))

有効な **212-89** 問題集は GoShiken.com が提供された合格しやすい 212-89 試験問題集！ GoShiken.com が最新の **212-89** 試験問題集を提供しています。GoShiken.com 212-89 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 212-89 問題集をゲットする人はこちら: <https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (**30530%OFF**問題集溶と正解付きで **30%w** 特別割引コード:

Freepdfdumps)

最新問題: 152

分散型サービス拒否 (DDoS) 攻撃は、より一般的な種類の DoS 攻撃であり、単一のシステムが

インターネット上の多数の感染したマシンの標的となります。DDoS 攻撃では、攻撃者はまず感染します。

として知られる複数のシステム:

A. スパイウェア

B. トロイの木馬

C. ワーム

D. ゾンビ

Answer: D ([メッセージを残す](#))

最新問題: 153

ケースを処理するときに CSIRT が使用する一般的な正しいアクティビティの順序は次のとおりです。

A. 情報の記録、通知、リリース、連絡先の維持、フォローアップと報告

B. 記録、連絡先の維持、情報のリリース、通知、フォローアップ、および報告

C. 記録、通知、連絡先の維持、情報のリリース、フォローアップとレポート

D. 記録、連絡先の維持、通知、情報のリリース、フォローアップと報告

Answer: C ([メッセージを残す](#))

Valid 212-89 Dumps shared by GoShiken.com for Helping Passing 212-89 Exam!

GoShiken.com now offer the **newest 212-89 exam dumps**, the GoShiken.com 212-89 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 212-89 dumps with Test Engine here:

<https://www.goshiken.com/EC-COUNCIL/212-89-mondaishu.html> (305 Q&As Dumps,
30%OFF Special Discount: **Freepdfdumps**)