EC-COUNCIL.312-39.v2024-04-26.q46

試験コード:	312-39
試験名称:	Certified SOC Analyst (CSA)
認定資格:	EC-COUNCIL
無料問題数:	46
バージョン:	v2024-04-26
アクセス数:	309
ページビュー数:	460
https://www.jpnpdf.com/EC-COUNCIL.312-39.v2024-04-26.q46-mondaishu.html	

最新問題: **1**
インシデント処理および対応プロセスの次のステップのうち、インシデントの範囲と程度を制限することに重点を置いているのはどれですか?
A. 根絶
B. データ収集
C. 識別
D. 封じ込め
Answer: D (メーッセージを残す**)**

最新問題: **2**
SOC アナリストのジョンは、Windows エンドポイントからのプロセス作成アクティビティの試行を監視したいと考えています。
次の Splunk クエリのうち、プロセス作成に関連する関連ログを取得するのに役立つものはどれですか?
A. index=windows LogName=Security EventCode=3688 NOT (Account_Name=*$) .. .. ..
B. index=windows LogName=Security EventCode=4688 NOT (Account_Name=*$) .. .. ..
C. index=windows LogName=Security EventCode=5688 NOT (Account_Name=*$) ... ...
D. index=windows LogName=Security EventCode=4678 NOT (Account_Name=*$) .. ..
Answer: B (メーッセージを残す**)**

最新問題: **3**
Identify the password cracking attempt involving a precomputed dictionary of plaintext passwords and their corresponding hash values to crack the password.
A. Dictionary Attack
B. Bruteforce Attack
C. Syllable Attack
D. Rainbow Table Attack

Answer: A (メーッセージを残す)

最新問題**: 4**
必ずしも重要ではないが、将来の問題の可能性を示している可能性があるイベントについて、Windows ログ内のイベント重大度レベルを特定します。
A. 警告
B. エラー
C. 失敗の監査
D. 情報
Answer: (解答を表示する)

最新問題**: 5**
サイバー脅威インテリジェンスを SOC チームに適切に適用することは、TTP の発見に役立ちます。
これらの TTP は何を指しますか?
A. ターゲット、脅威、プロセス
B. 戦術、テクニック、手順
C. 戦術、脅威、手順
D. 戦術、目標、プロセス
Answer: B (メーッセージを残す)

最新問題**: 6**
SIEM がアナリストにコンテキストと情報を提供するために使用する脅威インテリジェンスは次のどれですか。
脅威アクターの TTP、マルウェア キャンペーン、脅威アクターが使用するツールを使用した 状況認識」。
1.戦略的脅威インテリジェンス
2.戦術的脅威インテリジェンス
3.運用上の脅威インテリジェンス
4.技術的脅威インテリジェンス
A. 2 および 3
B. 1 および 2
C. 3 と 4
D. 1 および 3
Answer: A (メーッセージを残す)

最新問題**: 7**
Which of the following is a Threat Intelligence Platform?
A. SolarWinds MS
B. TC Complete

C. Keepnote
D. Apility.io
Answer: A (メーッセージを残す**)**

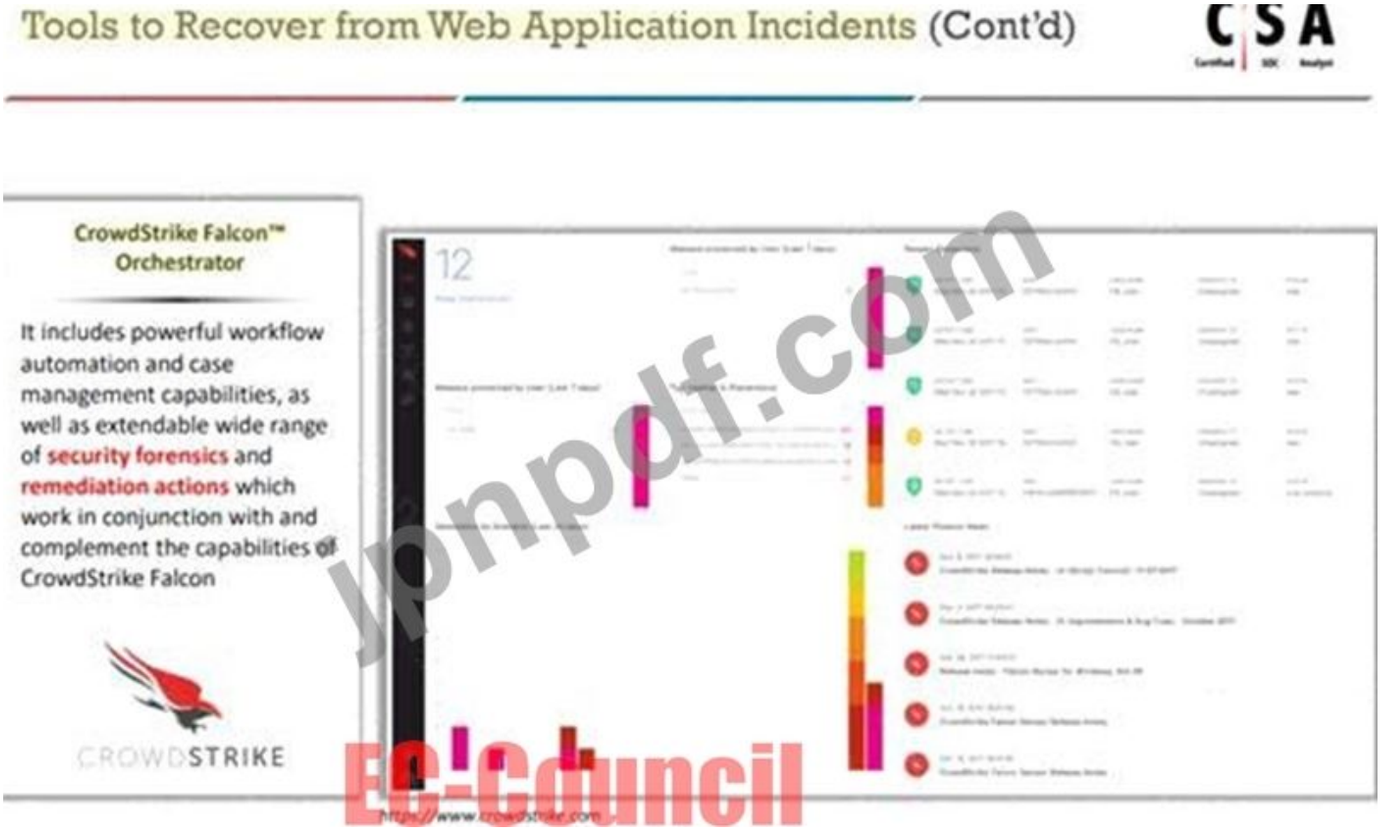
最新問題**: 8**
次のインシデント処理および対応段階のうち、フォレンジック結果からインシデントの根本原因を見つける必要があるのはどれですか?
A. システムの回復
B. 証拠の収集
C. 証拠の処理
D. 根絶
Answer: B (メーッセージを残す**)**

最新問題**: 9**
検索エンジンやフォーラムでユーザー入力を表示する前に、英数字以外の文字をすべて HTML 文字エンティティに変換することで根絶できる攻撃は次のうちどれですか?
A. XSS 攻撃
B. 壊れたアクセス制御攻撃
C. Web サービス攻撃
D. セッション管理攻撃
Answer: A (メーッセージを残す**)**

最新問題**: 10**
誤検知の調査の負担を軽減するのに役立つのは次のうちどれですか?
A. セキュリティ デバイスを信頼していません
B. コンテキスト データの取り込み
C. すべてのアラートを高レベルとして扱います
D. デフォルトのルールを維持する
Answer: D (メーッセージを残す**)**

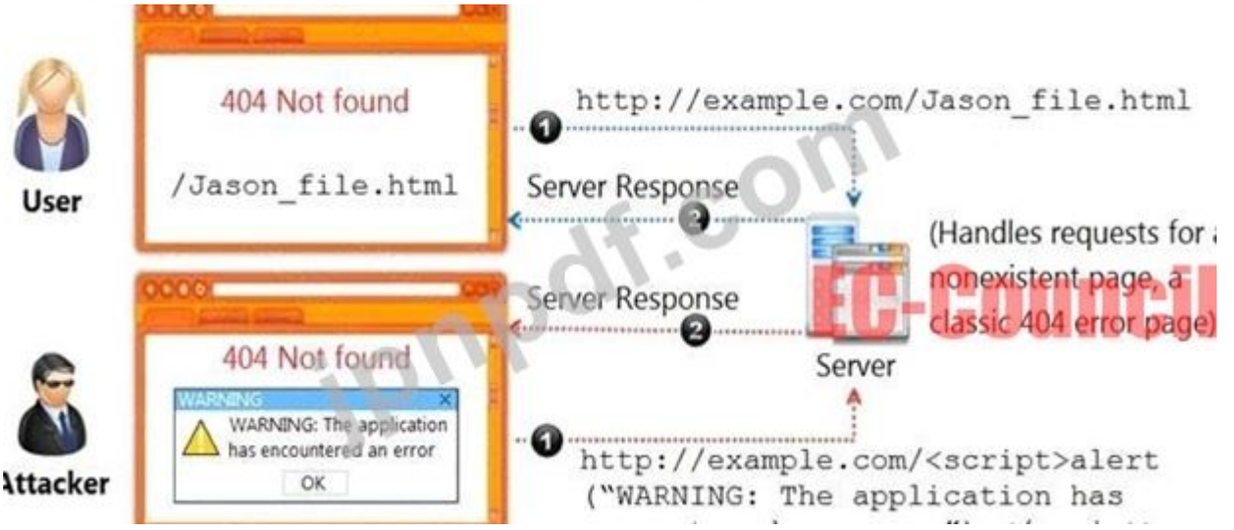
最新問題**: 11**
リスクを表す式は次のうちどれですか?
A. リスク = 可能性 * 重大度 * 資産価値
B. リスク = 可能性 * 結果 * 重大度
C. リスク = 可能性 * 影響 * 重大度
D. リスク = 可能性 * 影響 * 資産価値
Answer: D (メーッセージを残す**)**

最新問題: **12**
Web アプリケーション インシデントから回復するために使用されるツールは次のどれですか?
A. CrowdStrike FalconTM オーケストレーター
B. シマンテック セキュア Web ゲートウェイ
C. スムーズウォール SWG
D. プロキシ ワークベンチ
Answer: (解答を表示する**)**



最新問題: **13**

Identify the type of attack, an attacker is attempting on www.example.com website.



A. SQL Injection Attack

B. Cross-site Scripting Attack

C. Denial-of-Service Attack

D. Session Attack

Answer: B (メーッセージを残す**)**

最新問題: **14**

SOC アナリストの Juliea は、ログを監視しているときに、大規模な TXT、NULL ペイロードに気づきました。

これは何を示しているのでしょうか?
A. DHCP 枯渇試行
B. トラックのカバーの試行
C. 同時 VPN 接続試行
D. DNS 抽出の試み
Answer: D (メーッセージを残す**)**

最新問題**: 15**
SOC アナリストである John は、ネットワークに到達する Tor トラフィックの量を懸念しています。彼は、SIEM にダッシュボードを準備して、TOR トラフィックの送信元の場所を特定するためのグラフを取得したいと考えています。
ダッシュボードを準備するために次のデータ ソースのどれを使用しますか?
A. IPtoName 解決を使用して IP アドレスまたはホスト名を維持できる DHCP/ログ。
B. IP アドレスを含む DNS/Web サーバーのログ。
C. IP アドレスとユーザー エージェントの IPtouseragent 解決を含む IIS/Web サーバーのログ。
D. IP アドレスとホスト名を含む Apache/Web サーバーのログ。
Answer: D (メーッセージを残す**)**

最新問題**: 16**
安全な API を使用してインタプリタの使用を完全に回避することで根絶できる攻撃は次のうちどれですか?
A. LDAP インジェクション攻撃
B. ファイルインジェクション攻撃
C. SQL インジェクション攻撃
D. コマンドインジェクション攻撃
Answer: C (メーッセージを残す**)**

最新問題**: 17**
コンピュータフォレンジックラボをセットアップするための正しいフローは次のうちどれですか?
A. 計画と予算編成 -> 科学捜査研究所のライセンス -> 物理的な場所と構造設計の考慮事項 -> 作業エリアの考慮事項 -> 物理的セキュリティに関する推奨事項 -> 人的リソースの考慮事項

B. 計画と予算編成 -> 物理的な場所と構造設計の考慮事項 -> 作業エリアの考慮事項 -> 人的資源の考慮事項 -> 物理的セキュリティに関する推奨事項 -> 法医学研究所のライセンス
C. 計画と予算編成 -> 物理的な場所と構造設計の考慮事項 -> 科学捜査研究所のライセンス -> 人的資源の考慮事項 -> 作業エリアの考慮事項 -> 物理的セキュリティに関する推奨事項
D. 計画と予算編成 -> 物理的な場所と構造設計の考慮事項 -> 科学捜査研究所のライセンス -> 作業エリアの考慮事項 -> 人的資源の考慮事項 -> 物理的セキュリティに関する推奨事項
Answer: (解答を表示する**)**

最新問題**: 18**
Syslog メッセージの重大度レベルは、レベル 0 からレベル 7 までのラベルが付けられています。レベル 0 は何を示しますか?
A. アラート
B. 通知
C. 緊急事態
D. デバッグ
Answer: C (メーッセージを残す**)**

Severity Levels of Cisco Router Logs

Log messages in Cisco routers are categorized into eight severity levels ranging from 0 to 7. Each severity level determined a number and its corresponding name and UNIX syslog definitions. The lower severity number represents the high severity, and higher severity number represents the least severity.

Level	Level name	Syslog definition	Description
0	Emergencies	LOG_EMERG	System unusable
1	Alerts	LOG_ALERT	Immediate action needed
2	Critical	LOG_CRIT	Critical conditions
3	Errors	LOG_ERR	Error conditions
4	Warnings	LOG_WARNING	Warning conditions

最新問題**: 19**
パフォーマンスの尺度、適切なプロジェクトおよび時間管理の詳細が含まれているものは次のうちどれですか?
A. インシデント対応戦術
B. インシデント対応ポリシー
C. インシデント対応プロセス
D. インシデント対応手順
Answer: D (メーッセージを残す**)**

最新問題**: 20**

Emmanuel is working as a SOC analyst in a company named Tobey Tech. The manager of Tobey Tech recently recruited an Incident Response Team (IRT) for his company. In the process of collaboration with the IRT, Emmanuel just escalated an incident to the IRT.
What is the first step that the IRT will do to the incident escalated by Emmanuel?

A. Incident Analysis and Validation

B. Incident Recording

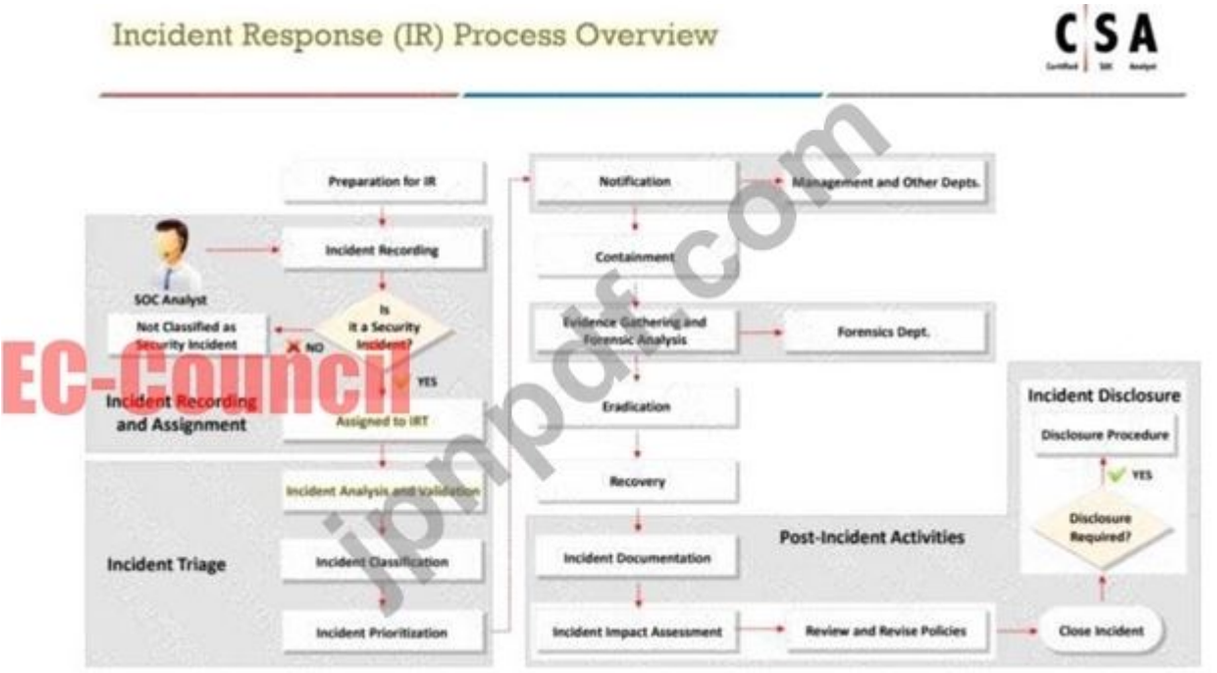
C. Incident Classification

D. Incident Prioritization

Answer: C (メーッセージを残す)

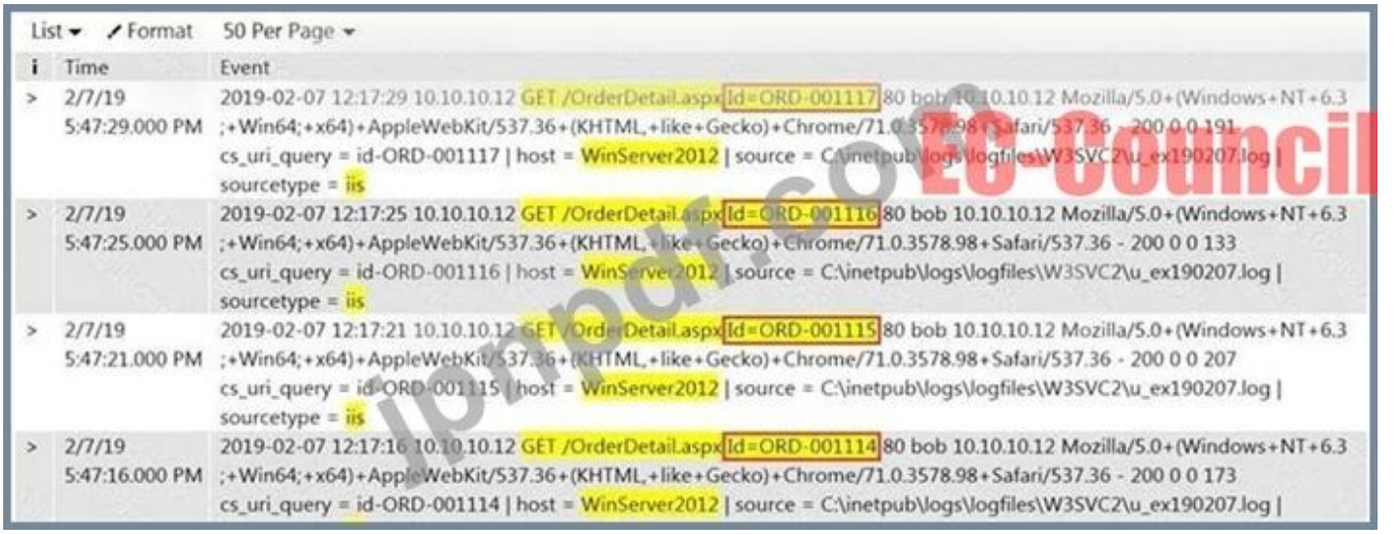
Explanation

Graphical user interface Description automatically generated



最新問題: 21

SOC アナリストの Rinni は、IDS ログを監視中に、次の図に示すイベントを検出しました。



このイベント ログは何を示していますか?

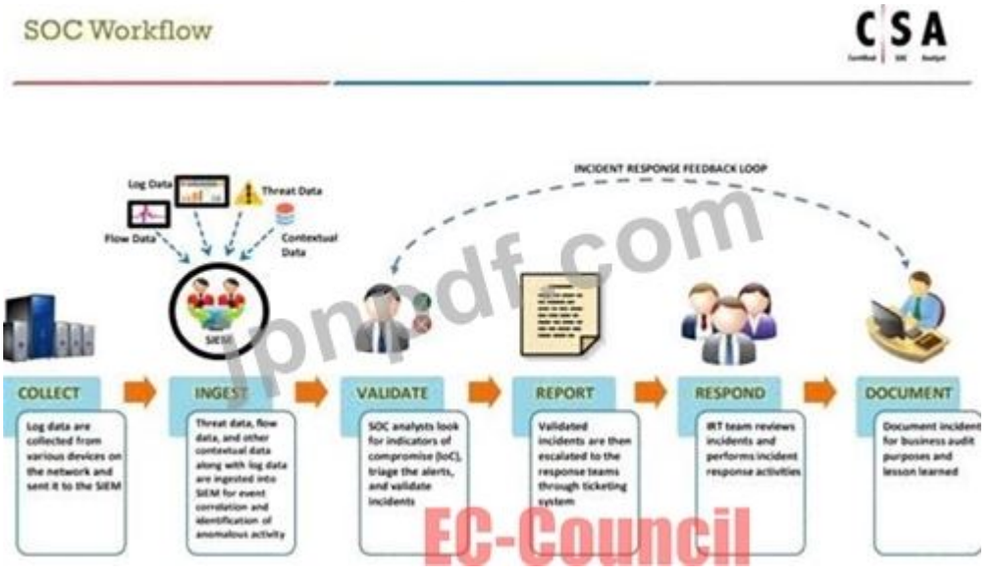
A. SQL インジェクション攻撃
B. パラメータ改ざん攻撃
C. XSS 攻撃
D. ディレクトリトラバーサル攻撃
Answer: B (メーッセージを残す**)**

最新問題**: 22**
Mike is an incident handler for PNP Infosystems Inc. One day, there was a ticket raised regarding a critical incident and Mike was assigned to handle the incident. During the process of incident handling, at one stage, he has performed incident analysis and validation to check whether the incident is a true incident or a false positive.
Identify the stage in which he is currently in.
A. Post-Incident Activities
B. Incident Recording and Assignment
C. Incident Triage
D. インシデントの開示
Answer: C (メーッセージを残す**)**

最新問題**: 23**
次のプロセスのうち、データが目的の受信者に届かなかったことを送信元に通知せずに、ルーティング レベルでパケットを破棄することを指すものはどれですか?
A. リクエストの削除
B. ロード バランシング
C. レート制限
D. ブラック ホール フィルタリング
Answer: D (メーッセージを残す**)**

最新問題: **24**
次のイベント検出技術のうち、ユーザーおよびエンティティ行動分析 (UEBA) を使用するものはどれですか?
A. ヒューリスティックベースの検出
B. シグネチャベースの検出
C. ルールベースの検出
D. 異常ベースの検出
Answer: (解答を表示する**)**

最新問題: **25**
SOC ワークフローの正しい順序は何ですか?
A. 収集、取り込み、検証、文書化、レポート、応答
B. 収集、取り込み、文書化、検証、レポート、応答
C. 収集、応答、検証、取り込み、レポート、文書化
D. 収集、取り込み、検証、レポート、応答、文書化
Answer: D (メーッセージを残す**)**



最新問題: **26**
ファイル拡張子の突然の変更、またはファイル名の変更が急速に増加する原因となる攻撃は、次のどれですか?
A. ファイルインジェクション攻撃
B. DHCP スターベーション攻撃
C. DoS 攻撃
D. ランサムウェア攻撃
Answer: D (メーッセージを残す**)**

最新問題: **27**

有効なプレフィックス (IP アドレス) から発信されるフラッディング攻撃から保護し、真の発信元を追跡できるようにする技術は次のうちどれですか?
A. レート制限
B. 出力フィルタリング
C. スロットリング
D. イングレスフィルタリング
Answer: D (メーッセージを残す**)**

最新問題**: 28**
組織は、SIEM 導入アーキテクチャを実装したいと考えています。ただし、機能できるのはログ収集のみであり、残りの SIEM 機能は MSSP によって管理される必要があります。
組織はどの SIEM 導入アーキテクチャを採用しますか?
A. 自己ホスト型、自己管理型
B. 自己ホスト型、共同管理型
C. クラウド、MSSP マネージド
D. セルフホスト型、MSSP 管理型
Answer: D (メーッセージを残す**)**

最新問題**: 29**
ウェスリーは、マディソンテックという会社のインシデントハンドラーです。ある日、彼は安全でない逆シリアル化攻撃を根絶するためのテクニックを学んでいました。
ウェスリーは次のうち、検討を避けるべきものは何ですか?
A. シリアル化と逆シリアル化に与えられるセキュリティ権限を理解する
B. セキュリティが重要なクラスのシリアル化を許可します。
C. 信頼できない入力を検証します。シリアル化されたデータに信頼できるクラスのみが含まれていることを確認するためにシリアル化されます。
D. 信頼できるデータの逆シリアル化は信頼境界を越える必要があります
Answer: (解答を表示する**)**

最新問題**: 30**
Maximus Tech の SOC アナリストである Jason は、Cisco ASA ファイアウォールのログを調査しており、次のログ エントリを発見しました。
May 06 2018 21:27:27 asa 1: %ASA -5 - 11008: ユーザー 'enable_15' が 'configure term' コマンドを実行しました 上記のログのセキュリティ レベルは何を示していますか?
A. 通常だが重要なメッセージ
B. 警告状態メッセージ
C. 重大な状態のメッセージ
D. 情報メッセージ
Answer: B (メーッセージを残す**)**

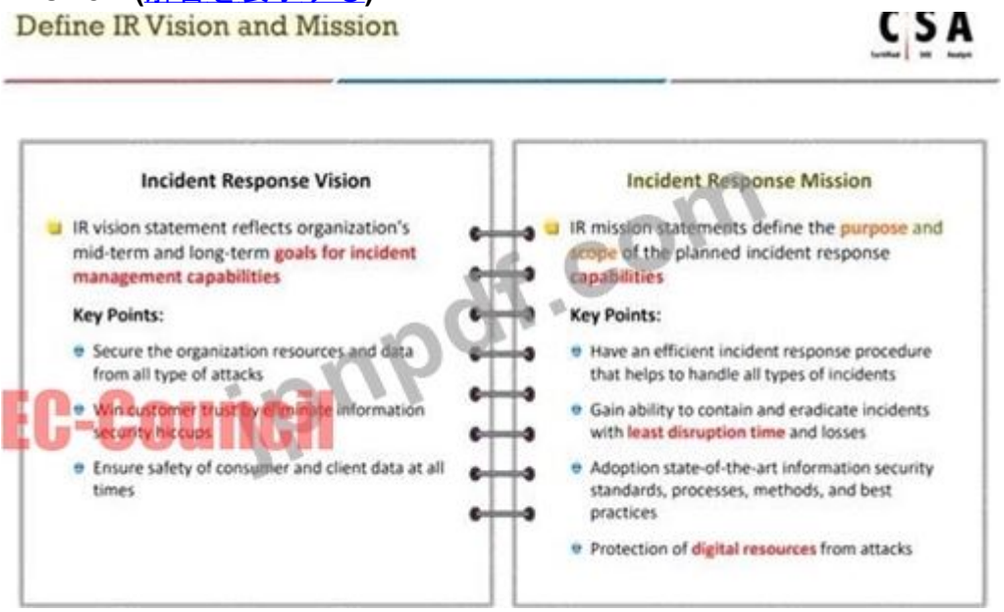
最新問題: **31**
HTTPS ステータス コード 403 は何を表しますか?
A. 見つからないエラー
B. 禁止されたエラー
C. 内部サーバー エラー
D. 不正なエラー
Answer: B (メーッセージを残す**)**

最新問題: **32**
What is the process of monitoring and capturing all data packets passing through a given network using different tools?
A. Port Scanning
B. Network Sniffing
C. Network Scanning
D. DNS Footprinting
Answer: B (メーッセージを残す**)**

最新問題: **33**
不適切な XML 構文をフィルタリングすることで根絶できる攻撃は次のうちどれですか?
A. SQL インジェクション攻撃
B. Web サービス攻撃
C. 不十分なログ記録と監視攻撃
D. CAPTCHA 攻撃
Answer: A (メーッセージを残す**)**

最新問題: **34**
Which of the following formula represents the risk levels?
A. Level of risk = Consequence * Likelihood
B. Level of risk = Consequence * Impact
C. Level of risk = Consequence * Asset Value
D. Level of risk = Consequence * Severity
Answer: B (メーッセージを残す**)**

最新問題: **35**
ダニエルは、Mesh Tech という名前の会社で最近設立された IRT のメンバーです。彼は、計画されているインシデント対応機能の目的と範囲を見つけたいと考えていました。
彼は何を探しているのでしょうか？
A. インシデント対応インテリジェンス
B. インシデント対応ミッション
C. インシデント対応ビジョン
D. インシデント対応リソース
Answer: (解答を表示する**)**



最新問題: **36**
iptables でのログ記録を有効にするために使用されるコマンドは次のどれですか?
A. $ iptables -A INPUT -j LOG
B. $ iptables -B INPUT -j LOG
C. $ iptables -A OUTPUT -j LOG
D. $ iptables -B OUTPUT -j LOG
Answer: (解答を表示する**)**

最新問題: **37**
リスクを表す式は次のうちどれですか?
A. リスク = 可能性 * 影響 * 重大度
B. リスク = 可能性 * 結果 * 重大度
C. リスク = 可能性 * 重大度 * 資産価値
D. リスク = 可能性 * 影響 * 資産価値
Answer: (解答を表示する**)**

最新問題: **38**

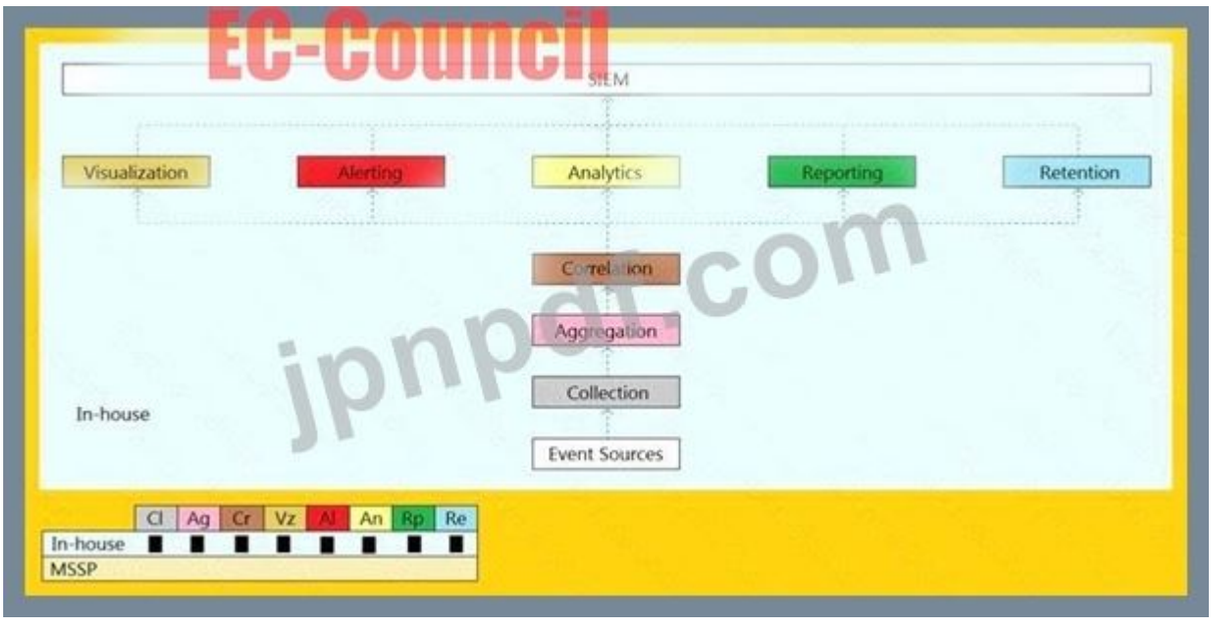
Shawn は、Lee Inc Solution で働くセキュリティ マネージャーです。彼の組織は、脅威インテリジェントな戦略計画を策定したいと考えています。同氏は、脅威インテリジェント戦略計画の一環として、脅威インテリジェンスの要件分析、インテリジェンスと収集計画、資産の特定、脅威レポート、インテリジェンスの賛同など、さまざまなコンポーネントを提案した。
効果的なものにするために、上記の脅威インテリジェント戦略計画に含めるべきコンポーネントは次のうちどれですか?
A. 脅威の賛同
B. 脅威のピボット化
C. 脅威の強化
D. 脅威の傾向
Answer: A (メーッセージを残す**)**

最新問題**: 39**
Syslog メッセージの重大度レベルは、レベル 0 からレベル 7 までのラベルが付けられています。レベル 0 は何を示しますか?
A. アラート
B. 緊急事態
C. デバッグ
D. 通知
Answer: D (メーッセージを残す**)**

最新問題**: 40**
Windows イベント ID 4740 は何を示していますか?
A. ユーザー アカウントがロックアウトされました。
B. ユーザー アカウントが無効になりました。
C. ユーザー アカウントが有効になりました。
D. ユーザー アカウントが作成されました。
Answer: (解答を表示する**)**

最新問題**: 41**
リスク マトリックス テーブルによると、攻撃の可能性が非常に低く、その攻撃の影響が大きい場合のリスク レベルはどれくらいになりますか?
A. 極端な
B. 低
C. 中
D. 高
Answer: (解答を表示する**)**

最新問題**: 42**
組織は、次の機能を備えた SIEM を実装および展開しています。



組織はどのような種類の SIEM 導入アーキテクチャを実装する予定ですか?

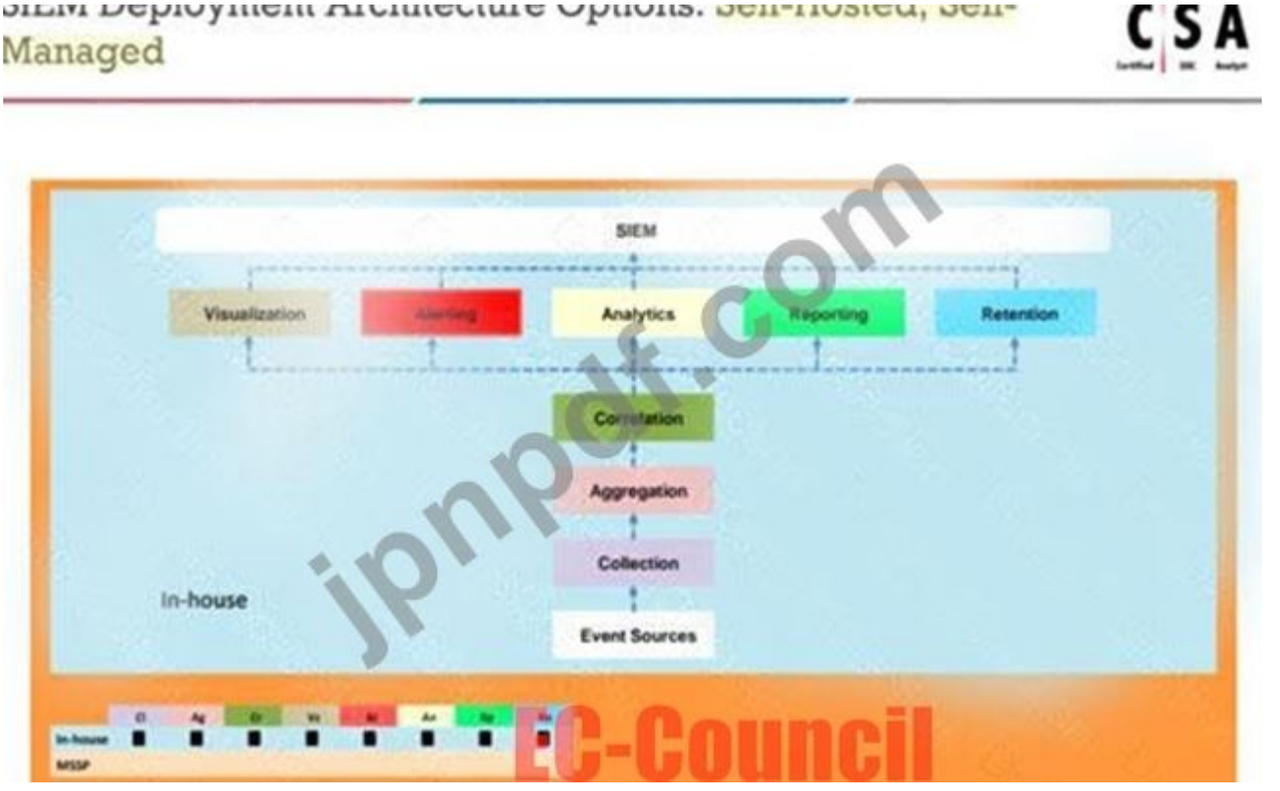
A. クラウド、MSSP マネージド

B. 自己ホスト型、共同管理型

C. 自己ホスト型、自己管理型

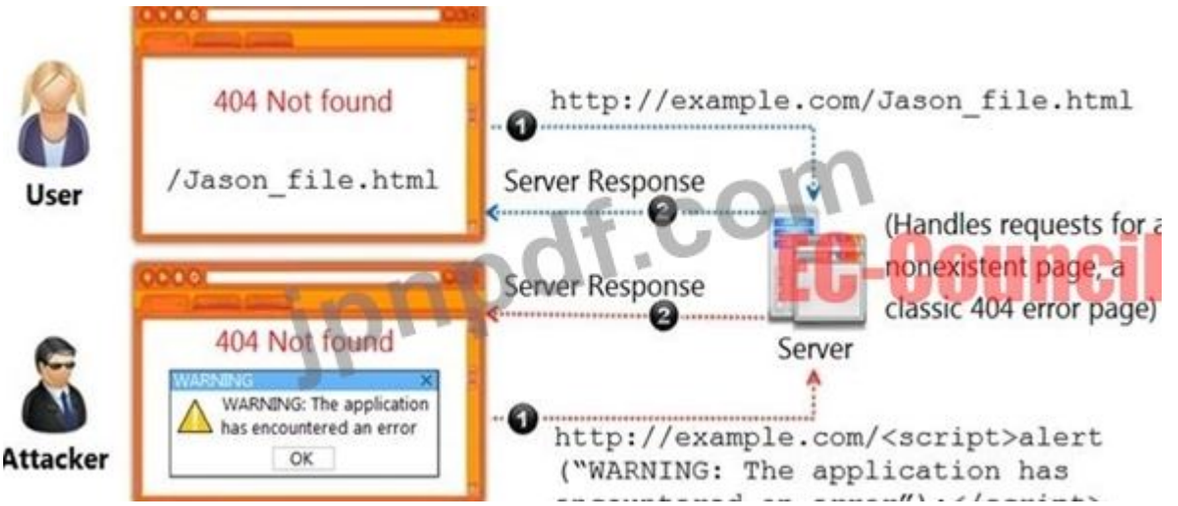
D. セルフホスト型、MSSP 管理型

Answer: C (メーッセージを残す)



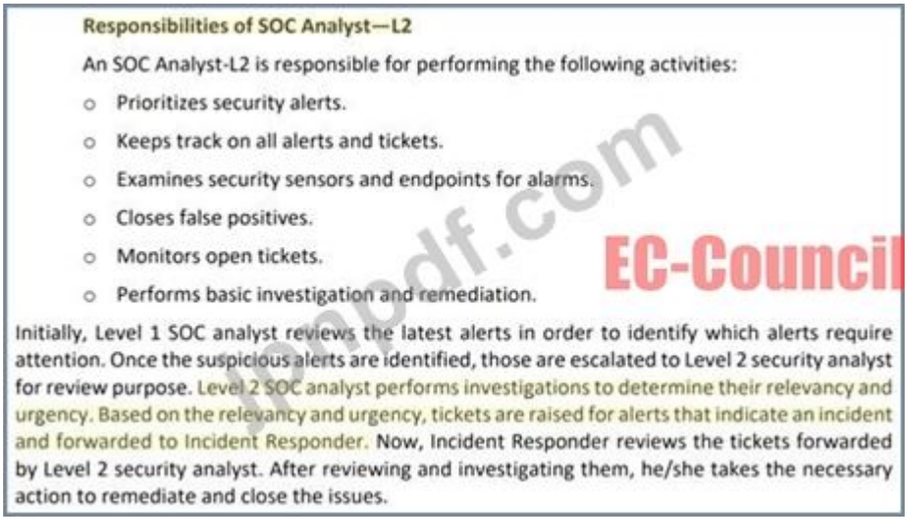
最新問題: **43**

攻撃者が www.example.com Web サイトに対して試みている攻撃の種類を特定します。



A. サービス拒否攻撃
B. SQL インジェクション攻撃
C. クロスサイト スクリプティング攻撃
D. セッション攻撃
Answer: (解答を表示する**)**

最新問題**: 44**
Charline は L2 SOC アナリストとして働いています。ある日、L1 SOC アナリストが、さらなる調査と確認を求めて彼女にインシデントを報告しました。チャーリーン氏は徹底的な調査を行った後、この事件を確認し、最初の優先順位を付けました。
What would be her next action according to the SOC workflow?
A. She should immediately escalate this issue to the management
B. She should immediately contact the network administrator to solve the problem
C. She should communicate this incident to the media immediately
D. She should formally raise a ticket and forward it to the IRT
Answer: (解答を表示する**)**



最新問題**: 45**

攻撃者は、電子商取引 Web サイトのロジック検証メカニズムを悪用します。彼は、クライアントとサーバー間で交換される URL を変更することで、100 ドル相当の商品を 10 ドルで購入することに成功しました。
オリジナル
URL: http://www.buyonline.com/product.aspx?profile=12
&デビット=100
変更された URL: http://www.buyonline.com/product.aspx?profile=12
&デビット=10
上記のシナリオで示されている攻撃を特定します。
A. サービス拒否攻撃
B. SQL インジェクション攻撃
C. パラメータ改ざん攻撃
D. セッション固定攻撃
Answer: C (メーッセージを残す**)**

最新問題**: 46**
SIEM アーキテクチャの選択を決定する要因は次のどれですか?
A. SMTP 構成
B. DNS 構成
C. ネットワーク トポロジ
D. DHCP 構成
Answer: B (メーッセージを残す**)**