Understanding Cisco Cybersecurity Operations Fundamentals (200-201 Japanese Version)

1. SOC アナリストは、Cisco StealthWatch を介して、HR エンドポイントの 1 つからメインの HR データベース サーバへの既知の C&C への接続およびポート スキャン アクティビティを検出しました。NISTSP800-61 インシデント処理プロセスに従って、SOC チームが行う次の 2 つのステップは何ですか? (2つお選びください)

A. 影響を受けるエンドポイントを隔離し、分析のためにディスク イメージを取得します。

B. 人事マネージャーと従業員にセキュリティ意識向上トレーニングを提供する

C. 境界の次世代ファイアウォールでこの C&C サーバーへの接続をブロックします

D. 影響を受けるエンドポイントのウイルス対策シグネチャ データベースを更新して、C&C への接続をブロックします。

E. 攻撃ベクトルを検出し、C&C 接続を分析します。

Answer(s): A,C

---

2. 正当なトラフィックをブロックすることでネットワーク トラフィックに影響を与えるシグネチャはどれですか?

A. 偽陰性

B. 真陽性

C. 真陰性

D. 偽陽性

Answer(s): D

3. ネットワーク エンジニアは、外国政府が自国の防衛請負業者の 1 社をハッキングし、知的財産を盗んだことを発見します。この状況での脅威エージェントは何ですか?

A. 盗まれた知的財産

B. 知的財産を保管した防衛請負業者

C. 攻撃を実行するために使用された方法

D. 攻撃を行った外国政府

Answer(s): D

---

4. アナリストは、さまざまなオペレーティング システムの機能を調査しています。

A. Microsoft Services for Linux がインストールされている Linux デバイスを照会します

B. 自動化された方法で Windows オペレーティング システムを展開します

C. Active Directory を操作するための効率的なツールです。

D. インストールされているハードウェアとソフトウェアを説明する Common Information Model があります。

Answer(s): D

---

5. 侵入検知システムが多数のソースから異常に大量のスキャンを受信し始めた場合、どの回避手法が示されますか?

A. リソース枯渇

B. トンネリング

C. トラフィックの断片化

D. タイミングアタック

Answer(s): A

---

6. HTTP ヘッダー、統一リソース ID、および SSL セッション ID 属性に基づいてルーティングを決定するソリューションを実装するには、どのテクノロジを使用する必要がありますか?

A. AWS

B. IIS

C. ロードバランサ

D. プロキシサーバー

Answer(s): C

---

7. RC4 のようなストリーム暗号が同じキーで 2 回使用された場合、ネットワークはどの攻撃に対して脆弱ですか?

A. 偽造攻撃

B. 平文のみの攻撃

C. 暗号文単独攻撃

D. 中間者攻撃

Answer(s): C

---

8. エンジニアがセキュリティ侵害を調査するために完全なパケット キャプチャを使用する必要があるのはなぜですか?

A. エンジニアが疑わしいパケットに焦点を当てて悪意のあるアクティビティを特定できるように、各パケット内に設定されている TCP フラグをキャプチャします。

B. エンジニアが分析するためのメタデータ (並べ替え、解析、インデックス付けされた IP トラフィック パケット データなど) を収集します。

C. エンジニアがメタデータに従って入ってくる脅威を識別するための完全な TCP ストリームを提供します。

D. イベントを再構築し、エンジニアが侵害中に何が起こったかを確認して根本原因を特定できるようにします。

Answer(s): D

---

9. IDS/IPS デバイスを回避しようとする場合、ユーザーが特定のキー、証明書、またはパスワードなしでデータを理解できないようにするメカニズムはどれですか?

A. 断片化

B. ピボット

C. 暗号化

D. 速記

Answer(s): C

---

10. 「Tcpdump」ツールの不正使用事件について、エンジニアが調査を行っています。分析の結果、悪意のあるインサイダーが特定のインターフェイスでトラフィックを傍受しようとしたことが明らかになりました。悪意あるインサイダーはどのような種類の情報を入手しようとしましたか?

A. ネットワークで使用されているタグ付きプロトコル

B. すべてのファイアウォール アラートとその結果の軽減策

C. ネットワークで使用されているタグ付きポート

D. データグラム内のすべての情報とデータ

Answer(s): D

---

11. ホストベースのファイアウォールはワークステーションを何から保護しますか?

A. ゼロデイ脆弱性

B. 不要なトラフィック

C. 悪意のある Web スクリプト

D. ウイルス

Answer(s): B

---

12. 展示を参照してください。実行ファイルはどこにありますか?

A. 情報

B. タグ

C. MIME

D. 名前

Answer(s): D

---

13. エンジニアは、Nmap を使用して IDS デバイスで侵入ポートスキャン アラートをトリガーせずに、192.168.1.0/24 の範囲内で稼働中のホストを検出する必要があります。どのコマンドがこの目標を達成しますか?

A. nmap --top-ports 192.168.1.0/24

B. nmap -sP 192.168.1.0/24

C. nmap -sL 192.168.1.0/24

D. nmap -sV 192.168.1.0/24

Answer(s): B

---

14. ハイエンド テクノロジーを開発する組織が内部監査を受けています。 組織は 2 つのデータベースを使用しています。 メイン データベースには特許情報が保存され、セカンダリ データベースには従業員の名前と連絡先情報が保存されます。 コンプライアンス チームは、インフラストラクチャを分析して保護されたデータを特定するよう求められます。 この 2 つのうちどれですか保護されるデータの種類を特定する必要がありますか? (2つお選びください)

A. 個人識別情報 (PII)

B. ペイメント カード業界 (PCI)

C. 保護された炉床情報 (PHI)

D. 知的財産 (IP)

E. サーベンス・オクスリー法 (SOX)

Answer(s): A,D

---

15. サーバーにSyslog収集ソフトウェアがインストールされているログを封じ込めるために、FATタイプのパーティションを持つディスクが使用されます。エンジニアは、4GBのタイルサイズを超えるとログファイルが破損していると判断しました。問題を解決するアクションはどれですか？

A. 既存のパーティションにスペースを追加し、保持期間を下げます。

B. FAT32を使用して、4GBの制限を超えます。

C. 最大16 TBのファイルを保持できるため、Ext4パーティションを使用します。

D. ログファイルの封じ込めにNTFSパーティションを使用する

Answer(s): B

---

16. イベントを調査する場合、データの漏えいが発生したかどうかを判断するための調査機能を提供するのはどのタイプのデータですか？

A. フルパケットキャプチャ

B. NetFlowデータ

C. セッションデータ

D. ファイアウォールログ

Answer(s): A

---

17. 従業員に、仕事を遂行するために必要なリソースのみへのアクセスを許可する慣行は何ですか?

A. 最小権限の原則

B. 組織の分離

C. 職務の分離

D. 原理を知る必要がある

Answer(s): A

---

18. 改ざんされたディスクイメージと改ざんされていないディスクイメージがセキュリティインシデントに与える影響の 2 つの違いは何ですか? (2つ選んでください。)

A. セキュリティ調査過程で改ざんされていない画像を使用

B. 改ざんされた画像は、セキュリティ調査プロセスで使用されます

C. 保存されたハッシュと計算されたハッシュが一致する場合、画像は改ざんされます

D. 改ざんされた画像は、インシデントの回復プロセスで使用されます

E. 保存されたハッシュと計算されたハッシュが一致する場合、画像は改ざんされていません

Answer(s): A,E

---

19. 改ざんされたディスクイメージと改ざんされていないディスクイメージの違いは何ですか?

A. 改ざんされたイメージには、同じ保存および計算されたハッシュが含まれます。

B. 改ざんされた画像が証拠として使用されます。

C. 改ざんされていないイメージはフォレンジック調査に使用されます。

D. 改ざんされていない画像は証拠として保存するために意図的に変更されています

Answer(s): C

---

20. ユーザーは、コンテンツを開く前に、標的を絞ったスピアフィッシングメールを受信し、疑わしいと特定しました。このタイプのイベントは、サイバーキルチェーンモデルのどのカテゴリに属しますか？

A. 兵器化

B. 配達

C. 搾取

D. 偵察

Answer(s): B
