Implementing Cisco Cybersecurity Operations (210-255)

試験概要: Implementing Cisco Cybersecurity Operation (SECOPS) 試験（210-255）は、Cisco CCNA Cyber Ops 認定の取得に必要な試験のうち2つ目に受験する試験であり、試験時間は 90 分、問題数は 60 ～ 70 問です。セキュリティ オペレーション センター（SOC）内でアソシエイトレベルのサイバーセキュリティ アナリストとしてキャリアを目指すための第一歩となります。SECOPS 試験では、SOC に勤務するアソシエイトレベルのセキュリティ アナリストのタスク、任務、責務に必要な知識とスキルをテストします。

次に、この試験の一般的な出題内容を示します。ただし、試験によっては、ここに示されていない関連項目も出題される場合があります。試験内容をより適切に反映し、明確にするために、次のガイドラインは予告なく変更されることがあります。

15 %　1.0　エンドポイント脅威分析とコンピュータ調査

1.1 AMP Threat Grid や Cuckoo Sandbox などのマルウェア分析ツールの出力レポートの解釈

1.2 CVSS 3.0 で定義されているこれらの用語についての説明:
- 1.2.a 攻撃ベクトル
- 1.2.b 攻撃の複雑さ
- 1.2.c 必要な権限
- 1.2.d ユーザ関与
- 1.2.e 対象範囲

1.3 CVSS 3.0 で定義されているこれらの用語についての説明:
- 1.3.a 機密性
- 1.3.b 完全性
- 1.3.c 可用性

1.4 Microsoft Windows ファイル システムに関連するこれらの項目の定義:
- 1.4.a FAT32
- 1.4.b NTFS
- 1.4.c 代替データ ストリーム
- 1.4.d MACE
- 1.4.e EFI
- 1.4.f 空き領域
- 1.4.g ファイル システムのタイムスタンプ

1.5 Linux ファイル システムに関連するこれらの用語の定義:
- 1.5.a EXT4
- 1.5.b ジャーナリング
- 1.5.c MBR
- 1.5.d スワップ ファイル システム

1.5.e MAC

1.6 3項目の比較対照
- 1.6.a 最良証拠
- 1.6.b 補完証拠
- 1.6.c 間接証拠

1.7 2項目の比較対照
- 1.7.a 変更されたディスク イメージ
- 1.7.b 変更のないディスク イメージ

1.8 調査におけるこれらの属性の役割についての説明:
- 1.8.a アセット
- 1.8.b 攻撃者

22 % 2.0 ネットワーク侵入分析

2.1 基本的な正規表現の解釈

2.2 侵入分析に関連するこれらのプロトコル ヘッダー フィールドについての説明:
- 2.2.a イーサネット フレーム
- 2.2.b IPv4
- 2.2.c IPv6
- 2.2.d TCP
- 2.2.e UDP
- 2.2.f ICMP
- 2.2.g HTTP

2.3 セキュリティ イベントで発生する NetFlow v5 レコードの要素の特定

2.4 特定の PCAP ファイルでのこれらの侵入の主要要素の特定:
- 2.4.a 送信元アドレス
- 2.4.b 宛先アドレス
- 2.4.c 送信元ポート
- 2.4.d 宛先ポート
- 2.4.e プロトコル
- 2.4.f ペイロード

2.5 PCAP ファイルおよび Wireshark が与えられた場合の TCP ストリームからのファイルの抽出

2.6 イベントによく見られる以下のアーティファクト要素の解釈とアラートの特定:
- 2.6.a IP アドレス(送信元/接続先)
- 2.6.b クライアントおよびサーバ ポートのアイデンティティ
- 2.6.c プロセス(ファイルまたはレジストリ)
- 2.6.d システム(API 呼び出し)
- 2.6.e ハッシュ

2.6.f URI/URL

2.7 提示されたイベントとこれらのソース技術とのマッピング
- 2.7.a NetFlow
- 2.7.b IDS/IPS
- 2.7.c ファイアウォール
- 2.7.d ネットワーク アプリケーション コントロール
- 2.7.e プロキシ ログ
- 2.7.f ウイルス対策

2.8 これらの項目が与える影響と影響のない場合の比較対照:
- 2.8.a フォールス ポジティブ
- 2.8.b フォールス ネガティブ
- 2.8.c トゥルー ポジティブ
- 2.8.d トゥルー ネガティブ

2.9 提示された侵入イベントおよびホスト プロファイルの解釈と、Firepower Management Center(FMC)が生成する影響フラグの計算

18 % 3.0 インシデント対応

3.1 NIST.SP800-61 R2 でインシデント対応計画に含めるように指示されている要素についての説明

3.2 NIST-SP800-61 R2 に基づいた、各要素とこれらの分析ステップとのマッピング:
- 3.2.a 準備
- 3.2.b 検出と分析
- 3.2.c 封じ込め、根絶、リカバリ
- 3.2.d インシデント後分析(知見)

3.3 NIST IR カテゴリ(C2M2 p.2、NIST.SP800-61 R2 p.21 ～ p.41)と組織のステークホルダーとのマッピング:
- 3.3.a 準備
- 3.3.b 検出と分析
- 3.3.c 封じ込め、根絶、リカバリ
- 3.3.d インシデント後分析(知見)

3.4 所定の CSIRT の目標についての説明
(https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm)
- 3.4.a 社内 CSIRT
- 3.4.b National CSIRT
- 3.4.c 調整センター
- 3.4.d 分析センター
- 3.4.e ベンダー チーム
- 3.4.f インシデント対応プロバイダー(MSSP)

3.5 ネットワーク プロファイリングに使用されるこれらの要素の特定:

3.5.a スループット合計
3.5.b セッション継続時間
3.5.c 使用ポート
3.5.d 重要な資産のアドレス空間

3.6 サーバ プロファイリングに使用するこれらの要素の特定:
3.6.a リスニング ポート
3.6.b ログイン ユーザ/サービス アカウント
3.6.c 実行中のプロセス
3.6.d 実行中のタスク
3.6.e アプリケーション

3.7 これらのコンプライアンス フレームワークとデータ タイプとのマッピング:
3.7.a PCI
3.7.b HIPPA(医療保険の相互運用性と説明責任に関する法令)
3.7.c SOX

3.8 特定の標準(PCI-DSS)に関して保護する必要があるデータ要素の特定

23 % 4.0 データおよびイベント分析

4.1 データ正規化プロセスについての説明
4.2 共通のデータ値のユニバーサル形式での解釈
4.3 5 タプル相関付けの説明
4.4 グループ化された一連のログで感染したホストを切り分ける 5 タプル アプローチについての説明
4.5 ファイル分析レポートから悪意のあるファイルを見つけるレトロスペクティブ分析法についての説明
4.6 悪意のある IP アドレスまたはドメインを含む脅威分析レポートに基づいた、ネットワーク内での感染が疑われるホストの特定
4.7 攻撃者を見つけるための DNS ログと HTTP ログのマッピング
4.8 DNS、HTTP、および脅威インテリジェンス データのマッピング
4.9 Firepower Management コンソールを使用して複数のデータ ソースから得られた所定のイベント セットの中から、最も重要なアラートを見分けるための相関ルールの特定
4.10 確定的な分析および見込み的な分析の比較対照

22 % 5.0 インシデントの処理

5.1 侵入のダイヤモンド モデルで定義されているこれらのカテゴリへの侵入イベントの分類:
5.1.a 調査
5.1.b 武装化
5.1.c 配信
5.1.d エクスプロイト
5.1.e インストール
5.1.f 命令と制御
5.1.g 目的実行

5.2 イベントへの NIST.SP800-61 R2 インシデント対応プロセスの適用

5.3 インシデント処理に関連するこれらのアクティビティの定義:
- 5.3.a 特定
- 5.3.b 範囲設定
- 5.3.c 封じ込め
- 5.3.d 修復
- 5.3.e 知見に基づいた強化
- 5.3.f レポート

5.4 NIST SP800-86 で文書化されているこれらの概念の説明:
- 5.4.a 証拠収集指示
- 5.4.b データの整合性
- 5.4.c データの保管
- 5.4.d 揮発性データ収集

5.5 特定のインシデントへの VERIS スキーマのカテゴリの適用