コースの詳細

McAfee SIEM Advanced Administration 201

Customer Instructor-Led トレーニング

McAfee® SIEM アプライアンスは、すべてのシステム、ネットワーク、データベース、およびアプリケーションでのアクティビティをほぼリアルタイムで可視化するため、管理者は数分で IT インフラストラクチャ全体の脅威を検出して相関付けし、修復することができます。SIEM Administration 101 の続きとなるこのコースでは、SIEM の機能を利用したさらに詳しい分析手法について説明します。実践的なラボでの演習では、マカフィーが推奨するベストプラクティスと手法を活用し、アップグレード、調整、ワークフロー分析を通じて SIEM を最適化する方法を学習します。

推奨する事前作業

SIEM Administration 101 コースを修了した、SIEM アプライアンスの 1 年以上の使用経験がある方に推奨されるクラスです。

コースの目標

- SIEM アプライアンスを設置し、企業環境に合わせて構成する
- 企業の資産を活用して SIEM イベントにコンテキストを提供する
- ポリシールールの調整とカスタマイズを行う
- 効果的な相関ルールを記述する
- サードパーティフィードに組み込むワークフロービューを作成する

トピックの概要

1 日目

- クラスの紹介
- 講義 - 第 1 章: SIEM の設置と設定
- ラボ: SIEM デバイスのアップグレード
- ラボ: ESM と Receiver の設定
- 講義 - 第 2 章: SIEM でのコンテキストの設定

2 日目

- ラボ: ゾーンの定義
- ラボ: 資産のインポート
- ラボ: データエンリッチメントの実施

対象者

- このコースは、ネットワーキングとシステム管理の概念に関する実際的な知識、コンピュータセキュリティの概念に対する十分な理解、ネットワーキングとアプリケーションソフトウェアに関する一般的な知識と経験をお持ちの方を対象にしています。

今すぐトレーニングに登録する

intel Security

コースの詳細

トピックの概要 (続き)

- 講義 - 第 3 章: SIEM の操作と調整
- ラボ: 誤りのあるイベントのフィルタリング
- ラボ: 変数の設定
- ラボ: 相関ルールの修正
- 講義 - 第 4 章: 相関ルール

3 日目

- ラボ: カスタム相関ルールの作成
- 講義 - 第 5 章: ワークフローと分析
- ラボ: コンテンツパックの使用方法
- ラボ: URL アクションの実施
- ラボ: 脅威フィードのインポート
- ラボ: サイバー脅威フィードの使用方法
- ラボの開始: 最終試験の準備とディスカッション

4 日目

- ラボの続き:最終試験のプレゼンテーションとディスカッション

コースの概要

SIEM の設置と設定

- デバイスの概要
- SIEM ソフトウェアのアップグレード
- 手動ルール更新の実行
- データソースを初めて追加する際に推奨する方法
- すべてのデータソースがロギングされていることの検証
- ログイン認証のための AD への接続
- 変数の設定

SIEM でのコンテキストの設定

- ゾーンとタグの定義
- 資産インポートのための SIEM と Windows ドメインコントローラの接続
- データエンリッチメントの実施

SIEM の操作と調整

- ルールの調整
- 解析のカスタマイズ

相関ルール

- ルール相関
  - イベントフロー
  - ルールの記述

ワークフローと分析

- SIEM テクノロジ導入曲線のレビュー
- コンテンツパック
- ベースライン
- URL アクションの実施
- 脅威管理
- 脅威フィード
- 状況認識のユースケース

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com