McAfee Enterprise Security Manager の管理 SOC アナリスト・レベル1

研修サービス / インストラクターによるトレーニング
このコースを終了すると最大 32 の CPE を獲得します

McAfee Enterprise Security Manager ー当社の Security Information and Event Management（SIEM）の要ー はシステム、ネットワーク、データベース、およびアプリケーションのすべての活動をよりリアルタイムに可視化するソリューションを提供します。これにより、IT インフラストラクチャ全体において数分間で脅威を検出し、相関分析や復旧を実施することができます。このコースでは、Enterprise Security Manager のアナリストが Enterprise Security Manager が提供する機能を理解し、使用するための準備をします。実践的なラボ演習では、McAfee 推奨のベストプラクティスと方法論を使用して Enterprise Security Manager を最適化する方法を学習します。

アジェンダの概要

1 日目

- コースの紹介
- Enterprise Security Manager の概要
- Enterprise Security Manager のビュー
- データソース

2 日目

- Application Data Monitor と Database Event Monitor
- 集約
- ポリシーエディタ

3 日目

- クエリフィルタ
- 相関
- ウォッチリストとアラーム

4 日目

- レポート
- Enterprise Log Manager と Enterprise Log Search
- ラップアップシナリオ

対象者

Enterprise Security Manager のアナリストとして活動する管理者は、McAfee Enterprise Security Manager ソリューションを使用して、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のアクティビティを監視します。

受講者は、コンピュータセキュリティの概念と、ネットワーキングおよびアプリケーションソフトウェアの一般的な理解を十分に理解している必要があります。

学習目標

Enterprise Security Manager の概要

Enterprise Security Manager および SIEM の概念を定義し、アプライアンスとその機能を理解し、Enterprise Security Manager のソリューション・コンポーネント・アーキテクチャーについて説明します。

Enterprise Security Manager の インターフェイス ビュー

ダッシュボードを効率的に操作し、カスタムの Enterprise Security Manager データビューを作成します。

データソース

さまざまなデータソース、資産、豊富なデータを使用して、イベントを特定し、ケースを管理します。

Application Data Monitor と Database Event Monitor

Application Data Monitor と Database Event Monitor の機能を理解し、それぞれのデータソースを使用して特定のイベントを特定します。

集約

イベントとフローの集約に関連する利点と差異を列挙し、定義します。

ポリシーエディタ

Enterprise Security Manager ポリシーエディタをナビゲートし、高度な Syslog パーサールールが Syslog で受信したイベントをどのように解析するかを記述します。

クエリフィルタ

ビューでフィルタを適用し、フィルタセットを作成し、文字列正規化を使用し、正規表現の基本構文を理解します。

相関

複数のユースケースに対する複雑な相関ルールを設計する。

ウォッチリストとアラーム

ウォッチリストとアラームを作成および設定します。

レポート

レポートの作成と設定。

Enterprise Log Manager と Enterprise Log Search

Enterprise Log Manager および Enterprise Log Search でイベント情報を検索します。

ラップアップシナリオと最終試験

機密情報の盗難や弱いパスワードの使用など特定のイベントを特定するには、Enterprise Security Manager ダッシュボードとビューを使用します。

推奨する事前知識

- 受講者はアナリストとしての役割を理解し、Enterprise Security Manager と SIEM の用語に精通していることが推奨されます。

関連コース

- McAfee Enterprise Security Manager の管理 - エンジニア・レベル1
- McAfee Enterprise Security Manager の管理 - エンジニア・レベル2
- McAfee Enterprise Security Manager の管理 - SOC アナリスト・レベル2

McAfee Together is power.

マカフィー株式会社 www.mcafee.com/jp

東京本社 〒150-0043 東京都渋谷区道玄坂 1-12-1 渋谷マークシティウエスト 20F TEL：03-5428-1100（代） FAX：03-5428-1480
西日本支店 〒530-0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL：06-6344-1511（代） FAX：06-6344-1517