McAfee Enterprise Security Manager の管理 SOC アナリスト・レベル2

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 のインターフェイスビュー
- アナリストのタスク

2 日目

- ユースケースの概要
- マネジメント層からの指令に関連するユースケース

3 日目

- 組織ポリシーに関連するユースケース
- コンプライアンスに関連するユースケース

4 日目

- 現在の脅威に関連するユースケース
- インシデントの識別に関連するユースケース

対象者

Enterprise Security Manager ア ナリストとして活躍する管理者は、ユースケースの計画、設計、および文書化を担当します。

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。

アナリストのタスク

分析に従いチューニングの推奨事項を作成するため、即時、遅延または無アクションのイベントを特定し、Enterprise Security Manager が出力する情報の有用性を最大限に高めるアクションを選択します。

ユースケースの概要

ユースケースを定義し、明確なユースケースを開発するプロセスに沿うようにします。

マネジメント層からの指令に関連する ユースケース

機密データの抽出とファイルの削除に関連するマネジメント層の指令に関するユースケースを作成します。

組織ポリシーに関連するユースケース

電子メールコントロール、Web コントロール、サービス拒否（DoS）イベント、ログに関する組織ポリシーのユースケースを作成します。

コンプライアンスに関連するユースケース

業界規制等からユースケースを作成し、コンプライアンスを検証します。

現在の脅威に関連するユースケース

現在の脅威と自組織に対する脆弱性の調査からユースケースを作成します。

インシデントの識別に関連するユースケース

インシデントを調査し、ユースケースを作成して、以前に修復されたインシデントを迅速に特定します。

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。
- 受講者は、このコースに参加する前に、Enterprise Security Manager の管理 - SOC アナリスト・レベル1コースに参加する必要があります。

関連コース

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

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