Microsoft セキュリティ運用アナリスト
コース SC-200

クラスルーム型トレーニング : 4 日間

コースの説明

このコースでは、Azure Sentinel、Azure Defender、Microsoft 365 Defender を使用して、脅威の調査、対応、追跡を行う方法について説明します。また、これらのテクノロジーを使用してサイバー攻撃の脅威を軽減する方法についても取り上げています。具体的には、Kusto Query Language (KQL) に加えて Azure Sentinel を設定して使用し、検出、分析、レポート作成を行います。このコースは、セキュリティ運用の職務に就いている方を対象としています。

受講者のプロフィール

このコースの対象者

- セキュリティ エンジニア
- セキュリティ運用アナリスト

アジェンダ

1 日目

- Microsoft Defender for Endpoint を使用した脅威の軽減
- Microsoft 365 Defender を使用した脅威の軽減

2 日目

- Azure Defender を使用した脅威の軽減
- クエリ言語 (KQL) を使用した Azure Sentinel のクエリの作成

3 日目

- Azure Sentinel 環境の構成
- ログを Azure Sentinel に接続する

4 日目

- Azure Sentinel を使用して検出を作成し、調査を実行する
- Azure Sentinel を使用した脅威ハンティング

詳細情報

前提条件となる知識と実務経験 :

- Microsoft 365 に対する基本的な理解
- Microsoft のセキュリティ、コンプライアンス、ID 製品に対する基本的な理解
- Windows 10 に対する中程度の理解
- Azure サービス (特に Azure SQL Database と Azure Storage) に精通していること
- Azure Virtual Machine と仮想ネットワークに精通していること
- スクリプトの概念に対する基本的な理解

セキュリティは初めてですか ?

コース SC-900: Microsoft セキュリティ、コンプライアンス、および ID の基礎または Microsoft Learn のラーニング パスを受講してください。

このコースは、次の資格取得の準備にも役立ちます。

Microsoft 認定資格 : Security Operations Analyst Associate

試験 SC-200: Microsoft セキュリティ運用アナリス

試験で評価されるスキル

- Microsoft 365 Defender を使用した脅威の軽減
- Azure Defender を使用した脅威の軽減
- Azure Sentinel を使用した脅威の軽減

コースの詳細は コース SC-200 をご覧ください。

LxP でこのコースを予約する。

コース カバレッジ

25% レクチャー/ディスカッション | 25% デモンストレーション | 50% ハンズオン ラボ