コースコード：CO-SECAIPLUS
税込価格：176,000円 (税抜価格：160,000円)
日数：2日間

ここに注目!!

サイバー攻撃がAIを駆使して高度化している中、従来のセキュリティ知識だけでは対応しきれない時代になりつつあります。同時に、防御側としてもAIツールを使いこなし、セキュリティ業務に活用するスキルが重要視されています。
本トレーニングでは、AIシステムの安全確保だけでなく、セキュリティ運用におけるAIの適用やワークフローの自動化など、AIテクノロジーの活用方法も学びます。

CompTIA SecAI+は、AIシステムのセキュリティ対策や、サイバーセキュリティ分野におけるAIの実践的活用に焦点を当てた新たな認定資格で、CompTIAが提供する初のExpansion Seriesです。

受講対象者

このトレーニングはこのような方におすすめです。

セキュリティアナリスト、SOCアナリスト、ペネトレーションテスター、クラウドエンジニア、DevSecOpsエンジニア、リスク/コンプライアンスのプロフェショナルなど、すでにサイバーセキュリティの分野で実務経験があり、Security+、CySA+、PenTest+、SecurityXなどの主要なサイバーセキュリティ認定資格を保持しているか、同等の実務経験がある方

前提条件/前提知識

このコースを受講する前に受講者が習得しておく必要がある知識およびスキルは次のとおりです。

・3～4年のIT経験（少なくとも2年のサイバーセキュリティ実務経験を含む）
・AI対応セキュリティツールの基礎的な知識

下記のコースを受講済み、または同等の知識を有する方

CompTIA Security+ 任意、受講されていれば望ましい
CompTIA Cybersecurity Analyst (CySA+) 任意、受講されていれば望ましい
CompTIA PenTest+ 任意、受講されていれば望ましい
CompTIA SecurityX 任意、受講されていれば望ましい

目的

このコースを修了すると次のことができるようになります。

・AIの概念を適用して、組織のサイバーセキュリティ体制を強化します。
・高度な制御と保護を使用してAIシステムを保護し、データ、モデル、インフラストラクチャを保護します。
・AIテクノロジーを活用して、ワークフローを自動化し、インシデント対応を加速し、セキュリティ運用を拡張します。

・グローバルなGRCフレームワークをナビゲートして、業界全体で倫理的でコンプライアンスに準拠したAIの導入を確保します。
・敵対的攻撃、自動化されたマルウェア、生成AIの悪意のある使用など、AI主導の脅威から防御します。
・AIをDevSecOpsパイプラインとエンタープライズセキュリティ戦略に安全に統合します。

アウトライン

＜テキスト＞
1 サイバーセキュリティにおけるAIおよびデータの概念を概観する
1.1 サイバーセキュリティにおけるAI概念
1.2 AIモデルのトレーニングとプロンプトエンジニアリング
1.3 AIデータのセキュリティの確保
1.4 モジュールクイズ

2 脅威モデリング実装とAIシステムの安全確保
2.1 AI脅威モデリングの利用
2.2 AIシステムのセキュリティ制御の実施
2.3 モジュールクイズ

3 AIアクセス制御のインストール
3.1 AIのアクセス制御のデプロイ
3.2 AIセキュリティへのデータセキュリティ制御の適用
3.3 AIシステムの監視と監査の実施
3.4 モジュールクイズ

4 AI関連の脅威と補正コントロールの区別
4.1 AIライフサイクルにおけるセキュリティの重要性を示す
4.2 AIシステムへの攻撃を分析し、補正コントロールを活用する
4.3 モジュールクイズ

5 セキュリティにおけるAIの活用と、AIの悪用の理解
5.1 セキュリティタスクにAI対応ツールを使用する
5.2 AI対応およびAI強化型の攻撃ベクターを要約する
5.3 AIによるセキュリティタスクの自動化
5.4 モジュールクイズ

6 AIガバナンス、リスク、コンプライアンスの理解
6.1 AIのための組織的なガバナンス構造を分類する
6.2 AIに関連するリスクを定義する
6.3 コンプライアンスがAIのビジネス利用と開発に与える影響について説明する
6.4 モジュールクイズ

＜ラボ＞ ※コース内でのラボ実施は一部に限られます
1 サイバーセキュリティにおけるAIおよびデータの概念を概観する
1.1 サイバーセキュリティにおけるAI概念
1.2 AIモデルのトレーニングとプロンプトエンジニアリング
1.3 AIデータのセキュリティの確保

2 脅威モデリング実装とAIシステムの安全確保
2.1 AI脅威モデリングの利用
2.2 AIシステムのセキュリティ制御の実施

3 AIアクセス制御のインストール
3.1 AIのアクセス制御のデプロイ

3.2 AIセキュリティへのデータセキュリティ制御の適用
3.3 AIシステムの監視と監査の実施

4 AI関連の脅威と補正コントロールの区別
4.1 AIライフサイクルにおけるセキュリティの重要性を示す
4.2 AIシステムへの攻撃を分析し、補正コントロールを活用する

5 セキュリティにおけるAIの活用と、AIの悪用の理解
5.1 セキュリティタスクにAI対応ツールを使用する
5.2 AI対応およびAI強化型の攻撃ベクターを要約する
5.3 AIによるセキュリティタスクの自動化

6 AIガバナンス、リスク、コンプライアンスの理解
6.1 AIのための組織的なガバナンス構造を分類する
6.2 AIに関連するリスクを定義する
6.3 コンプライアンスがAIのビジネス利用と開発に与える影響について説明する