コースコード：CG-AISTB
税込価格：77,000円 (税抜価格：70,000円)
日数：1日間

ここに注目!!

AIを悪用した攻撃の手法を実際に体験できる演習を通じて、理論だけでなく体験を通して学んでいただきます。

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。

・これからAIの導入を検討している技術者や担当者の方
・すでにAIを活用しているが、セキュリティ対策が不十分な企業の従業員や管理者の方
・AIとサイバーセキュリティの両面からリスクを正しく理解し、より実践的な知識を身につけたい方

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。

・AIを利用したことがある方
・ChatGPTを使用します
※事前のダウンロードなどは必要ございません
・会議ツールはMicrosoft Teamsを使用します

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。

・生成AIの利用に伴うリスクを軽減
:情報漏洩や不適切利用によるインシデントを未然に防ぐ力を養います
・生成AIリテラシーの向上
:従業員一人ひとりが生成AIを正しく理解し、安全に活用できるなリテラシーを養います

アウトライン

座学：AIの基礎と歴史

AIの基本的な定義、その歴史的発展、現在の普及状況、そして基盤となる技術

座学：AIとサイバー脅威の現状

AIがサイバー攻撃にどのように活用され、現在の脅威状況がどうなっているか、統計データや攻撃と防御の非対称性

座学：AIセキュリティの課題とリスク

AIの導入・運用における新たなリスク、技術的・組織的な障壁、データプライバシーや整合性に関する課題

座学：AIの攻撃手法と悪用例

AIシステムに対する具体的な攻撃の種類、戦術、そして攻撃者がAIを悪用するためのツールや技術

演習：プロンプトインジェクションを体験しよう

プロンプトインジェクション攻撃を実体験することで、AI特有の攻撃について理解を深める

座学：AIの防御的活用とツール

AIがサイバーセキュリティの防御側にどのように役立つか、セキュリティチームの業務変革、およびAI駆動型ツール

演習：AIセキュリティのフレームワークとベストプラクティス

AIシステムのセキュリティを確保するための標準的なフレームワーク、ガイドライン、および実践的な対策

座学：今後の対策

AIとサイバーセキュリティの未来、今後の進化、および新たな脅威と防御の

形