コースコード：GX-SAIE
税込価格：220,000円 (税抜価格：200,000円)
日数：2日間

ここに注目!!

【攻撃・防御・設計を横断するカリキュラム】
攻撃者視点と防御の限界を理解したうえで、セキュリティ設計にまで落とし込む横断的なカリキュラムです。

【最新の業界標準フレームワークに準拠】
攻撃・防御・AIガバナンスの検討に活用できる最新の業界標準フレームワークに準拠した内容です。（OWASP, MITRE ATLAS, ISO/IEC 42001）

【個人ワークと最終成果物】
受講して終わりではなく、 自組織ですぐに使える実務的な 成果物を持ち帰ります。

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。

本講座は、AIを業務で扱うアプリケーション開発エンジニア、インフラ・運用を担うエンジニア、情シス担当者、セキュリティコンサルタントの方を主な対象としています。
AIを活用したシステム開発や業務改善に関わる中で、セキュリティ面の判断に不安を感じている方に特におすすめです。

・アプリケーション開発エンジニア
AIを組み込んだアプリケーションを攻撃を前提に設計する判断が求められる方

・インフラ／ネットワークエンジニア
AIを活用するシステムの基盤について、構成・運用・セキュリティの観点で判断する立場の方

・セキュリティコンサルタント／セキュリティエンジニア
AIを含むシステムについて、設計や構成の妥当性をセキュリティの観点から判断する立場の方

・AIを業務で使用している方
セキュリティ設計について、体系的に学んだことがなく不安を感じている方

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。

・ITの基礎知識
・セキュリティの基礎知識
・アプリケーションやインフラ系エンジニアとして、2-3年以上の実務経験を推奨

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。

本トレーニングは、AIを活用するだけでなく、攻撃・防御・設計・ガバナンスを踏まえて安全に判断できるエンジニアの育成を目的としています。

アウトライン

1．AI基礎：エンジニアが"安全に"AIを扱うための最低限の土台
AI・機械学習・生成AIの基礎構造を理解し、AIの限界や特性、誤用によるリスクを把握します。「AIの正しい前提知識」を身につけます。

2．AI活用：エンジニアとしてAIを業務に活かす実践スキル
コード生成やレビュー支援、ログ整理など、業務でAIを使う際の活用ポイントと注意点を学びます。「AIの出力を鵜呑みにしない」前提で安全に使いこなす力を養います。

3．生成AIを使ったサイバー攻撃・脅威の変化（攻撃者視点）
攻撃者がAIをどう悪用するかを理解します。フィッシングの高度化やマルウェア生成など、AIによって攻撃の敷居が下がる現状を学び、防御側視点の優先課題を把握します。

4．生成AIを使ったセキュリティ対策の現状（防御側視点）
SOC/CSIRTでのAI活用、ログ分析や異常検知など、防御側がAIをどう使うべきかを学びます。AIと人間の適切な役割分担や、過度な依存のリスクも整理します。

5．AIを組み込んだアプリケーション/基盤のセキュリティ（設計視点）
AI機能を持つシステムの設計で注意すべきポイントを学びます。入力・出力の安全性確保、ログ設計、外部AIサービス利用時の責任分界など、セキュリティを後付けではなく、「設計」から組み込むための視点を身につけます。

6．エンジニアとしてのAIガバナンス・責任・倫理
AI利用に関する社内ルール、機密情報リスク、責任所在の明確化など、組織的・倫理的な側面を学びます。AI導入を安全に進めるためのガバナンス視点を習得します。