コースコード：EC-COASP
税込価格：663,300円 (税抜価格：603,000円)
日数：5日間

ここに注目!!

AIシステムやLLM、AIエージェントを対象に、攻撃と防御を体系的に学べます。
以下3つの特徴があります。

1．AIを狙う攻撃者視点を体系的に理解
LLM、学習データ、AIインフラ、サプライチェーンなど、AIシステムに関わる複数の領域を網羅的に学習します。AIセキュリティを個別の攻撃手法だけでなく、評価・検証の観点から体系的に理解できます。

2．国際的なフレームワークを参照
OWASP LLM/ML Top 10、MITRE ATLAS、NIST AI RMFなど、AIシステムの脅威や攻撃手法を整理した国際的なフレームワークに基づいて、カリキュラムが構成されています。

3．ハンズオンを通じて実践的に学習
プロンプトインジェクション、モデル抽出、敵対的攻撃などを含む30の演習シナリオが用意されています。講義で知識を学ぶだけでなく、AIシステムに対する攻撃・検証スキルを実践的に習得できます。

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。

ペネトレーションテスター、脆弱性診断要員、セキュリティエンジニア、AIエンジニアにおすすめです。
・ペネトレーションテスター
・脆弱性診断要員
・セキュリティエンジニア
・AIエンジニア
・SOCアナリスト（L2, L3）

AIシステムを活用・提供・支援する企業に、COASPの導入価値があります。
AIを業務やサービス、開発プロセスなどに組み込む企業では、業種を問わず、攻撃者視点でAIシステムを検証し、セキュリティを強化できる人材育成が重要です。

AIシステムを開発する企業：SIer、システム開発会社など
顧客向けAIシステムやLLMアプリケーションのリスク説明・対策提案において、説得力や実践力を高められます。

AIサービスを提供する企業：SaaS企業、AIプロダクト提供企業など
RAGやAPI連携などを含むAIサービスの攻撃面を洗い出し、安全性検証や継続的な改善に活用できます。

セキュリティ支援を行う企業：セキュリティベンダー、コンサル会社など
AI特有の攻撃手法や脆弱性を理解し、診断、レッドチーミング、対応支援の高度化につなげられます。

高い説明責任が求められる企業：金融、医療、公共、重要インフラなど
機密情報・個人情報・業務継続性への影響が大きい領域において、AI活用に伴うリスクを技術的に評価し、安全な導入・運用判断に活かせます。

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。

・CCNAレベルのネットワークに関する知識
・PIC Level1程度のLinuxに関する知識
・企業で導入されているFirewallなどネットワーク・セキュリティ機器の構成に関する知識
・下記ツールの使い方に関する知識
Wireshark、tcpdump、nmap、ローカルプロキシ (Burp Suite、OWASP ZAP、Fiddler)
・AI/ML/LLMなど、AIシステムの基本的な仕組み

AIや機械学習の基礎概念の理解に不安がある方は、本講座の理解をより深めるため、
事前に「セキュリスト（SecuriST）®｜認定AIセキュリティエンジニア
」のご受講を推奨いたします。

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。

COASPは、さまざまな実践演習を通じて、AIセキュリティ関する攻撃・検証スキルを習得します。
以下は、演習で身につけられるスキルの一部抜粋です。
・AIモデルの脆弱性調査・堅牢性評価
・AIエンドポイントに対するAPI偵察・モデル抽出
・AIチャットボットにおけるプロンプトインジェクション・ペルソナベースの権限昇格
・AIシステムに対するRAGポイズニング・コンテキストプロンプトインジェクション
・AIエージェントに対する権限昇格・コマンドインジェクション

アウトライン

攻撃的AIとAIシステムハッキングの手法

AI偵察とアタックサーフェスのマッピング

AI脆弱性スキャンとファジング

プロンプトインジェクションとLLMアプリケーション攻撃

敵対的機械学習とモデルプライバシー攻撃

データおよび学習パイプライン攻撃

Agentic AIおよびモデル間攻撃

AIインフラおよびサプライチェーン攻撃

AIセキュリティテスト、評価、およびハードニング

AIインシデントレスポンスとフォレンジック