コースコード：VER-IOTHACK
税込価格：484,000円 (税抜価格：440,000円)
日数：3日間

ここに注目!!

・実機を用いたハンズオンで理解を深めます
Wi-Fiルーター等のIoTデバイスを題材に、ソフトウェア／ハードウェアの両面からセキュリティリスクを確認します。車載ECUを模擬した環境でCANプロトコルへの攻撃手法も扱います。

・IoTデバイス特有のリスクを横断的に学びます
ファームウェア解析、デバッグインターフェース、通信など、IoTデバイスに関わる複数の観点を扱います。

・攻撃者視点を設計・評価・対策に生かします
攻撃者がIoTデバイスのどこに着目するのかを理解し、設計レビュー、実装、評価、脆弱性対応、社内教育に生かせる視点を習得します。

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。

IoTデバイス／組み込み機器の以下に関わる方
・企画/設計/開発に関わる方
・検査/品質保証に関わる方
・導入/運用/インシデント対応に関わる方

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。

Linuxの基本操作経験がある方、コマンドライン操作に抵抗がない方

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。

・IoTデバイス、組み込み機器に特有のセキュリティリスクへの理解
・ファームウェア解析、ハードウェアインターフェース、通信解析の基礎
・IoTデバイスに対する攻撃者視点
・リバースエンジニアリングの基本的な考え方
・CANプロトコルおよび車載ECU攻撃手法の基礎
・設計レビュー、実装、評価、脆弱性対応、社内教育に生かせる観点

アウトライン

・1日目
IoTを取り巻く脅威やセキュリティの基本概念に慣れ親しんでいただくところから始まります。

その後、実際のIoTデバイスを想定した環境を用いて、機器の構成や外部から確認できる情報を調査し、潜在的なセキュリティ上の問題を発見する方法を学びます。
さらに、発見した問題がどのような影響につながるのかを検証し、IoTデバイスに対するセキュリティ評価の一連の流れを実践的に体験していただきます。

・2日目
IoTデバイスの内部構造や、機器を構成するハードウェアおよびソフトウェアの仕組みについて理解を深めます。
その知識を基に、機器内部に保存された情報やプログラムを調査・解析し、セキュリティ上の問題を発見する方法を学びます。
さらに、IoTデバイスやネットワークに対するさまざまな攻撃とその影響を体験すると共に、発見した脆弱性への対策や修正方法についても実践的に学習します。

・3日目
車載アーキテクチャの内部概念およびCANプロトコルを理解いただくところから始まります。
そして、車載を模擬したシミュレーション環境にて、CAN通信の内容を取得・解析し、その通信を再現する手法や、車載ECUのセキュリティ機能の一つであるUDSのSecurityAccess認証機能への攻撃など、車載ECUへのサイバー攻撃に関する基本的な手法を学習します。