コースコード：CG-IDE
税込価格：330,000円 (税抜価格：300,000円)
日数：2日間

前提条件

・PLCの操作設定について最低限の知識がある
・システム部門またはセキュリティ部門で１年以上従事経験がある
・インターネットブラウザを使用して日本語で各種情報を検索・閲覧できる

受講対象者

制御システム担当者、SOCアナリスト（OT）

コース概要

OT(Operational Technology)におけるサイバーセキュリティに必要な概念を習得します。特に、OT分野では一般的に用いられるPLCを交えた環境を想定し、セキュリティを確保するための技術と方法論について網羅的な知見を身につけることを目標とします。本トレーニングでは、イスラエルのセキュリティエンジニア率いるレッドチームと連携し、仮想化技術によって分離された安全な環境下で、工場プラントとPLCを用いた実際の攻撃をリアルタイムに体験します。

目的

制御装置への実際のサイバー攻撃を体験し、複数の検出・監視ツールを駆使してサイバーインシデントを検出し、その初期分析を行うためのスキルを習得します。
＜習得できるスキル＞
・複数の検出・監視ツールを駆使して、制御装置・システムにおけるサイバーインシデントを検出
・検出したインシデントの初期分析

アウトライン

1日目
●モーニングセッション
・トレーニング確認と進め方について
●産業制御システムの概念
・ICS基礎やICSでのセキュリティ概要や対策などの基本的なことについて
●ケーススタディ
・OT分野で実際に発生した脆弱性に対する攻撃や侵入インシデントに関してのケース スタディ
・コロニアルパイプライン、スタックスネット
●WireShark
・ネットワーク解析ツール「WireShark」の利用法解説
●WireShark演習
・演習用のキャプチャデータを「Wireshark」で解析するハンズオン演習
●ICS 攻撃ベクトル
・攻撃者が侵入するまでの流れや手法について
・使用されるプロトコル例（Modbus）
●ICS 侵入テスト 演習
・Kali Linuxを使用してペネトレーションテスト、（もしくはデモンストレーション）
●サマリ

・1日のまとめと質疑応答

2日目
●モーニングセッション
・スケジュール概要
●インシデントレスポンス（初動）
・インシデント対応プロセスや方法について
・初動対応について
●キックオフ
・アリーナを利用した演習について
●アリーナ環境説明(IT)
・ITシナリオのトレーニングで利用するアリーナのネットワーク構成やサービス、セキュリティシステム、インフラについて
●APT演習 (IT)
・ITシナリオデモ
●アリーナ環境説明(OT)
・OTシナリオのトレーニングで利用するOT環境の設備とワークステーションの紹介
●APT演習 (OT)
・OTシナリオ演習
●インシデント報告
・受講者によるOT演習内で取集した方向を元にインシデントの経緯や対処内容、今後の対策などの報告
●演習の振り返り
・攻撃者を交えた、演習の振り返り
●クロージングセッション
・講習全体の統括と質疑応答

※トレーニングプログラムは一部変更になることがあります
※単独開催の場合には、お客様に応じてカスタマイズも承っております