コースコード：CG-CTDE
税込価格：275,000円 (税抜価格：250,000円)
日数：2日間

前提条件

・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
※プログラミングの知識や経験は問いません

受講対象者

・IT担当者
・情報セキュリティ担当者
・SOCアナリスト
・情報処理安全確保支援士

コース概要

サイバーセキュリティの基礎となる理論と、実際にAPT攻撃を検知するのを実体験するハンズオンを含んだ実践的なトレーニングです。
ハンズオン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て実施します。仮想化技術で隔離され、安全に演習が実施できる環境下でAPT攻撃を体験できます。APT攻撃は熟練したホワイトハッカー（トレーニングを受けたサイバー攻撃のスペシャリスト）が実施し、トレーニングに有益なサイバーセキュリティの実践的な知見を導入致します。

目的

実際のサイバー攻撃を受け、複数の検出・監視ツールを駆使してサイバー攻撃を検出し、その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サイバーインシデント攻撃を検出
・検出したサイバー攻撃インシデントの初期分析

アウトライン

本コースは、オンライン開催(座学)と現地開催(演習)を組み合わせた2日間のトレーニングです。
下記PROGRAMのうち、★マークはオンライン受講対象カリキュラムです。
また、オンライン受講対象カリキュラムの副教材としてオンデマンド（ビデオ）を視聴いただけます。
オンラインならびにオンデマンド受講方法の詳細に関しましては、下記の『受講者向けガイドライン』をご参照ください。

受講者向けガイドライン

●オープニングセッション
・トレーニングの概要とスケジュール説明
●サイバーセキュリティの概念 ★
●アクティブディフェンスの概念 ★
・情報セキュリティの概念

・セキュリティシステムのレイヤー解説
●WireShark概要 ★
・ネットワーク解析ツール「WireShark」の利用法解説
●WireShark演習
・演習用の解析データを実際にWireSharkで解析するハンズオン演習
●Sysinternals概要 ★
・Windowsで利用できる汎用解析ツール「Sysinternals」をセキュリティの問題解析で利用する手法の解説
●マルウェアフォレンジック演習
・あらかじめマルウェアを配置したOS環境で脆弱性を検知する ハンズオン演習
●SIEM概論 ★
・SIEM(Security Information and Event Management)ツールの概要と操作に ついて解説
●アリーナインフラについて
・トレーニングで利用するアリーナのセキュリティシステムと インフラについて説明
●APT攻撃演習
・イスラエルのレッドチームが行うAPT攻撃に対して、受講者（ブルーチーム）がチームで連携して攻撃を検知・防御するハンズオン演習
●演習レビュー
・行われたAPT攻撃演習の振り返り
●クロージングセッション
・講習全体の総括と質疑応答

＜習熟度評価基準＞
演習に取り組んだ結果の報告提出を求め、あらかじめ設定した各演習目標に到達していてかつ所要時間内で演習を完遂できたかをもって習得技術の把握・測定を行います。
＜修了認定の判断基準＞
・修了認定は、演習問題の審査に合格した者に対して行います
・演習結果において、60点以上を合格とします

※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