コースコード：CG-FT
税込価格：440,000円 (税抜価格：400,000円)
日数：2日間

前提条件

・セキュリティ業務経験3年以上 ・オペレーティングシステム／ネットワークについての理解

受講対象者

IT担当者、情報セキュリティ担当者、情報処理安全確保支援士

コース概要

フォレンジックの能力を習得します。

目的

実践的なトレーニングを通じて、組織内におけるデジタルフォレンジックの全工程を自ら組み立て、中心的立場で実行することができる能力を習得します。
＜習得できるスキル＞
・ワークステーション内のマルウェアを発見し、被害状況や影響範囲を確認
・ネットワークフォレンジックを理解し、攻撃者や攻撃ツールを特定し、影響範囲を確認
・エビデンスの収集についてのルールや手法

アウトライン

●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
●ファーストレスポンダー
・役割と責任
・方法論（インシデント対応）
●マルウェアの概要
・APTモデルフェーズ
・マルウェアの種類
・検出技術
●Sysinternalsの概要
・Process Explorer, TCP View, Process Monitor, Autoruns
・不審な兆候
・実演
●演習フォレンジック①
・感染したワークステーションを個別に分析し、収集したデータを分析して、感染が疑われるかどうか、またどのワークステーションが疑わしいかを判断する
●演習フォレンジック②
・感染したワークステーションを個別に分析し、収集したデータを分析して、感染が疑われるかどうか、またどのワークステーションが疑わしいかを判断する
●デジタルエビデンスの収集
・証拠収集のために使用される方法とツール
●デジタルエビデンス収集のタイムライン
・学習したツールと手法を活用して、感染したマシンからデータをエクスポートする

●ネットワークフォレンジックの概要
・ネットワークフォレンジックの概要
・ネットワークフォレンジックの方法論
・マルウェア通信
・不審な兆候
・パケット分析
・シグニチャベースのネットワークトラフィック
●ネットワークフォレンジック演習
・総合演習
●機密ファイルを盗む -上級
・組織のネットワークから機密情報を盗む
●クロージングセッション
・講習全体の総括と質疑応答

※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