コースコード：CG-SIDT
税込価格：660,000円 (税抜価格：600,000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

コース概要

SIEMの概要からシステム使用方法までを体系的に学習します。

目的

SIEMとデータソースを最適化しながらシステム侵入やデータ侵害の検出を分析のスキルを習得します。
＜習得できるスキル＞
・SIEMとそのデータソースを最適化しながら、サイバー攻撃を特定する
・システム侵入やデータ侵害の検出と分析をし、SIEMのルールを最適化する

アウトライン

1日目
●オープニングセッション
・スケジュール確認と進め方
●インシデントレスポンス（CSIRT＆SOC概要）
・インシデントハンドリング方法論
・インシデントマネジメントチームやSOCについての概要
●ログ分析
・ログ解析についての講義
●ログ分析 演習
・ファイアウォールやWindowsログ、アクセスログなどを解析する
●SIEM概論
・SIEMの基本について
●Qradarアーキテクチャ
・基本的なSIEM構造（Qradar）の理解
・Qradarの基本的な使用方法
●Qradar 基本リソース
・Qradarをベースとして、SIEMで一般的に使用されるフィルダーやルール設定の方法
●Qradar フィルター 演習
・Qradarのフィルター機能やサーチ機能の演習
●Qradar ルール 演習
・Qradarのルールの設定
●デイリーサマリ
・その日の要約とフィードバック

2日目

●オープニングセッション
・スケジュール確認と進め方
●Qradar ルール 演習
・Qradarのルールの設定
●キックオフ
・APT演習の概要やルールの説明、役割分担環境確認
●Qradarルール作成
・攻撃に備えQradarのルールの作成を行う
●APT演習
・総合演習
●デブリーフィング
・攻撃とQradarのルールの振り返り
●デイリーサマリ
・その日の要約とフィードバック

※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