コースコード：GX-MicroHardening
税込価格：132,000円 (税抜価格：120,000円)
日数：1日間

前提条件

インターネットに関する知識 ECサイトの構造を理解していること
SSHを使いLinuxのリモートホストに接続し、コマンドを実行できること

受講対象者

情報システム部門のエンジニア
CSIRTメンバーやSOC担当者
セキュリティエンジニアやテクニカルコンサルタント
公開系システムを開発、運用するエンジニア
エンジニア職の新入社員

コース概要

本コースは、サイバー攻撃を「知っている」から「対応できる」レベルへ高めることを目的としたトレーニングです。
1セット45分間の実践演習を4セット繰り返し行います。ECサイトの管理者としてインシデント対応を体験することで、現場において必要な経験と対応イメージを体得します。
毎回同じタイミングで同じ攻撃が発生するように設定されていますので、再チャレンジするたびに少しずつ攻撃の状況を把握し、対処方法を実際に試すことで、どのような事が起こるのかというスリルと、クリアする快感を伴って「経験」できます。
今まで培った知識を現実に即した「攻撃への対処」として実践する事で、短時間で大きな経験が得られると共に、現在の“ 自身のインシデント対応力 ”を確認し、今後の強化Pointを明確にすることができます。
(活用シーン)
・CSIRTチームやSOC担当者の対応訓練
・情報システム部門のインシデント対応訓練
・テクニカルコンサルタントやエンジニアのインシデント対応訓練
・インフラエンジニア、運用エンジニアの対応訓練 など

目的

被害を受けるパターンとその対策について疑似体験を通して学びます。
サイバー攻撃発生時の対応方法をインシデン対応の実経験を通して習得することができます。
インシデント対応に於ける見える化と事前準備の重要性を認識することができます。
インシデント対応の運用とチームコミュニケーションの重要性を経験を通し理解できます。

アウトライン

《1日の流れ》
1. 事前解説：ルールと環境について解説します
2. インシデント対応演習（1セット45分 x 4セット）：
様々なサイバー攻撃からECサイトを守り、最大の売上を目指すチーム対抗戦
3. チームディスカッション
4. 解説&フィードバック

オンライントレーニングにご参加の方は、以下のページをご覧ください。