コースコード：TO-CYBER2
税込価格：217,800円 (税抜価格：198,000円)
日数：3日間

前提条件

一般的なOS、コンピュータ・アーキテクチャ、ネットワーキングの基本概念に関わるある程度のスキル
サイバーセキュリティ、セキュリティ技術に関するある程度の知識

受講対象者

情報セキュリティの責任者/監査人/専門家

コース概要

標的型攻撃手法を理解し、実践することで対処方法に役立てる事を目的としたトレーニングです

目的

サイバーレンジトレーニングとは、攻撃手法を理解し、実践することで対処方法に役立てる事を目的としたトレーニングです。
実際に日本で発生した標的型攻撃を再現したシナリオに沿って、まずは攻撃する側になって擬似的に用意した攻撃対象ネットワークに侵入します。その後、自身が行った攻撃をサイバー攻撃分析官の立場として分析します。
1日目は、最新のサイバー空間における脅威および、標的型サイバー攻撃に使用されるコマンドなどを学びます。続いて、攻撃を理解した上で攻撃の敷居を上げるためのハードニング手法を学びます。
2日目は、King Of The Hill形式で1日目に学んだ手法を用い、攻撃者に扮し、日本を標的にした実際の攻撃シナリオに沿って、疑似的に用意された企業ネットワークに侵入し、機密情報を盗み出します。
３日目は、インシデントハンドラーとしてフォレンジック、マルウェア技術を駆使し、調査、分析を行い、自身が実施した攻撃が端末上にどのような痕跡を残すのか、また残さないのかを学び、攻撃の成功を妨げたり、記録する手法について考えていきます。

アウトライン

1. サイバー空間の脅威について
2. 標的型攻撃について
3. 侵入前調査に使われる手法について
4. 内部侵入に使われる手法について
5. 情報探索に使われる手法について
6. コンピュータネットワークと防衛の基礎
7. ホストセキュリティ
8. ActiveDirectory ハードニング
9. King Of The Hill
10. インシデント対応プロセス
11. 証拠保全について
12. 不審なプロセスの調査
13. 不審なプログラムの動的解析
14. イベントログ解析
15. ディスクフォレンジック
16. OSINTを使った攻撃調査