コースの詳細

Ultimate Malware Analysis

Foundstone® Services トレーニングコース

TM

詳細な技術を紹介するこの包括的なコースを受講すると、インシデントに適切に対応し、セキュリティ体制を強化することができます。環境保護を担当する IT プロフェショナルは多くの作業に追われているため、マルウェア攻撃に対応できないことや、攻撃を誤ってシステムやネットワークの問題と診断してしまうことがあります。このコースでは、マルウェア関連のインシデントを特定して対応し、環境を正常な状態に戻すために必要なテクニックを習得できます。

コースの目標

- 攻撃を特定して対応する
- 適切なフォレンジック調査を実施する
- マルウェア解析

トピックの概要

- はじめに
- インシデント対応
- ライブ対応とネットワークの調査
- ドキュメント分析
- マルウェア解析
- ルートキットとメモリ分析
- ネットワークフォレンジック

対象者

- このコースは、マルウェアアウトブレークやネットワーク調査を担当するネットワーク管理者、企業セキュリティ担当者、監査担当者、警察官、コンサルタントを対象としています。

intel Security

コースの詳細

推奨する事前作業

このコースで得られる成果を最大限に高めるには、UNIX、Windows OS、コンピュータフォレンジック、TCP/IP ネットワーキングに関する基本的な知識が必要です。

コースの概要

モジュール 1—はじめに

- はじめに
- 目的
- コースの目標
- 教室内のルール
- インシデント対応とマルウェアについて

モジュール 2—インシデント対応

- マルウェアの分類
- 感染媒体
- マルウェアの繁殖
- ブラウザマルウェア

モジュール 3—ライブ対応とネットワークの調査

- ライブ対応について
- オープンソースツールを使用したドメインと IP の調査

モジュール 4—ドキュメント分析

- 攻撃媒体
- PDF 難読化技法
- Adobe SWF の分析
- PDF ファイル
- 悪質な Office ドキュメント

モジュール 5—マルウェア解析

- 静的解析と動的解析の比較
- マルウェアのプロファイリング
- 動的解析
- 武装化されたマルウェア
- 静的解析
- 解析の自動化

モジュール 6—ルートキットとメモリ分析

- ルートキット
- メモリの理解
- 揮発性メモリからのメモリダンプの分析
- 持続メカニズム
- メモリダンプに対するアプローチ
- Firewire とコールドブート攻撃

モジュール 7—ネットワークフォレンジック

- ネットワークセキュリティ監視 (NSM) ツール
- Wireshark と Snort
- マルウェアの動作とパターン
- Wireshark と Network Miner

To order, or for further information, please call 1 888 847 8766 or email SecurityEducation@intel.com.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com