コースの詳細

McAfee® Advanced Threat Defense Administration コース

Intel Security Education Services Administration コース

TM

Intel Security の研修サービスが実施している McAfee® Advanced Threat Defense Administration コースは、McAfee Advanced Threat Defense アプライアンスのセットアップ、構成、管理、および総合的なネットワークセキュリティ環境へのこのアプライアンスの統合方法の実践的なトレーニングを提供します。

コースの目標

- マルウェア解析用のサンドボックスイメージのメリットを理解するとともに、構成と管理を行う
- ネットワークを介して送信されるマルウェアを検出して解析する
- ATD を他の McAfee 製品 (McAfee Web Gateway、McAfee Threat Intelligence Exchange など) に統合する
- McAfee Advanced Threat Defense レポートを表示/エクスポートする

トピックの概要

1 日目

- このコースについて
- マルウェアの概要
- インシデント対応の概要
- ATD の概要
- ATD の導入戦略
- ATD のアーキテクチャ
- ATD の設置
- ATD のコマンドラインと Web インターフェイス
- ライセンスとアップデート
- ロギング
- 管理者の構成

対象者

- このコースは、システム管理者、ネットワーク管理者、セキュリティ担当者、監査担当者、およびネットワークやシステムセキュリティに関連しているマルウェアアナリストを対象としています。

今すぐトレーニングに登録する

intel Security

トピックの概要（続き）

2 日目

- ATD ポリシー
- 仮想イメージの作成
- ATD 統合
- マルウェア解析
- レポートと通知

3 日目

- McAfee Data Exchange Layer と Threat Intelligence Exchange
- ATD と TIE の統合

4 日目

- インシデント対応のレビュー
- トラブルシューティング

推奨する事前作業

Microsoft Windows の管理、コンピュータセキュリティの基本的な概念、一般的なインターネットサービスの実用的な知識を習得しておくことを推奨します。

コースの概要

モジュール 1：このコースについて

- McAfee University のカリキュラム
- はじめに
- このコースについて
- 演習の環境

モジュール 2：マルウェアの概要

- マルウェアのタイプ
- マルウェアのタイプ
- マルウェアの媒体
- マルウェアの検出
- マルウェアのライフサイクル

モジュール 3：インシデント対応の概要

- インシデント対応の原則
- インシデント対応ライフサイクル
- インシデント対応と ATD

モジュール 4：ATD の概要

- セキュリティ環境内の ATD
- ATD の静的および動的解析
- サポートされるファイルタイプ

モジュール 5：ATD の導入戦略

- ネットワークトポロジ
- ATD のインタラクション
- ATD と GTI

モジュール 6：ATD のアーキテクチャ

- ATD アプライアンスのハードウェア
- ATD のアーキテクチャ
- リモートの管理と監視
- ATD ネットワークポート

モジュール 7：ATD の設置

- ATD の設置と構成
- ATD の接続

モジュール 8：ATD のコマンドラインとオペレーティングシステム

- Advanced Threat Defense のコマンドラインインターフェイス
- 主な CLI コマンド
- ATD の Web インターフェイス
- [Dashboard] タブ
- [Analysis] タブ
- [Policy] タブ
- [Manage] タブ

モジュール 9：ライセンスとアップデート

- Advanced Threat Defense のライセンス
- ATD ディスクのセットアップ
- ATD アプライアンスのアップデート
- ATD のバックアップ
- 設置のトラブルシューティング

コースの詳細

モジュール 10: ロギング
- ATD ロギング
- システムのログとステータス
- ATD ダッシュボード

モジュール 11: 管理者の構成
- ATD のユーザー
- ATD の役割
- 管理者ポリシーの構成

モジュール 12: ATD ポリシー
- ATD ポリシー
- VM プロファイル
- アナライザープロファイル
- ATD マルウェアインターネットアクセス
- ATD ポリシーワークフロー

モジュール 13: 仮想イメージの作成
- 仮想マシンの作成
- VMDK ファイルの作成
- ATD 用オペレーティングシステムの設定
- ATD への VMDK のインポート
- VMDK ファイルから ATD イメージファイルへの変換

モジュール 14: ATD 統合
- ATD 統合の概要
- FTP
- RESTful API
- McAfee Web Gateway
- Network Security Platform
- ホストオペレーティングシステムの識別
- ePO との統合

モジュール 15: マルウェア解析
- サポートされるファイルタイプ
- ATD マルウェア解析
- ホワイトリスト
- ブラックリスト
- マルウェアエンジンと GTI
- サンドボックス解析
- 解析ステータス

モジュール 16: 通知とレポート
- ATD 解析レポート
- ATD サンドボックス解析サマリー
- ドロップされたファイル
- 逆アセンブリ結果
- ロジックパスグラフ
- ユーザー API ログ
- 完了結果
- ATD レポート形式
- ATD 通知

モジュール 17: McAfee DXL/TIE
- McAfee Data Exchange Layer
- McAfee Threat Intelligence Exchange
- TIE ワークフロー
- TIE サーバーの構成

モジュール 18: ATD と TIE の統合
- ATD DXL/ePO の構成
- ePO ポリシーの構成
- マルウェア解析ワークフロー
- ePO レポート

モジュール 19: インシデント対応のレビュー
- マルウェアインシデントレポートライフサイクル
- 準備
- 検出
- 解析
- 封じ込め、駆除、復旧
- インシデント後の活動

モジュール 20: トラブルシューティング
- ATD トラブルシューティングリソース
- ATD のトラブルシューティング
- ATD ログファイル
- ATD の一般的な問題
- 統合のトラブルシューティング

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