McAfee Network Security Platform の管理

研修サービス / インストラクターによるトレーニング
このコースを終了すると最大 32 の CPE を獲得します

McAfee の研修サービスが実施している McAfee Network Security Platform の管理コースは、侵入防止戦略を成功に導くために不可欠なトレーニングです。実践的なラボ演習では、実際の攻撃から組織を保護する Network Security Platform ソリューションの導入および構成方法を習得します。ここで習得した新しいスキルをビジネスの保護のために即座に利用し、Network Security Platform への投資を最大限に活用することができます。

アジェンダの概要

1 日目

- はじめに
- Network Intrusion Prevention について
- 計画
- 基本操作
- ユーザー管理
- 管理ドメイン
- Network Security Sensor の概要
- 基本的なセンサー管理

2 日目

- 仮想化（サブインターフェイス）
- ポリシーの構成
- ポリシーのカスタマイズ
- Threat Explorer
- 高度なマルウェアからの保護

3 日目

- 高度なボットネットの検出
- サービス拒否攻撃
- エンドポイントのレピュテーション
- Web サーバー保護

4 日目

- Threat Analyzer
- ファイアウォールポリシーの構成
- ポリシーの調整
- レポートの生成
- 運用ステータス
- データベースの保守

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コンサルタントを対象としています。

コースの概要

モジュール 1：はじめに

- このコースについて
- 略語と用語
- コースの計画
- McAfee Business Web サイト上のリソース
- マカフィー製品トレーニング
- セキュリティトレーニング
- ServicePortal
- セキュリティコンテンツのリリースノート
- 製品の機能改善リクエスト
- ビジネスコミュニティ
- 役立つリンク
- 教室ラボのトポロジ

モジュール 2：Network Intrusion Prevention について

- セキュリティの脅威：高まるリスク
- 脅威と攻撃とは
- 一般的な攻撃のタイプ
- 攻撃の動機と要因
- 侵入検知と侵入防止の比較
- 侵入防止システムのタイプ
- Network IPS が重要な理由
- Network Security Platform の概要
- このリリースの新機能
- ソリューションのコンポーネント
- 攻撃検出フレームワーク
- トラフィックの正規化
- NSP の 10 の使用手順
- 侵入防止を超えて

モジュール 3：McAfee Network Security Platform の導入計画

- 導入オプションの選択
- 導入の要件と推奨事項
- NSM サーバーの要件
- NSM クライアントの要件
- 画面表示とブラウザの設定
- 仮想サーバーの最小要件
- 仮想マシンの要件
- NSP 8X センサーのサポート
- NSP サーバーポート
- デスクトップファイアウォールの要件
- NSM でのウイルス対策ソフトウェアの使用
- Wireshark
- 単一および中央の NSM の導入
- データベース要件の決定
- センサーの導入
- センサー配置の決定 センサー数の決定
- 高可用性と障害時復旧
- 実装プロセスチェックリスト

モジュール 4：基本操作

- Manager インターフェイスへのログイン
- Manager インストールウィザード
- Manager インターフェイスへのアクセスの検証
- 運用モニター

推奨する事前知識

Microsoft Windows の管理、システム管理の概念、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。

- セキュリティモニター
- Manager インターフェイスのナビゲーション
- ダッシュボードモニターの管理
- 基本機能のセットアップ
- Manager Disaster Recovery（MDR）の概要
- MDR ペアの構成
- Central Manager の概要
- Central Manager プロキシサーバーでの信頼の定義
- プロキシサーバーの構成
- IPS イベント通知の概要
- IPS イベントのサマリーの表示
- Simple Network Management Protocol（SNMP）の概要
- SNMP 通知の構成
- Syslog 通知の概要
- Syslog 通知の構成
- 電子メールサーバーと通知の概要
- 電子メールサーバーと通知の構成
- スクリプト通知の構成
- 障害通知の概要
- 障害通知の構成
- 障害の一般的な設定の構成
- アクセスイベント通知の概要
- ユーザーアクティビティの概要
- ユーザーアクティビティの構成：SNMP
- ユーザーアクティビティの構成：Syslog
- Global Threat Intelligence（GTI）の 概要
- GTI 統合の要件
- GTI 統合の有効化

モジュール 5：ユーザー管理

- ユーザー管理の概要
- 最小限のアカウントの構成
- ロール割り当ての概要
- ロールと特権の表示
- デフォルトのルート管理ユーザーの編集
- ユーザーの追加、編集、削除
- ユーザー資格情報の検証
- カスタムロールの作成
- ドメインとロールの割り当て
- My Account の管理
- GUI アクセスの管理
- ユーザーアクティビティの表示
- バナーテキストとイメージの構成
- セッション制御の構成
- パスワード制御の構成
- 監査設定の指定
- 認証
- 認証構成のサマリー
- LDAP 外部認証
- LDAP の構成（最大 4 サーバー）
- LDAP 認証の割り当て
- RADIUS 外部認証
- RADIUS 外部認証の構成
- RADIUS 認証の割り当て

モジュール 6：管理ドメイン

- 管理ドメインの概要
- 管理ドメインの階層構造

- 管理ドメインの仕組み
- 管理ドメインの管理
- ルート管理ドメインの編集
- 子管理ドメインの追加
- 子ドメインへのユーザーの追加

モジュール 7：Network Security Sensor の概要

- M シリーズセンサーポートフォリオ
- NS シリーズセンサーポートフォリオ
- 仮想 IPS シリーズセンサーポートフォリオ
- センサーの主な機能
- 応答
- 検査
- 分類
- キャプチャ
- 仮想化（サブインターフェイス）
- セキュアソケットレイヤー（SSL）復号化
- アクセラレーションと動作
- 動作モード
- フェイルクローズとフェイルオープン（インラインのみ）
- マルチポートの監視
- インターフェイスグループ（ポートクラスタリング）
- 高可用性
- 大規模ネットワーク：境界、コア、内部への 配置
- ベストプラクティス

モジュール 8：ネットワークセキュリティにおける基本的なセンサー管理

- 物理センサーの設置
- 仮想センサーのインストール
- センサーの管理
- [Devices] ページ：[Global] タブ
- [Devices] ページ：[Device] タブ
- Manager でのセンサーのインストール
- トラストの確立
- シグネチャセットのダウンロード
- デバイスサマリーのレビュー
- 物理ポートの表示 / 編集
- ポートタイプ
- 名前解決
- ネットワークタイムプロトコル（NTP）
- プロキシサーバー
- アクティビティレポートとログのレビュー
- CLI ロギング
- IPS イベントロギング
- アラートオプション
- リモートアクセス：TACACS+
- リモートアクセス：NMS ユーザーとデバイス
- ログインバナーのカスタマイズ
- 特別な構成
- 高可用性
- ATD 統合の概要
- DXL 統合の概要
- 保守
- 保留中の変更の展開
- デバイスソフトウェアの導入
- トラブルシューティング
- パフォーマンス監視

モジュール 9：仮想化

- 仮想化（サブインターフェイス）の概要
- 有効なインターフェイスのタイプ
- 仮想化前と仮想化後
- VLAN および CIDR の論理構成
- VLAN のブリッジ
- ポリシーの適用
- 方向の決定
- VLAN タグ付け
- ダブル VLAN タグ付け
- CIDR ブロックオプション
- VLAN 仮想インターフェイスの構成
- CDIR 仮想インターフェイスの構成
- VLAN 仮想インターフェイスの構成
- VLAN サブインターフェイスの構成
- CDIR サブインターフェイスの構成

モジュール 10：ポリシーの構成

- 侵入防止の概要
- ポリシーとは
- ポリシーの用語と概念
- シグネチャ
- 攻撃の定義
- IPS ポリシーのタイプポリシーの割り当て
- 継承
- ポリシーの適用方法
- ポリシー管理の概要
- 管理ドメインの IPS ポリシーの追加
- 管理ドメインの IPS ポリシーのコピー / 編集
- 管理ドメインの IPS ポリシーの削除
- インターフェースの IPS ポリシーの追加
- インターフェースの IPS ポリシーの編集
- IPS ポリシーページの使用
- プロパティの定義
- 攻撃定義の表示
- ポリシーの割り当て
- Policy Manager の使用
- [Interface] タブ
- 変更の展開
- ポリシーバージョンの管理
- ポリシーの削除
- ポリシーのインポートとエクスポート
- レガシー偵察ポリシーの管理
- 偵察攻撃設定マージユーティリティ

モジュール 11：ポリシーのカスタマイズ

- 攻撃定義の仕組み
- [Traffic Processing and Analysis Attack Definitions] タブ
- 攻撃の分類と重大度
- 攻撃保護カテゴリ
- [Attack Definitions] タブ
- ビューのカスタマイズ
- [Attack Definitions] タブ:クイック検索、ソート、列、グループ、フィルタ、詳細
- [Attacks Detail] ペイン：説明
- 無害なトリガの可能性（Benign Trigger Probability：BTP）
- [Attacks Detail] ペイン：[Settings] タブ
- ポリシーグループの管理

モジュール 12：Threat Explorer

- 脅威の分析
- Threat Analyzer ビューのカスタマイズ
- ソース / 宛先 IP アドレスの分析
- 上位の攻撃
- 上位の攻撃者
- 上位のターゲット
- 上位のアプリケーション
- 上位の攻撃実行ファイル
- 上位のマルウェア
- ガイドライン

モジュール 13：高度なマルウェアからの保護

- 高度なマルウェアからの保護の概要
- マルウェア対策エンジン
- ポリシー管理の概要
- 高度なマルウェア対策ポリシーの構成の概要
- [Advanced Malware Policies] ページの使用
- Policy Manager の使用
- マルウェア対策ポリシーパラメータ
- ファイルタイプ
- ブラックリスト / ホワイトリストエンジン
- TIE/GTI レピュテーションエンジン
- PDF 解析エンジンと Flash 解析エンジン
- ゲートウェイマルウェア対策エンジン
- ATD エンジン
- McAfee クラウドエンジン
- マルウェアエンジン解析順序
- 信頼性レベル
- アクションしきい値
- マルウェア解析
- マルウェア解析の概要
- 上位マルウェア検出モニター
- [Malware Detections] ページ
- マルウェアファイルのアーカイブ
- ベストプラクティス

モジュール 14：高度なボットネットの検出

- 高度なボットネットの検出の概要
- ゼロデイおよび標的型ボットネットの検出
- ヒューリスティック
- 実装済みヒューリスティックの例
- 既知のボットネットの検出
- C&C サーバー / コールバックの検出
- DNS 応答パケットの検査
- ホワイトリスト / ブラックリストドメインの検出
- 例：ブラックリストドメインの検出
- 検査オプションポリシー
- 検査オプションポリシーの仕組み
- ポリシー管理の概要
- 検査オプションポリシーの構成の概要
- [Properties] タブ
- [Inspection Options] タブ
- トラフィックの検査の構成
- 高度なボットネットの検出の構成
- 高度なボットネットの検出オプション
- レガシーマルウェアの検出オプション
- センサーリソースへのポリシーの割り当て

- 変更の展開
- ボットネットの分析
- 上位のアクティブなボットネットモニター
- [Active Botnets] ページ：組織

モジュール 15：サービス拒否攻撃の構成

- DoS 攻撃の進化
- DoS 攻撃のタイプ
- ボリュームベース攻撃
- DoS 学習モード
- DoS 学習攻撃
- DoS 学習攻撃のカスタマイズ
- DoS 学習プロファイルの管理
- DoS しきい値モード
- ボリュームベース攻撃のしきい値の構成
- 接続制限ポリシー
- 接続制限ポリシーの追加
- レート制限（QoS ポリシー）
- QoS とレート制限の構成の概要
- QoS ポリシーの追加
- レート制限ルールの構成
- プロトコル設定
- プロトコル設定の構成
- スプーフィング対策
- ステートフル TCP エンジン
- DNS 保護コマンド
- ケーススタディ

モジュール 16：エンドポイントのレピュテーション

- Global Threat Intelligence のレビュー
- IP レピュテーション
- ポリシー管理の概要
- IP レピュテーション構成の概要
- エンドポイントレピュテーション分析オプション
- 変更の展開

モジュール 17：Web サーバー保護

- Web サーバー保護の概要
- Web サーバーヒューリスティック分析の仕組み
- ポリシー管理の概要
- ヒューリスティック Web アプリケーションサーバー検査構成の概要
- 前提条件：SSL 復号化
- プライベート SSL 証明書
- 前提条件：必要な攻撃
- Web サーバーヒューリスティック分析の構成
- Web サーバーの DoS 防御
- Web サーバーのレイヤ 7DoS 防御
- Web サーバー - DoS 防御の構成の概要
- Web サーバーの構成 – DoS 防御
- センサーリソースへのポリシーの割り当て

モジュール 18：ファイアウォールポリシーの構成

- ファイアウォールポリシーの概要
- ファイアウォールポリシーの管理
- 前提条件：SSL 復号化
- [Firewall Policies] ページの使用

- Policy Manager の使用
- ルールオブジェクトの概要
- ルールオブジェクトの追加
- ステートレスアクセスルール
- ユーザーベスアクセスルール
- アプリケーション識別
- ポリシーのエクスポートとポリシーのインポート
- ファイアウォールアクセスのロギング
- ファイアウォールアクセスイベント
- ファイアウォールポリシー定義構成レポート

モジュール 19：Threat Analyzer

- Threat Analyzer の概要
- Threat Analyzer の起動
- メニューバー
- [Dashboard] ページ
- NSP ヘルスダッシュボード
- 円グラフの詳細の表示
- 保留中の変更の展開
- ISP ダッシュボード
- 円グラフの詳細の表示
- 時系列の攻撃の表示
- 統合された攻撃の表示
- NTBA ダッシュボード
- アプリケーション /GTI ビューダッシュボード
- ダッシュボードとモニターの追加
- [Dashboard] タブのカスタマイズ
- ダッシュボードの追加
- モニターの追加
- [Alerts] ページ
- アラートの詳細の表示
- アラートの管理
- 右クリックオプション
- 無視ルールの例
- [Endpoints] ページ
- [Forensics] ページ
- [Preferences] ページ

モジュール 20：ポリシーの調整

- 調整とは
- 調整を実行する理由
- 調整の前に
- ポリシー調整の 2 つのフェーズ
- 誤検出とノイズ
- 誤検出の識別
- 誤検出を低減するステップ
- 誤検出の防止
- ハイボリューム攻撃での使用
- パターン探し
- 今後の誤検出の防止
- 攻撃とアラートの無効化
- プロセスへの重大度の低い攻撃の追加
- 過剰なアラート
- ハイレベルボトムアップアプローチ
- イベントの分析
- 攻撃名によるソート
- ケーススタディ

モジュール 21：レポートの生成

- レポートの概要
- ロールの割り当て
- レポートの環境設定
- 構成レポートの概要
- 構成レポートの実行
- 次世代レポートの概要
- デフォルトの次世代レポートの実行
- 次世代レポートの追加、複製、編集
- 通常レポートの概要
- 通常レポートの実行
- ユーザー定義レポートの追加
- レポート自動化の構成
- 自動生成レポートの表示

モジュール 22：運用ステータス

- 運用モニターの概要
- デバイスサマリーモニター
- Manager サマリー
- McAfee モニターからのメッセージ
- タスクモニターの実行
- システムヘルスモニター
- 障害の管理
- ダッシュボードでの Manager 障害の表示
- ダッシュボードでのデバイス障害の表示
- [Manager] ページでの障害の表示
- Alert Relevance (アラートの妥当性)
- Alert Relevance の表示
- システムログ
- システムログの表示
- システムログのエクスポート
- タスクの実行
- ユーザーアクティビティログの表示

モジュール 23：データベースの保守

- 保守の概要
- マルウェアファイルのアーカイブ
- データのバックアップ
- データベースバックアップの自動化
- スケジューラ詳細の表示
- バックアップファイルのエクスポート
- バックアップファイルの削除
- データベース調整の概要
- 調整の実施
- 調整の自動化
- アラート削除の有効化と定義
- 最大アラート数の計算
- ファイルとデータベースの削除の構成
- データのアーカイブ
- データのアーカイブの実施
- データのアーカイブの自動化
- アーカイブのエクスポート
- アーカイブの復元

マカフィー株式会社　www.mcafee.com/jp

東 京 本 社　〒 150-0043　東京都渋谷区道玄坂 1-12-1　渋谷マークシティウエスト 20F　TEL：03-5428-1100（代）　FAX：03-5428-1480
西日本支店　〒 530-0003　大阪府大阪市北区堂島 2-2-2　近鉄堂島ビル 18F　TEL：06-6344-1511（代）　FAX：06-6344-1517