コースの詳細

McAfee® VirusScan および ePolicy Orchestrator Administration コース

Intel Security Education Services Administration コーストレーニング

Intel Security の研修サービスが実施している McAfee® VirusScan および ePolicy Orchestrator Administration コースは、McAfee 製品の一元的な管理と導入に役立つ詳しいトレーニングを提供します。受講者は、マカフィーのセキュリティソリューションの機能を十分に理解し、構成ミスのリスクを低減できるだけでなく、インストールしたソリューションの保護機能を最大限に活用することが可能になります。

コースの目標

- 導入計画を立案する
- ePolicy Orchestrator ソフトウェアをインストールして構成する
- ePolicy Orchestrator サーバーをセットアップする
- ユーザーとリソースを管理する
- ネットワークセキュリティ、ポリシー、データベースを管理する
- ネットワークセキュリティステータスを監視し、レポートを作成する
- McAfee Agent をインストールする
- VirusScan Enterprise テクノロジを実装する

トピックの概要

1 日目

- はじめに
- Security Connected と ePO の概要
- McAfee ePO の導入計画
- McAfee ePO のインストール
- 権限セットとユーザーの管理
- システムツリーの作成
- タグカタログの使用

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。

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

- システムツリーのソート
- McAfee エージェント
- システム情報
- クライアントタスク
- ポリシーの管理
- 管理対象システム向けソフトウェアの導入

3 日目

- リポジトリ
- 製品の保守とリポジトリ
- ダッシュボードとモニターの管理
- クエリとレポートの使用
- 自動応答と通知

4 日目

- データベースの保守とサーバーユーティリティ
- 障害時復旧
- VirusScan Enterprise の概要
- VirusScan Enterprise のベストプラクティス – パート 1
- VirusScan Enterprise のベストプラクティス – パート 2

推奨する事前作業

ネットワーク、システム、セキュリティ管理の実務的な知識を習得しておくことを推奨します。事前に McAfee ePO を使用しておくことも推奨します。

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
- リソースの場所の特定
- 演習の環境

モジュール 2：Security Connected と ePolicy Orchestrator の概要

- マカフィーの Security Connected について
- Security Connected の特徴
- Security Connected フレームワーク
- サードパーティ製品との統合
- Security Connected ソリューションプラットフォーム
- ソリューションの概要
- このリリースの新機能
- 基本的なソリューションコンポーネント
- Web インターフェイス
- メニューページ
- ユーザーインターフェイスのカスタマイズ
- アーキテクチャと通信
- ユーザーインターフェイス
- 機能プロセスロジック
- データストレージ

モジュール 3：McAfee ePolicy Orchestrator の導入計画

- 計画の概要
- サーバーハードウェアの評価
- ePO サーバーのハードウェア要件
- ePO サーバーのオペレーティングシステム
- 翻訳言語
- Microsoft の必須ソフトウェア
- SQL Server データベースの要件
- サポートされる Web ブラウザ
- 仮想インフラストラクチャの要件
- ポートの要件

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

コースの詳細

- 導入に関する考慮事項
- 導入シナリオ
- 構成
- ストレージエリアネットワーク (SAN) デバイス
- 拡張性の管理
- 環境要因
- 実装プロセスチェックリスト
- 変更管理

モジュール 4: ePolicy Orchestrator ソフトウェアのインストール

- プラットフォームの要件
- 通信ポート
- 導入ガイドライン
- 変更管理
- データベースのサイジング
- 拡張性の管理
- 環境要因
- インストールの計画
- エクスプレス、カスタム、クラスタインストールワークフロー
- SQL Server のインストール
- ePO ソフトウェアのインストール
- インストール前のタスク
- ePO への最初のログイン
- ルート証明書のインポート
- 自動製品構成ツールの使用
- ガイド付き構成の使用
- ePO でのポート割り当ての表示/編集
- SQL Database の保守
- データベースの消去
- 基本的なトラブルシューティング
- ePO での複数の NIC の構成
- ePO のアップグレード

モジュール 5: 権限セットとユーザーアカウントの管理

- 権限セットの概要
- デフォルト権限セット
- ガイドラインの構成
- 権限セットの複製/追加
- 権限セットの編集/削除
- すべてのエクスポート/インポート
- ユーザーアカウントの概要
- 認証方式のガイドライン
- ユーザーアカウントの作成
- 個人設定の概要
- 個人設定の変更
- デフォルトセッションタイムアウト間隔の編集
- AD でのユーザーの管理
- LDAP Server の登録
- Active Directory ユーザーログインの有効化
- 権限セットのマッピング

モジュール 6: システムツリーの作成と配置

- システムツリーの概要
- システムツリーの計画: 考慮事項
- システムツリーの計画: 境界
- システムツリーの計画: ツリーの構築方法
- システムツリーの計画: エージェントインストール
- 手動でのグループの追加
- システムツリー構造のインポート
- AD および NT ドメインの同期の概要
- NT ドメインの同期の概要
- NT ドメインの同期
- エージェントプッシュ設定の構成
- AD の同期の概要
- LDAP Server の登録

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

コースの詳細

- AD の同期
- 同期の維持
- グループとシステムの移動
- ベストプラクティス

モジュール 7: タグカタログの使用

- タグカタログ
- タグの使用者
- タググループの使用
- 新しいタグビルダーでのタグの追加
- システムからのタグの適用とクリア
- 自動的なタグ付けからのシステムの除外
- タグから除外されたシステムの表示
- 条件ベースのタグの適用
- タグの管理

モジュール 8: システムツリーのソート

- システムツリーのソート
- ePO による配置の決定方法
- 条件ベースのソート
- IP アドレスフィルタリングの仕組み
- IP 整合性のチェック
- ソート順序の変更
- 即座のソートの開始
- テストソートの開始
- システムの移動の開始

モジュール 9: McAfee エージェント

- ソリューションの概要
- McAfee エージェントと SuperAgent
- 管理対象システム
- このリリースの新機能
- インストール/導入の計画
- プラットフォームの要件
- インストールと導入の比較
- アップデートとアップグレードの比較
- 通信
- インストールの概要
- エージェント導入の概要
- エージェントのプッシュ
- エージェントの導入
- エージェントインストールパッケージの使用
- クライアント側ダウンロード URL の作成
- スマートインストーラの使用
- Windows ログインスクリプトの使用
- エージェントイメージの使用 (Windows)
- エージェントの Managed Mode への変換
- McAfee エージェントの削除
- コマンドラインを使用したカスタマイズ
- システムトレイアイコンの使用
- エージェントアクティビティログの表示

モジュール 10: システム情報

- [Systems] タブの概要
- [Systems] タブのカスタマイズ
- 列の選択
- データのフィルタリング
- システム情報の表示
- システム情報モニターの使用
- サマリーモニターのカスタマイズ
- プロパティモニターのカスタマイズ
- チャートモニターのカスタマイズ
- システム情報テーブルの使用
- [System Properties] タブの概要

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

コースの詳細

モジュール 11：クライアントタスク

- クライアントタスクの概要
- クライアントタスクの使用
- クライアントタスクの作成
- クライアントタスクの編集
- クライアントタスクの削除
- クライアントタスクの複製
- クライアントタスクの割り当て
- タスクの継承
- 継承ブロックのためのタスクの編集
- その他のクライアントタスク
- VirsScan On-Demand Scan タスク
- McAfee Agent 統計クライアントタスク
- McAfee Agent のウェークアップ（Windows のみ）
- McAfee Agent：リポジトリのミラーリング（Windows）
- 製品の配備

モジュール 12：ポリシーの管理

- ポリシーの概要
- ポリシーカタログ
- ポリシーの複製、作成、編集
- ポリシー所有者の変更
- ポリシーのエクスポートとインポート
- ポリシーの名前変更/削除
- 割り当てと施行のロック
- ポリシーの割り当てと施行
- 中断した継承の表示とリセット
- ポリシーの比較

モジュール 13：管理対象システム向けソフトウェアの導入

- ソフトウェアコンポーネントの取得
- Software Manager
- Software Manager の使用
- 拡張機能の手動でのインストール
- パッケージの手動でのチェックイン
- チェックポイント：ePO サマリーダッシュボード
- 製品配備の概要
- 製品配備プロジェクト
- 製品配備プロジェクトの作成
- 配備プロジェクトの管理
- 製品配備の詳細の表示
- クライアントタスクカタログ
- 製品アップデートの考慮点

モジュール 14：リポジトリ

- マスターリポジトリ
- ソースリポジトリ
- フォールバックサイト
- 分散リポジトリ
- デフォルトリポジトリ
- リポジトリプラットフォームとロール
- リポジトリブランチ
- ソースサイトの追加
- ソースサイトへのアクセスの確保
- フォールバックサイトの有効化/無効化
- サイトの編集/削除
- 分散リポジトリの追加
- フォルダ共有の有効化
- SuperAgent 分散リポジトリの作成
- SuperAgent の LazyCaching 機能
- SuperAgent の階層の作成
- エージェントリレー機能
- McAfee Agent 統計情報の収集
- 管理対象外/ローカルリポジトリの追加
- 権限セット
- エクスポートとインポート

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

コースの詳細

モジュール 15: 製品の保守とリポジトリ

- グローバルアップデートの概要
- グローバルアップデートの要件
- SuperAgent リポジトリとグローバルアップデート
- グローバルアップデートの有効化
- CommonUpdater
- オートアップデートプロセス
- 増分アップデート
- アップデート進捗ダイアログ
- サーバータスクログ
- ログエントリのドリルダウン
- サーバータスクの権限セット
- リポジトリのアップデート
- リポジトリプルタスクの作成
- リポジトリ複製タスクの作成
- プル/複製タスクのガイドライン
- タスク失敗のトラブルシューティング

モジュール 16: ダッシュボードとモニターの管理

- デフォルトダッシュボード
- ダッシュボードアクション
- ダッシュボード権限の割り当て
- ダッシュボードガイドライン
- モニターガイドライン
- モニターの追加、編集、削除
- ダッシュボードサーバーの構成
- デフォルトダッシュボードの指定
- デフォルトダッシュボードリフレッシュ間隔の編集
- ダッシュボードの設計
- Performance Optimizer
- 評価のタイプ
- サーバー評価タスク

モジュール 17: クエリとレポートの使用

- クエリとレポートの概要
- クエリの使用
- 基本クエリページの管理
- ダッシュボードモニターとしてのクエリの使用
- 公開クエリと個人用クエリ
- クエリビルダーの使用
- デフォルトクエリとアクション可能なクエリ
- 事前定義クエリの使用
- クエリグループと権限
- マルチサーバーデータロールアップの概要
- 自動クエリアクション
- 他の形式へのクエリ結果のエクスポート
- 個人用クエリの公開
- クエリの複製と共有
- クエリのインポート
- レポートの使用
- 印刷とエクスポートの設定
- レポートの作成と編集
- レポートへのエレメントの追加
- レポートエレメントの構成
- レポートのヘッダー/フッターのカスタマイズ
- レポート出力の表示
- 他のグループへのレポートの移動
- レポートの実行
- イベントのフィルタ

intel Security

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

コースの詳細

モジュール 18: 自動応答と通知

- 自動応答機能の仕組み
- デフォルトルールの有効化
- 自動応答ビルダー
- 独立ルールの構成
- コンポーネントと権限の準備
- 権限の割り当て
- 電子メール連絡先リストの指定
- 電子メールサーバーの構成
- 転送するイベントの決定
- イベント間隔の構成
- SNMP サーバーの指定
- .MIB ファイルのインポート
- 登録済み実行ファイルの指定

モジュール 19: データベースの保守とサーバーユーティリティ

- 保守の概要
- サーバータスクを使用した保守の自動化
- サーバータスクの権限セットの編集
- スケジュールでの cron 構文の使用
- 消去の概要
- 手動/自動でのデータの消去
- クエリを使用したレコードの消去
- イベントフィルタリング設定の編集
- バックアップの概要
- 手動でのバックアップの開始
- 復元の概要
- 復元の開始
- トランザクションログの概要
- トランザクションログの縮小
- Transact-SQL の使用
- サーバー設定の管理

モジュール 20: 障害時復旧

- 障害時復旧の概要
- 障害時復旧の仕組み
- スナップショットサーバータスクの使用
- ダッシュボードからのスナップショットの作成
- サーバースナップショットのステータスの特定
- 障害時復旧計画の決定
- シナリオ: 単純な障害時復旧計画
- シナリオ: サーバークラスタ
- シナリオ: コールド/ホットスペア - 単一物理サイトシナリオ: コールド/ホットスペア - 2 つの物理サイト
- 復元インストールのワークフロー
- 復元インストールの実行
- 障害時復旧のベストプラクティス

モジュール 21: VirusScan Enterprise の概要

- ソリューションの概要
- 利点と機能
- 基本コンポーネント
- DAT (シグネチャ)
- スキャンエンジン
- DAT とスキャンエンジンのアップデート
- Artemis と McAfee Labs
- オプションのコンポーネント
- VSE 導入計画
- サポートされるオペレーティングシステム
- サポートされる言語選択肢
- 特別なインストールケースのガイドライン
- インストールの概要
- 事前構成、導入、アップデート
- McAfee Installation Designer の使用
- VirusScan Console の使用
- VirusScan のテスト
- VSE 削除オプション

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

コースの詳細

モジュール 22: VirusScan のベストプラクティス – パート 1

- アクセス保護の概要
- アクセス保護の構成
- バッファオーバーフローからの保護の概要
- バッファオーバーフローからの保護の構成
- 不要なプログラムの概要
- PUP の構成
- オンアクセススキャンの概要
- オンアクセススキャンの構成
- On-Delivery Email Scanner の概要
- On-Delivery Email Scan ポリシーの構成
- Quarantine Manager
- Quarantine Manager ポリシーの構成
- オンデマンドスキャンの概要
- オンデマンドスキャンタスクの構成
- VirusScan Mirror タスク
- サーバータスク
- 保護の監視と分析
- 保護の微調整

モジュール 23: VirusScan のベストプラクティス – パート 2

- 有効なプロセスの無効化
- Trusted Installer のスキャンの構成
- 除外の概要
- 除外アイテムの追加/編集
- ワイルドカード除外記号の使用
- ハードウェアパスでの除外の管理
- Windows ファイル保護
- McAfee Agent の除外
- 低/高リスクプロセスポリシーの定義
- スキャニングポリシー数の決定
- 低リスクとして追加できるプロセス
- システム活用の構成
- 1051 および 1059 イベントのフィルタリング

61707brf_ngfw-sales-expert-courses_0215

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