コースの詳細

McAfee® Data Loss Prevention Endpoint

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® Data Loss Prevention Endpoint Administration コースは、知的財産の保護とコンプライアンス対応を可能にする McAfee Data Loss Prevention Endpoint の設計、実装、構成、操作に必要なツールに関する詳細なトレーニングを提供します。このコースでは、McAfee Data Loss Prevention Endpoint が、一元管理機能を提供する McAfee® ePolicy Orchestrator をどのように活用するかを詳しく理解できます。また、電子メール送受信、Web への投稿、印刷、クリップボードの使用、スクリーンキャプチャ、デバイス制御、クラウドへのアップロードをはじめとする、エンドユーザーのリスクを伴う行動を日常的に監視し、対処する方法も説明します。

コースの目標

- 導入計画を立案する
- McAfee ePolicy Orchestrator サーバーに McAfee Data Loss Prevention Endpoint ソフトウェアをインストールして構成する
- McAfee Data Loss Prevention Endpoint クライアントをエンドポイントにインストールする
- 分類、タグ付け、保護ルールを使用して機密情報を保護する
- エンドポイント検出ルールを使用して情報の場所を特定する
- インシデントとイベントを監視し、クエリとレポートを生成する

トピックの概要

1 日目

- はじめに
- ソリューションの概要
- 導入計画
- McAfee ePO のレビュー
- 企業環境の準備
- McAfee DLPe ソフトウェアのインストール
- 権限セット

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

- McAfee DLPe クライアントソフトウェアの導入
- DLP ポリシーの概要とクライアントの構成
- DLP Policy Manager の概要と初期構成
- DLP 特権ユーザーとエンドユーザーグループ
- デバイス制御

3 日目

- コンテンツ保護の概要
- 分類とタグ付け
- リムーバブルストレージの保護
- 電子メールの保護
- Web の保護
- 印刷の保護
- スクリーンキャプチャの防止
- クリップボードの保護
- クラウドの保護
- アプリケーションファイルアクセス保護用の McAfee デバイスルールセットとルール

4 日目

- エンドポイント検出
- 監視とレポート
- 基本的なトラブルシューティング

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

- はじめに
- このコースについて
- このコースで使用する略語と用語
- 役立つリソースの把握
- Intel Security Expert Center
- 演習の環境

モジュール 2：McAfee Data Loss Prevention Endpoint ソリューションの概要

- データ損失の発生源
- データ損失の原因
- McAfee Data Loss Prevention（DLP）ポートフォリオ
- Data Loss Prevention ソリューションの選択
- McAfee DLP Endpoint の概要
- DLPE 9.4X の新機能と機能強化
- McAfee DLPe の仕組み
  - 分類
  - 追跡
  - 保護
  - 監視

モジュール 3：McAfee ePolicy Data Loss Prevention Endpoint の導入計画

- 計画の概要
- 戦略と目標：内部評価
- 戦略と目標：ロール
- 評価
- 戦略と目標：技術評価
- 戦略と目標：リスク評価
- 戦略と目標：プライバシー法
- 分類：機密性
- 分類：手法
- 分類のシナリオ：組織レベル

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 3：McAfee ePolicy Data Loss Prevention Endpoint の導入計画（続き）

- 分類のシナリオ：アプリケーション
- 分類のシナリオ：エンドユーザーおよび顧客
- 分類：検出、適用、施行
- 導入計画
- ソリューションの要件：ePO プラットフォーム
- ソリューションの要件：データベース
- ソリューションの要件：クライアント
- サポートされるサードパーティソフトウェア
- パイロットの計画
- パイロット後の検証と企業環境へのロールアウト
- その他の計画の考慮事項
- リソース：導入計画の質問票
  - ePO サーバーとインフラストラクチャの資格情報
  - 製品固有の質問
  - ネットワーク要件
  - McAfee ePO と McAfee Agent
  - Microsoft SQL Server の要件
  - クライアント要件

モジュール 4：企業環境の準備

- Active Directory セキュリティグループの追加
- Active Directory セキュリティグループへのユーザーの追加
- Active Directory グループメンバーシップの確認
- リソースフォルダーの準備
- リソースフォルダーの共有の構成
- リソースフォルダーのアクセス許可の構成
- 共有設定の確認
- カスタムのアクセス権限エントリの構成
- フォルダーのアクセス権限の変更
- 親からの継承可能なアクセス権限の削除
- チェックポイント
- アクセス権限エントリの追加
- 新しいアクセス権限エントリの確認

モジュール 5：McAfee ePolicy Orchestrator のレビュー

- McAfee ePO ソリューションの概要
- McAfee ePO プラットフォームの要件
- デフォルトポート
- 通信：Tomcat サービス
- McAfee ePO Web インターフェイスへのログイン
- McAfee ePO Web インターフェイスのクイックツアー
- レポートオプション
- システムオプション
- ポリシーオプション
- ソフトウェアオプション
- 自動処理オプション
- ユーザー管理オプション

モジュール 6：McAfee Data Loss Prevention Endpoint ソフトウェアのインストール

- McAfee DLPe ソフトウェアの入手
- McAfee DLPe ソフトウェアの概要
- McAfee DLPe パッケージのチェックイン
- McAfee DLPe 拡張ファイルのインストール
- McAfee DLPe ライセンスのインストール
- McAfee DLPe インストールの確認

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 7：権限セット

- DLP サーバー設定の表示と編集
- 権限セットの概要
- 新しい DLP 権限セットの追加
- デフォルトの DLP 権限：ポリシーカタログ
- デフォルトの DLP 権限：DLP Policy Manager
- デフォルトの DLP 権限：分類
- デフォルトの DLP 権限：定義
- デフォルトの DLP 権限：操作イベント
- デフォルトの DLP 権限：ケース管理
- ヘルプデスクの権限
- 事例：DLPe グループの管理
- 事例：インシデントレビューアー
- 事例：編集レビューア -
- ヘルプデスク権限セットの作成
- 管理者専用の権限
- ユーザー管理のレビュー
- 認証方式のガイドライン
- DLPe ユーザーの作成

モジュール 8：McAfee Data Loss Prevention Endpoint クライアントの導入

- McAfee DLPe クライアントの概要
- McAfee ePO コンソールからのクライアントソフトウェアの導入
- クライアントソフトウェア導入方法の比較
- 製品導入プロジェクトの作成
- クライアント導入タスクの作成
- DLP Endpoint コンソール

モジュール 9：McAfee DLP ポリシーの概要と初期構成

- レビュー：
  - DLP ポリシー
  - ルールとルールセット
  - 定義
  - ポリシーアーキテクチャ
  - 分類とタグ付け
- ポリシーの概要
- McAfee DLP クライアント構成ポリシー操作モード
  - デバイス制御と完全なコンテンツ保護と、デバイス制御のみの比較
- データ保護モジュール
- 保護設定：ホワイトリスト
- コンテンツ追跡
- 会社の接続性
- デバッグとロギング
- エビデンスコピーサービス
- 隔離
- リムーバブルストレージの保護
- スクリーンキャプチャの防止
- Web 投稿の保護
- ユーザーインターフェースコンポーネント
- McAfee DLP ポリシー
- 有効なルールセットの割り当て
- エンドポイント検出スキャンの設定
- グローバル設定の定義

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 10: McAfee DLP Policy Manager の概要

- McAfee DLP Policy Manager のレビュー
- [Rule Sets] タブ
- ルールのタイプ
- [Policy Assignment] タブ
- [Definitions] タブ
- サポートされる定義
- データ定義の例
- デバイス制御定義の例
- 定義の例: 通知
- 定義の例: その他
- 定義の例: ソース/宛先
- その他の機能

モジュール 11: 特権ユーザーとエンドユーザーグループの定義

- 概要: 特権ユーザー、エンドユーザーグループ定義、Active Directory
- LDAP サーバーの登録
- Active Directory に関する考慮事項
- 特権ユーザーの作成
- 特権ユーザーの例
- エンドユーザーグループ定義の指定
- エンドユーザーグループ定義の例
- 複数のユーザーセッション

モジュール 12: デバイス制御

- デバイス制御の概要
- デバイス管理の概要
- デバイス管理の概要: デバイスクラス
- デバイス管理の概要: デバイス定義
- デバイス管理の概要: PnP デバイス
- デバイス管理の概要: リムーバブルストレージ
- デバイス管理の概要: 固定ハードドライブ
- デバイスクラスの使用
- 組み込みのデバイスクラス (読み取り専用)
- 新しいデバイスクラスの追加
- デバイス GUI の特定
- デバイス定義の使用
- 組み込みのデバイス定義 (読み取り専用)
- 新しいデバイス定義の追加
- 命名規則の例: デバイス定義
- 例: ファイルシステム定義
- 例: プラグアンドプレイデバイス定義
- 例: リムーバブルストレージデバイス定義
- 例: ホワイトリスト登録のプラグアンドプレイデバイス
- DLP ポリシーのデバイスクラス設定の上書き
- インシデントの表示

モジュール 13: McAfee デバイスのルールセットとルール

- デバイスのルールセットとルールの概要
- デバイスの組み込みのルールセットとルール
- デバイスルールの使用
- [Device Control] の [ルール] タブ
- デバイスルールの追加
- 命名規則の例: デバイス定義
- 命名規則: デバイスルール
- Citrix デバイスルールの概要
- Citrix デバイスルールの構成
- 固定ハードドライブデバイスルールの概要
- 固定ハードドライブデバイスルールの構成
- プラグアンドプレイデバイスルールの概要

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 13: McAfee デバイスのルールセットとルール (続き)

- プラグアンドプレイデバイスルールの構成
- リムーバブルストレージファイルアクセスデバイスルールの例
- リムーバブルストレージファイルアクセスデバイスルールの構成
- リムーバブルストレージファイルアクセスデバイスルールの構成
- TrueCrypt デバイスルールの概要
- TrueCrypt デバイスルールの構成
- ケーススタディ

モジュール 14: コンテンツ保護の概要

- データ保護の概要
- 保護戦略の定義
- ビジネス要件
- ルールの構造
  - 分類条件が十分かどうか
  - タグ付け条件が必要かどうか
  - どのようなルールパラメータがあるのか
  - どのような効果/結果が期待されるのか
- レビュー: 定義
- 命名規則の例
- データ - ファイル拡張子の定義
- 通知 – ジャスティフィケーションの定義
- 通知 – ユーザー通知の定義
- 通知のプレースホルダーの構成
- アプリケーションテンプレートの定義
- メールアドレスの定義
- ローカルフォルダーの定義
- ネットワークアドレス (IP アドレス) の定義
- ネットワークポートの定義
- ネットワークプリンタの定義
- ネットワーク共有の定義
- プロセス名の定義
- URL リストの定義
- ウィンドウタイトルの定義
- すべてを統合
  - 保護ルールの作成
  - 命名規則: データ保護ルール

モジュール 15: コンテンツの分類とタグ付け

- 分類のレビュー
- タグの伝播
- タグ付けルール
- タグ付けの詳細
- 分類条件の作成
- 分類と条件の例
- タグ付け条件の作成
- 手動分類
- 文書の登録
- ホワイトリスト登録テキスト

モジュール 16: リムーバブルストレージ保護

- リムーバブルストレージ保護の概要
- リムーバブルストレージ保護詳細オプション
- TrueCrypt ローカルディスクのマウントの保護
- ポータブルデバイスハンドラー (メディア転送プロトコル)
- 高度なファイルコピー保護
- 削除モード
- リムーバブルストレージ保護の使用事例
- 構成例
- ユーザー通知

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 17: 電子メール保護
- 電子メール保護の概要
- クライアント設定のガイドライン
- サードパーティ電子メール分類
- 使用事例
- 構成例

モジュール 18: Web 保護
- Web 保護の概要
- ブラウザ
- クライアント設定のガイドライン
- 使用事例
- 構成例

モジュール 19: プリンタ保護
- プリンタ保護の概要
- クライアント設定のガイドライン
- 使用事例
- 構成例

モジュール 20: スクリーンキャプチャ防止
- スクリーンキャプチャ防止の概要
- 保護されるアプリケーション
- 使用事例
- 構成例

モジュール 21: クリップボード保護
- クリップボード保護の概要
- 使用事例
- 構成例

モジュール 22: クラウド保護
- クラウド保護の概要
- 使用事例
- 構成例

モジュール 23: アプリケーションファイルアクセス保護
- アプリケーションファイルアクセス保護の概要
- 使用事例
- 構成例

モジュール 24: エンドポイント検出
- エンドポイント検出の概要
- 検出クローラーの実行
- 検出設定の確認
- 検出のルールセットとルール
- デモ
- 検出ルールの作成
- スケジューラー定義
- スケジューラー定義の作成
- スケジューラー定義の例
- スケジューラー定義のフィールド
- 命名規則: エンドポイント検出ルール
- 検出スキャンのセットアップ
- エンドポイントスキャンの構成例
- 隔離されたファイルまたは電子メール項目

モジュール 25: 監視とレポート
- DLP インシデントマネージャー
- DLP インシデントマネージャー: [インシデントリスト]
- DLP インシデントマネージャー: [インシデントタスク]
- DLP インシデントマネージャー: [インシデント履歴]
- DLP 操作イベント
- レビューアー設定ルールの作成
- 自動メール通知ルールの作成
- DLP ケース管理
- ケースの作成
- レビューアー設定タスクの作成
- DLP サーバータスク
- サーバータスクの使用
- クエリの概要
- Data Loss Prevention のクエリ
- クエリの作成
- Data Loss Prevention のレポート

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 25: 監視とレポート (続き)

- レポートの作成
- レポートの使用
- DLP ダッシュボード
- DLP ダッシュボード
- ダッシュボードとモニターの使用

モジュール 26: 基本的なトラブルシューティング

- 診断ツールの概要
- クライアントバイパスキーの生成
- 診断ツールのレイアウトとデザイン
- [General Information] タブ
- [DLPE Modules] タブ
- [Data Flow] タブ
- [Tools] タブ
- [Process List] タブ
- [Devices] タブ
- [Active Policy] タブ
- ポリシーの調整: CPU 使用率が高い
- ポリシーの調整: タグ付け
- デバッグロギング

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