Offre éditeurs

Trellix Data Loss Prevention Endpoint - Administration

4 jours (28h00) | ★★★★½ 4,6/5 | MCA-DLP | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 23/05/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Mettre en pratique les outils nécessaires à la conception, la mise en oeuvre, la configuration et l'utilisation de Data Loss Prevention Endpoint pour protéger la propriété intellectuelle et assurer la conformité
- Expliquer comment cette solution utilise le logiciel ePolicy Orchestrator (ePO) pour une gestion centralisée
- Surveiller et traiter les actions quotidiennes à risque des utilisateurs finaux, telles que l'envoi de courriels, la publication d'articles sur le Web, l'impression, les presse-papiers, les captures d'écran, le contrôle des appareils, le téléchargement vers le Cloud, et plus encore.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

** nous consulter pour la faisabilité en distanciel*

*** ratio variable selon le cours suivi*

Prérequis

Avoir de solides connaissances de Windows, de l'administration système, des technologies de réseau, de la sécurité informatique, des concepts de sécurité du Cloud et des technologies Web. Il est également recommandé d'avoir une expérience préalable de l'utilisation du logiciel McAfee MVISION ePO.

Public concerné

Administrateurs système et réseau, membres d'une équipe de sécurité, auditeurs et/ou consultants concernés par la sécurité des points de terminaison (endpoints) des systèmes.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Introduction

- Se familiariser avec les ressources d'information et de support ainsi que les mécanismes de feedback

Présentation de la solution Data Loss Prevention

- Décrire la solution, ses caractéristiques et ses fonctionnalités

Principes fondamentaux de Data Loss Prevention Endpoint

- Décrire la solution Data Loss Prevention Endpoint, ses principales caractéristiques, l'architecture de déploiement, ainsi que les nouvelles fonctionnalités et améliorations de cette version

Planification du déploiement

- Décrire les exigences commerciales, logicielles, matérielles et de composants à prendre en compte lors de la planification du déploiement

Pré-installation de la configuration du système

- Identifier le workflow de conception des politiques dans Data Loss Prevention sur MVISION ePO
- Identifier les conditions préalables à l'installation
- Décrire les tâches de pré-installation

Installation

- Identifier le processus d'installation pour installer ou mettre à niveau Data Loss Prevention Endpoint à l'aide de MVISION ePO

- Décrire comment configurer le stockage dans le Cloud pour les preuves et les empreintes digitales

Déploiement des points de terminaison clients

- Décrire le processus de déploiement du logiciel sur les points de terminaison
- Vérifier la réussite du déploiement

Jour 2

Configuration du client

- Décrire comment configurer la politique de configuration du client Data Loss Prevention
- S'assurer que les politiques sont affectées aux groupes ou aux systèmes

Service d'assistance DLP et ensembles d'autorisations

- Décrire l'objectif du service d'assistance DLP et ses principales fonctionnalités
- Configurer la fonction d'assistance
- Utiliser la fonction d'assistance pour générer des clés

Présentation du Data Loss Prevention Policy Manager

- Accéder au Data Loss Prevention Policy Manager
- Naviguer dans les onglets de Data Loss Prevention Policy Manager pour se familiariser avec sa conception et son utilisation

Définitions des utilisateurs privilégiés et des groupes d'utilisateurs finaux

- Enregistrer le serveur Active Directory
- Créer un utilisateur privilégié
- Créer des définitions de groupe d'utilisateurs finaux

Contrôle des périphériques

- Décrire la fonction Device Control
- Configurer Device Control pour répondre aux besoins du client

Jour 3

Ensembles de règles et règles pour les dispositifs

- Identifier les ensembles de règles intégrés et les règles disponibles
- Décrire les éléments d'une règle de dispositif
- Créer des règles de dispositif pour répondre aux besoins du client

Exemple de travaux pratiques (à titre indicatif)

- *Etude de cas* :
  - *Décrire comment des règles ou des classifications spécifiques peuvent répondre aux besoins d'une entreprise ou d'un secteur d'activité*

Classification du contenu sensible

- Expliquer les définitions et les critères de classification ainsi que les fonctionnalités du module Classification

Règles relatives aux empreintes de contenu et aux critères de classification

- Créer des :
  - Critères d'empreintes de contenu
  - Règles de classification du contenu
- Décrire comment fonctionne l'empreinte persistante

Définitions de la protection des données

- Identifier les définitions de protection des données et les règles de protection des données qui leur sont associées
- Créer des définitions utilisées pour les règles de protection des données
- Configurer des notifications et justifications de l'utilisateur final

Jour 4

Configuration des règles de protection des données

- Identifier les éléments constitutifs de la protection des données ainsi que les règles
- Construire des règles de protection des données pour répondre aux besoins des clients
- Fournir des exemples de cas d'utilisation des règles de protection des données

Découverte des points de terminaison

- Identifier les ensembles de règles de découverte des points de terminaison intégrés et les règles disponibles pour une utilisation immédiate
- Identifier les parties d'une règle de découverte
- Créer des règles de découverte pour répondre aux besoins des clients

Gestion des incidents

- Identifier et utiliser les fonctions de surveillance et de reporting de Data Loss Prevention Endpoint, y compris Data Loss Prevention Incident Manager

Gestion des cas

- Décrire les fonctionnalités de Data Loss Prevention Case Management
- Créer des nouveaux cas pour regrouper des incidents connexes
- Administrer les cas à l'aide de McAfee Data Loss Prevention Case Management

Protection des fichiers avec la gestion des droits

- Expliquer le fonctionnement de la gestion des droits dans l'environnement Data Loss Prevention
- Configurer et utiliser les produits Right Management pris en charge

Espace de travail de protection

- Décrire les fonctionnalités de l'espace de travail de protection dans ePolicy Orchestrator

Protection des fichiers et des médias amovibles

- Décrire la solution File and Removable Media Protection

Dépannage de base

- Décrire l'utilisation de l'outil de diagnostic et comment utiliser la journalisation de débogage

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques

Les + de la formation

Le support de cours et les labs sont en anglais.

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.