Offre éditeurs

Trellix Application and Change Control - Administration 8.0

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

Contenu mis à jour le 13/10/2023. Document téléchargé le 27/07/2024.

Objectifs de formation

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

- Installer, configurer, utiliser et résoudre efficacement les problèmes liés à Trellix Application Control et Change Control pour protéger la propriété intellectuelle et garantir la conformité
- Utiliser Trellix ePolicy Orchestrator (Trellix ePO)
- Mettre en place seulement les applications de confiance s'exécutant avec Application Control
- Surveiller et prévenir les changements apportés au système de fichiers, au registre et aux comptes d'utilisateurs avec Change Control.

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 une solide connaissance de l'administration du système Microsoft Windows et des technologies réseau, de la sécurité informatique, de la syntaxe en ligne de commande, des logiciels malware / anti-malware, des virus / antivirus et des technologies Web. Avoir une expérience dans l'utilisation du logiciel Trellix ePolicy Orchestrator (Trellix ePO).

Public concerné

Administrateurs système et réseau ou toute personne concernée par la sécurité des terminaux système.

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

Vue d'ensemble de Trellix ePolicy Orchestrator (ePO)

Vue d'ensemble de Trellix Application Control et Change Control

- Décrire les composants, les fonctions et les fonctionnalités de Trellix Application Control et Change Control

Planification d'un déploiement géré

- Décrire les conditions préalables et les éléments-clés d'un plan de déploiement
- Identifier les contreparties de la solution et les phases du plan pilote

Installer l'extension Trellix Application Control et Change Control

- Comment ajouter l'extension Trellix Application Control et Change Control au serveur Trellix ePO ?
- Vérifier l'installation

Tâches du serveur et ensembles d'autorisations de Application Control et de Change Control

- Identifier les ensembles de permissions par défaut inclus avec le logiciel ePO, Application Control et Change Control
- Comprendre les tâches serveur spécifiques au produit créées après le déploiement

Application Control client

- Décrire comment activer et désactiver les tâches client Application Control
- Décrire les notifications, les évènements et les approbations des utilisateurs finaux
- Personnaliser les notifications des utilisateurs finaux

Jour 2

Les ensembles de règles et les autres principes

- Les ensembles de règles, leurs propriétés et leurs permissions
- Configurer et gérer les ensembles de règles
- Les onglets des ensembles de règles de Application Control, Change Control et Integrity Monitoring

Stratégies de Application Control

- Les stratégies de Application Control et leurs relations avec les ensembles de règles
- Définir le rôle de la politique et configurer les stratégies

Modèle de confiance de Application Control

- Les bases de l'inscription à une liste blanche (whitelisting)
- Concevoir le modèle de confiance Application Control

Modifier les fichiers protégés

- Comment utiliser le mode Update et le mode Observer ?
- Comment apporter des modifications aux règles ?

Jour 3

Inventaire de Application Control

- Naviguer dans les menus de l'inventaire, décrire comment faire des recherches
- Gérer un inventaire et expliquer comment comparer un inventaire

Change Control

- Utilisation de la protection d'écriture et de lecture dans les stratégies
- Définir les mises à jour et les utilisateurs autorisés
- Configurer Change Control

Integrity Monitoring

- Configurer les stratégies d'Integrity Monitoring
- Réduire le "bruit" à l'aide du filtre d'exclusion avancé
- Comment utiliser le suivi des changements de contenu ?

Evènements et alertes

- Comment les évènements Application Control sont traités dans le logiciel ePO ?
- Quand utiliser l'exclusion en un seul clic ?
- Configurer les alertes Application Control dans le logiciel ePO

Tableaux de bord et rapports

- Les tableaux de bord et les requêtes de Application Control
- Visualiser les rapports

Jour 4

Dépannage

- Identifier le client par rapport à l'utilisation du logiciel ePO géré
- Localiser le fichier log et les ressources-clés
- Utiliser des outils de dépannage
- Dépannage des problèmes d'implémentation des fonctionnalités

Administration à l'aide de l'interface en ligne de commande

- Utiliser l'interface en ligne de commande pour administrer des systèmes non connectés au serveur ePO

Pratiques recommandées

- Identifier les bonnes pratiques pour l'installation initiale, les tests, la création et la mise au point de stratégies, ainsi que la maintenance

Exemples de travaux pratiques (à titre indicatif)

- *Créez vos propres stratégies Application Control et Change Control sans aucune aide*
- *Créer une notification pour les violations de ces stratégies*

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.