Security

Protecting Against Malware Threats with Cisco AMP for Endpoints

SSFAMP

Version : 6.0
3 Jours

Objectifs

A l'issue de ce cours, le stagiaire sera en mesure d'atteindre ses objectifs :

- Identifier les composants clés et les méthodologies de Cisco Advanced Malware Protection (AMP)
- Reconnaître les caractéristiques et les concepts clés du produit AMP for Endpoints
- Naviguer dans l'interface de la console AMP for Endpoints et effectuer les tâches de configuration de la première utilisation
- Identifier et utiliser les principales fonctions d'analyse du produit AMP for Endpoints
- Utiliser les outils de AMP for Endpoints pour analyser un hôte compromis
- Analyser les fichiers et les événements à l'aide de la console AMP for Endpoints et être capable de produire des rapports sur les menaces
- Configurer et personnaliser AMP for Endpoints pour détecter les logiciels malveillants
- Créer et configurer une politique pour les terminaux protégés par AMP
- Planifier, déployer et dépanner une installation AMP for Endpoints
- Utiliser Cisco Orbital pour extraire des données de requête des connecteurs AMP pour points finaux installés.
- Décrire l'API AMP Representational State Transfer (REST) et les principes fondamentaux de son utilisation.
- Décrire toutes les fonctionnalités du menu Comptes pour les installations de clouds publics et privés.

Public Concerné

- Intégrateurs, revendeurs et partenaires de Cisco
- Administrateurs de réseau
- Administrateurs de sécurité
- Consultants en sécurité
- Ingénieurs systèmes
- Personnel de support technique

Pré-requis

Pour bénéficier pleinement de ce cours, vous devez posséder les connaissances et les compétences suivantes :

- Compréhension technique des réseaux TCP/IP et de l'architecture des réseaux
- Compréhension technique des concepts et protocoles de sécurité

La formation Cisco suivante peut vous aider à remplir ces conditions préalables :

- Implémentation et administration des solutions Cisco (CCNA)

Pour plus d'informations : info@learneo.fr ou 01 53 20 37 00

Plan du cours détaillé

Théorie

- Présentation des technologies AMP de Cisco
- Présentation de AMP for Endpoints Vue d'ensemble et architecture
- Naviguer dans l'interface de la console
- Utilisation de Cisco AMP pour les points finaux
- Identifier les attaques
- Analyse des logiciels malveillants
- Gérer le contrôle des épidémies
- Créer des politiques pour les points finaux
- Travailler avec AMP pour les groupes de points finaux
- Utiliser Orbital pour la visibilité des points d'accès
- Présentation de l'API AMP REST
- Navigation dans les comptes

Plan du laboratoire

- Auto-enregistrement du compte AMP
- Accès à AMP pour les terminaux
- Scénario d'attaque
- Outils d'analyse et rapports
- Contrôle des épidémies
- Politiques pour les points d'extrémité
- Groupes et déploiement
- Test de votre configuration
- Visibilité des points de terminaison à l'aide d'Orbital
- REST D'ORBITAL
- Isolation des points de terminaison à l'aide de l'API Cisco AMP
- Comptes d'utilisateurs

Mode d'évaluation des acquis

Evaluation par le formateur oralement chaque jour et auto-évaluation formalisée sur le Moodle. Nous utilisons également un test de positionnement au début et à la fin de la formation pour évaluer de manière exhaustive les connaissances de nos stagiaires. Ce processus nous permet de mesurer la progression individuelle et d'adapter notre approche pédagogique pour garantir une expérience d'apprentissage optimale.