Formation Protecting Against Malware Threats with Cisco AMP for Endpoints

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Le cours Protection contre les menaces de logiciels malveillants avec Cisco AMP for Endpoints (SSFAMP) vous montre comment déployer et utiliser Cisco® AMP for Endpoints, une solution de sécurité des terminaux de nouvelle génération qui prévient, détecte et répond aux menaces avancées. Grâce à des instructions d'experts et à des exercices pratiques en laboratoire, vous apprendrez à mettre en oeuvre et à utiliser cette solution puissante à travers plusieurs scénarios d'attaque étape par étape. Vous apprendrez à créer et à gérer un déploiement de Cisco AMP for Endpoints, à créer des politiques pour les groupes de points de terminaison et à déployer des connecteurs. Vous analyserez également les détections de logiciels malveillants à l'aide des outils disponibles dans la console AMP for Endpoints.

Référence	SSFAMP
Durée	3 jours (21h)
Tarif	2 390 €HT
Repas	60 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (ENG)

du 28 au 30 mai 2024
du 19 au 21 août 2024
du 11 au 13 novembre 2024
du 19 au 21 février 2025

VOIR TOUTES LES DATES

Objectifs

| Identifier les composants et méthodologies clés de Cisco Advanced Malware Protection (AMP)
| Reconnaître les principales fonctionnalités et concepts du produit AMP for Endpoints
| Naviguer dans l'interface de la console AMP for Endpoints et effectuez les tâches de configuration de première utilisation
| Identifier et utiliser les principales fonctionnalités d'analyse d'AMP for Endpoints
| Utiliser les outils AMP for Endpoints pour analyser un hôte compromis
| Analyser les fichiers et les événements à l'aide de la console AMP for Endpoints et soyez en mesure de produire des rapports sur les menaces
| Configurez et personnalisez AMP for Endpoints pour effectuer la détection des logiciels malveillants
| Créer et configurer une stratégie pour les points de terminaison protégés par AMP
| Planifier, déployer et dépanner une installation AMP for Endpoints
| Utiliser Cisco Orbital pour extraire les données de requête des connecteurs AMP for Endpoints installés.
| Décrire l'API REST (Representational State Transfer) AMP et les principes fondamentaux de son utilisation
| Décrire toutes les fonctionnalités du menu Comptes pour les installations de cloud public et privé

Public

| Toute personne impliquée dans le déploiement et l'utilisation de Cisco AMP for Endpoints

Prérequis

| Compréhension technique de la mise en réseau TCP/IP et de l'architecture réseau
| Compréhension technique des concepts et des protocoles de sécurité

Programme de la formation

Présentation des technologies Cisco AMP

| Cisco Talos
| Modèle de sécurité centré sur les menaces AMP
| Cadre de protection
| Cadre de rétrospection

| Cisco SecureX

Présentation de l'AMP pour la présentation et l'architecture des terminaux
| Cisco AMP pour les terminaux
| Architecture infonuagique Cisco AMP
| Nuage privé Cisco AMP
| Cisco AMP pour l'intégration des terminaux

Navigation dans l'interface de la console
| Activation de votre compte Cisco
| Configuration et déploiement de démarrage rapide
| Tableau de bord de la console
| Système de menus

Utilisation de Cisco AMP pour les terminaux
| Explorer votre environnement avec la console AMP
| Opérations système

Identification des attaques
| Identification et confinement d'une menace à faible prévalence
| Utilisation de CVE avec AMP pour les terminaux
| Utilisation de File Trajectory pour suivre une menace

Analyse des logiciels malveillants
| Analyser les événements
| Utilisation de Cisco Threat Grid
| Analyse de fichier
| Autres fonctionnalités d'analyse
| Rapports

Gestion du contrôle des épidémies
| Gestion des détections de logiciels malveillants
| Gérer les indices de compromission

Création de stratégies de point de terminaison
| Configuration des stratégies de point de terminaison - Notions de base
| Configuration des politiques de point de terminaison - Paramètres avancés

Travailler avec AMP pour les groupes de terminaux
| Groupes d'examen
| Configuration des exclusions
| Se préparer à un déploiement
| Déploiement des connecteurs Windows
| Installation de Windows et de l'interface du connecteur
| Dépannage de Cisco AMP pour points de terminaison

Utilisation d'Orbital pour la visibilité des terminaux
| Présentation de Cisco Orbital
| Console orbitale
| Utilisation de Cisco Orbital pour obtenir des informations sur les terminaux
| Syntaxe d'Osquery

Présentation de l'API REST AMP
| Examen de l'API REST AMP
| Documentation et ressources de l'API REST
| Structure de données de réponse à la requête : JSON
| Authentification API REST
| Exécution de transactions d'API REST
| Utilisation des données de l'API REST dans d'autres applications

Naviguer dans les comptes
| Administration des utilisateurs
| Autres options de compte

HUB Formation - 1-7, Cours Valmy - 92923 Paris - La Defense
01 85 77 07 07 - www.hubformation.com - SIREN 525 287 785

Laboratoires

| Auto-enregistrement de compte Amp
| Accéder à AMP pour les terminaux
| Scénario d'attaque
| Outils d'analyse et rapports
| Contrôle des épidémies
| Politiques de point de terminaison
| Groupes et déploiement
| Test de votre configuration
| Visibilité des terminaux avec Orbital
| API REST
| Isolation des terminaux à l'aide de l'API Cisco AMP
| Comptes utilisateur

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.