Formation Trend Micro Deep Security - certification

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

La formation Trend Micro (TM) Deep Se Les meilleures pratiques et les détails de dépannage pour une mise en oeuvre réussie et une maintenance à long terme du système sont également abordés. Ce cours comprend une variété d'exercices pratiques en laboratoire permettant aux participants de mettre le contenu de la leçon en pratique. Ce cours est dispensé par des formateurs certifiés par Trend Micro. À l'issue de ce cours, les participants peuvent choisir de passer l'examen de certification pour obtenir le statut de professionnel certifié Trend Micro pour la sécurité renforcée.

Référence	TRM-DS
Durée	3 jours (21h)
Tarif	2 250 €HT

PROCHAINES SESSIONS

Pour connaître les prochaines dates ou organiser un intra-entreprise, contactez-nous, nous vous répondrons sous 72 heures.

Objectifs

| Utiliser Trend Micro (TM) Deep Security.
| Connaître la sécurité de serveur avancée des ordinateurs physiques, virtuels et cloud.
| Étudier la Deep Security dans un environnement de laboratoire virtuel.

Public

| Administrateurs système
| Ingénieurs de réseau
| Ingénieurs de support
| Ingénieurs d'intégration
| Architectes de solutions et de sécurité

Prérequis

| Serveurs Windows et clients
| Pare-feu et dispositifs d'inspection de paquets
| VMware ESXi / vCenter / NSX
| Amazon AWS / Microsoft Azure / VMware vCloud
| Technologies de virtualisation

Programme de la formation

Présentation du produit
| Solutions Trend Micro
| Introduction à la sécurité profonde
| Modules de protection
| Composants Deep Security

Deep Security Manager
| Configuration requise pour le serveur et le système d'exploitation
| Exigences de base de données
| Architecture et composants de Deep Security Manager
| Installation de Deep Security Manager
| Connexion à la console Web Deep Security Manager

Deep Security Agent
| Architecture Deep Security Agent
| Installation d'agents de sécurité profonde
| Ajout d'ordinateurs
| Activation des agents de sécurité profonde

| Mise à niveau d'agents de sécurité profonds en relais
| Distribution de logiciels et de mises à jour de sécurité
| Affichage de l'état de protection de l'ordinateur
| Organisation des ordinateurs à l'aide de Smart Folders

Policies
| Création de stratégies basées sur des analyses de recommandation
| Créer de nouvelles politiques à partir de zéro
| Héritage et substitutions de règles
| Objets communs

Anti-Malware
| Plate-forme de solution anti-malware
| Analyse anti-programmes malveillants
| Activation de la protection contre les logiciels malveillants
| Mise en quarantaine de fichiers
| Smart Scan

Réputation Web
| Moteur de filtrage d'URL Trend Micro
| Activation de la réputation de sites Web
| Réglage du niveau de sécurité
| Localisation d'événements liés à la réputation de sites Web

Pare-feu
| Règles de pare-feu
| Ordre d'analyse des règles
| Filtrage à état et pseudo-état
| Évaluation des vulnérabilités

Prévention d'intrusion
| Patching virtuel
| Protocole d'hygiène
| Contrôle de protocole
| Protection des applications Web
| Activation de la prévention des intrusions
| Règles de prévention des intrusions
| Filtrage SSL

Integrity Control
| Activation de la surveillance de l'intégrité
| Détection des modifications sur l'objet de base
| Marquage d'événement

Contrôle d'application
| Activation du contrôle des applications
| Détecter les modifications logicielles
| Création et inventaire de logiciels approuvés

Inspection des logs
| Activation de l'inspection des journaux
| Exécution d'analyses de recommandation
| Suivi des événements

Logs et rapports
| Activation de la journalisation de débogage
| Définition des niveaux de journal
| Intégration SIEM et syslog
| Faire rapport
| Filtrage des données du rapport
| Création de packages de diagnostic

Multi-Tenancy
| Activation de la multi-location
| Création de locataires
| Gestion des locataires

| Activation des agents Deep Security sur les locataires
| Surveillance de l'utilisation

Défense connectée contre les menaces
| Exigences liées à la défense contre les menaces
| Analyseur de découverte en profondeur
| Trend Micro Control Manager
| Intégration de la sécurité profonde à la défense contre les menaces connectées

Protéger les environnements cloud
| Modèles de déploiement cloud
| Architectures de Cloud Deep Security
| Amazon AWS
| Microsoft Azure
| VMware vCloud
| Options d'installation dans le cloud

Deep Security Virtual Appliance
| Protection sans agent
| Déploiement de Deep Security dans les environnements VMWare ESXi

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.

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.