PROGRAMME DE FORMATION TREND MICRO – Deep Security

Intitulé : **Formation TREND MICRO Deep Security**
Cris Réseaux organisme de formation agréé N° 93130819313

Introduction :

Cette formation a pour but de présenter la mise en œuvre et le fonctionnent de la plateforme de gestion sécurité Trend Micro Deep Security.
Surveillance et sécurisation des serveurs, postes de travails, bureau virtuel (VDI) et environnement virtuel public ou privée.

Public :

Ce cours est conçu pour VAD, partenaires, revendeurs et professionnels de l'informatique responsables de la protection des réseaux, point de terminaison, Cloud et menaces de sécurité. Administrateur Sécurité Système & Réseaux, Ingénieur technique Avant-ventes, Technicien Intégrateur de solution.

Modalités pédagogiques mobilisées

La formation est délivrée soit en présentiel (en face à face pédagogique en salle), soit en distanciel (présence à distance du formateur grâce à un système de visio et utilisation de la plateforme).
La formation alterne cours théorique et travaux pratiques.
Les stagiaires reçoivent un support de cours en format PDF,
Le support de cours est composé des travaux pratiques (Labs) et de leurs corrections.
Afin de pouvoir mettre en pratique les éléments du cours, les stagiaires ont à leur disposition un environnement virtuel technique complet.

Objectifs de la formation

L'objectif de cette formation est de permettre aux participants de se familiariser avec Trend Micro Deep Security et ses principales fonctionnalités.
Cette formation vous apportera les connaissances nécessaires pour mettre en place une architecture complète Deep Security, les scénarios de déploiement.
A l'issue de cette formation, les participants seront capables :

- Installer Deep Security,
- Connaitre les détail de dépannage
- Configurer et administrer
- Déployer Deep Security dans un environnement d'un réseau sécurisé.

Modalités d'évaluation de la formation

- Travaux pratiques (Labs) et de leurs corrections
- Bilan de fin de formation.
- Examen de certification

Modalités, délais d'accès et Tarifs :

Nous contacter.

Lieu, durée et inscriptions

Cris Réseaux propose des sessions de formation inter-entreprise en présentiel ou distancielle.

Nos formateurs peuvent également intervenir en formation intra-entreprise (sur site ou à distance) à partir de 5 personnes.

La formation Trend Micro- Deep Security dure 21 heures, réparties en trois journées consécutives de 7h par jour.

Toutes les demandes d'inscription doivent être envoyées à notre service de formation formation@cris-reseaux.com.

L'effectif maximum est de 8 personnes par session.

Nos formations sont accessibles à toute personne en situation de handicap. Il est demandé de le signaler dès la prise de contact avec le service formation, fin d'anticiper au mieux les besoins et étudier les compensations nécessaires.

Prérequis Technique :

Public issu du technique en réseau et informatique.

Prérequis Matériel :

Matériel nécessaire : PC fixe ou portable, 8Go Ram, Navigateur Web, Audio Casque ou HP. Accès Internet 8 Mbs minimum.

Description détaillée de la formation : *Sur 3 Jours*

Jour 1 :

Présentation général et tour de table

1. Chapitre 1 : Trend Micro Vision Globale
    a. Les solutions
    b. Trend Micro Xgen Security
    c. Les modules de protection
    d. Caractéristique clés
    e. Détection des menaces
2. Chapitre 2 : Deep Security Manager
    a. Base de données
    b. Deep Security Manager Architecture
    c. Installation du DSM
    d. Mise à jour vers la solution Deep security 12
3. Chapitre 3 : Déploiement du Deep Security Agent
    a. Architecture du Deep Security Agent
    b. Déploiement

   c. Les Opérations à travers les lignes de commandes
   d. Visualiser le status de protection
   e. Les agents hors lignes
   f. Mise a jour vers deep security 12
   g. Regroupement des machines
      1. Lab 1 : Accès a l'environnement de Lab Deep Security
      2. Lab 2 : Déploiement de Deep Security Agent
4. Chapitre 4 : Les Mises à jour
   a. Mises à jour de sécurité
   b. Mise a jour logiciel
   c. Programmation
   d. Relais de mise a jour
      1. Lab 3 : Déploiement du Deep Security agent relais
5. Chapitre 5 : Trend Micro Smart Protection
   a. Service de réputation de fichier
   b. Service de réputation Web
   c. Service de Machine d'Apprentissage prédictif
   d. Service Census
   e. Service de logiciel certifié
   f. Smart feedback
   g. Smart protection source
6. Chapitre 6 : Les politiques
   a. Structure des politiques
   b. Création des politiques
   c. Objets Commun
   d. Exécuter un scan de recommandation

Jour 2 :

7. Chapitre 7 : Protéger les servers face au malware
   a. Plateform de solution Anti-malware
   b. Méthodes de scan
   c. Activation de la protection
   d. Retrouver les évènements et fichiers malveillant
   e. Smart scan
      1. Lab 4 : Protéger les servers contre les malwares
8. Chapitre 8 : Bloquer les sites web malicieux
   a. Moteur d'analyse d'url
   b. Activation de la protection
   c. Consulter les évènements
      1. Lab 5 : Bloquer les Sites web malicieux
9. Chapitre 9 : Filtrer le traffic en utilisant le pare feu
   a. Activation du pare feu
   b. Règles de pare feu
   c. Règles de pare-feu recommandées
   d. Ordre d'analyse
   e. Consulter les évènements
      1. Lab 6 : Filtrer le Traffic en utilisant le pare feu
10. Chapitre 10 : Protéger les servers contre les vulnérabilités
   a. Bloquer des exploits en utilisant la prévention d'intrusion
   b. Activation de la prévention d'intrusion
   c. Les règles de préventions
   d. Filtrage SSL

e. Protéger les applications web
f. Consulter les évènements
    1. Lab 7 : Protection contre les vulnérabilités
    2. Lab 8 : Bloquer le traffic avec les règles de prévention

11. Chapitre 11 : Détecter les changements des servers protégés
    a. Activation du moniteur d'intégrité
    b. Détection des changements
    c. Consulter les évènements
        1. Lab 9 : Détection des changements sur les servers protégés
12. Chapitre 12 : Bloquer les logiciels non approuvés
    a. Les modes de contrôle
    b. Activation du control applicatif
    c. Consulter les évènements
    d. Blocage global
    e. Pre-approuvé les mises à jour logiciels
    f. Ordre d'analyse de l'application control

Jour 3 :

13. Chapitre 13 : Inspecter les logs des servers protégés
    a. Activation de l'inspection des logs
    b. Consulter les évènements
    c. Monitorer les évènements Windows
        1. Lab 11 : Inspections des logs sur les serveurs protégés
14. Chapitre 14 : Evènements et alertes
    a. Transfert des évènements
    b. Les alertes
    c. Tag d'événements
    d. Les rapports
15. Chapitre 15 : Protections des containers
    a. Intégration continue / Déploiement continue
    b. Développement continue en utilisant les containers
    c. Concept et terminologie
    d. Protection des containers avec Deep security
16. Chapitre 16 : Automatisations des Opérations
    a. Tâche automatisée
    b. Tâche programmée
    c. Tâche basée sur un évènement
    d. Les modèles
    e. Préparation d'un agent sur une machine Amazon
    f. API
        1. Lab 12 : Accès a Deep Security à travers l'API
17. Chapitre 17 : Détection des malwares à travers la défense interconnectée contre les menaces
    a. Les phases de la défense inter connecté contre les menaces
    b. Trend Micro Apex central
    c. Deep Discovery analyser
    d. Traquer les objets suspicieux
        1. Lab 13 : Intégration à travers le Connected threat defense

18. Chapitre 18 : Activation et administration des tenants
    a. La segmentation a travers le multi-tenant
    b. Activation du mode multi-tenant
    c. Activation de l'agent Deep Security dans un tenant

    d. Superviser l'utilisation
    e. Administration
        1. Lab 14 : Activation de plusieurs tenants
19. Chapitre 19 : Protection des machines virtuelles à l'aide de Deep Security Virtual Appliance
    a. Deep security virtual appliance
    b. Déploiement et activation
    c. Deep security Manager et Vmware Vcenter
    d. Protection anti-malware sans agent
    e. Protection de l'intégrité sans agent
    f. Haute disponibilité Vmware
        1. Lab 15 : Configuré la protection sans agent

Examen de certification :

A l'issue de la formation les stagiaires ont accès sur leur espace privé à l'examen de certification en ligne avec 50 questions en 90 mn.
Le score minimum de certification est de 70%.
En cas d'échec, un deuxième et un troisième passage d'examen est possible.