PROGRAMME DE FORMATION TREND MICRO – Apex One

Intitulé : **Formation TREND MICRO ApexOneCris**

Réseaux organisme de formation agréé N° 93130819313

Introduction :

Suite à cette formation, les participants vont acquérir des connaissances techniques à utiliser Trend Micro APEX ONE.
Cette formation vous apportera

- les connaissances nécessaires pour mettre en place une architecture complète Apex One,
- les scénarios de déploiement,
- l'installation de base, les options de configuration et d'administration
- les détails de dépannage d'un réseau que les administrateurs doivent connaitre pour une mise en œuvre réussie et à long terme pour la maintenance.

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 technique complet.

Objectifs de la formation

L'objectif de cette formation est de permettre aux participants de se familiariser avec Trend Micro Apex One et ses principales fonctionnalités.
A l'issue de cette formation, les participants seront capables :

- Installer,
- Configurer et administrer
- Déployer Apex One dans un environnement de production.

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 Apex One 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 des stagiaires (tour de table)

1. Chapitre 1 : Trend Micro Vision Globale
    a. Les solutions
    b. Trend Micro Xgen Security
    c. Méthodes de déploiement
    d. Caractéristique clés
    e. Détection des menaces
2. Chapitre 2 : Trend Micro Apex one Server
    a. Apex One server services et composants
    b. Apex One base de données
    c. Installation de la solution
    d. Upgrade d'Officescan vers Apex one
    e. Upgrade vers Apex One as a service
    f. Plug-in et Utilitaires
3. Chapitre 3 : Trend Micro Apex One Console de management
    a. Interface de gestion et de management
    b. Intégration Active Directory
    c. Compte d'administration
    d. Retrouver un mot de passe perdu
4. Chapitre 4 : Administration des agents de sécurité

a. Les agents de sécurité - services et composants
b. Les agents de sécurité - Prérequis technique
c. Les agents de sécurité – Installation
d. Les agents de sécurité – Migration d'une autre solution de sécurité
e. Les agents de sécurité – Communication agent server
f. Déplacement d'agent entre différents servers
g. Les agents de sécurité – Désinstallation
h. Les agents de sécurité – Paramètre et regroupement
i. Les agents de sécurité –Protection et privilège

1. Lab 1 : Accès à l'environnement de Lab Deep Security
2. Lab 2 : Installer les agents de sécurité
3. Lab 3 : Regroupement des agents

5. Chapitre 5 : Administration des agents hors site
   a. Installation du server Edge Relais
   b. Enregistrement et Certificats
6. Chapitre 6 : Garder la solution Apex one a jour
   a. Active Update
   b. Mise à jour du server
   c. Mise à jour des clients
   d. Téléchargement et déploiement
   e. Outil

1. Lab 4 : Mise à jour des agents

Jour 2

7. Chapitre 7 : Trend Micro Smart Protection
   a. Service de réputation des fichiers
   b. Service de réputation Web
   c. Machine d'Apprentissage prédictif
   d. Service Census
   e. Service logiciel certifié
   f. Smart feedback
   g. Service d'url

1. Lab 5 : Installer un server smart protection server

8. Chapitre 8 : Protéger les machines contre les menaces
   a. Scan Malware
   b. La quarantaine
   c. Smart scan
   d. Prévention des épidémies

1. Lab 6 : Protéger les machines contre les malwares

9. Chapitre 9 : Protéger les machines à travers l'analyse comportemental
   a. Analyse comportementale
   b. Exception

1. Lab 7 : Protéger les machines a travers l'analyse comportemental

10. Chapitre 10 : Protéger les machines contre les menaces inconnues
    a. Vulnérabilités et exploit

   b. Machine d'Apprentissage prédictif
   c. Mode sans connexion
      1. Lab 8 : Protéger les machines des menaces inconnues
11. Chapitre 11 : Bloquer les menaces web
   a. La réputation Web
   b. Détection des connexions suspectes
   c. Protection contre les Exploits
      1. Lab 9 : Bloquer les menaces web
12. Chapitre 12 : Protéger les machines à travers le filtrage de Traffic
   a. Filtrage du Traffic
   b. Activation du pare feu
   c. Politique et profil
      1. Lab 10 : Protéger les machines a travers le pare feu
13. Chapitre 13 : Gestion de la perte de données
   a. Protection contre la perte de donnée
   b. Control des actifs
   c. Contrôle de périphériques
      1. Lab 11 : Prévention contre la perte de donnée

Jour 3

14. Chapitre 14 : Déployer les politiques à travers Apex Central
   a. Apex Central
   b. Mode de management
   c. Administration des politiques Apex One
   d. Héritage des politiques
   e. Politique de découverte de données
      1. Lab 12 : Administrer les politiques a travers l'Apex Central
15. Chapitre 15 : Détecter les menaces à travers le Connected Threat Defense
   a. Comment fonctionne la défense inter connectés
   b. Deep Discovery analyzer
   c. Les objets suspicieux
   d. Enregistrement d'Apex One a la liste des Objets Suspicieux
   e. Traquer les Objets suspicieux
      1. Lab 13 : Soumettre les fichiers suspicieux a l'analyse
16. Chapitre 16 : Bloquer les applications non approuvées
   a. Méthodes de blocage des applications
   b. Mode confinement
   c. Critère de control des applications
   d. Règle définie par utilisateur
   e. Bonne pratique pour l'activation de l'application control
      1. Lab 14 : Bloquer les applications non autorisées
17. Chapitre 17 : Protéger les machines des vulnérabilités
   a. Protection contre les vulnérabilités intégrées
   b. Les signatures

c. Moteur d'analyse réseau
    1. Lab 15 : Protection des machines contre les vulnérabilités

18. Chapitre 18 : Détecter et investiguer les incidents de sécurité
    a. Capteur intégré
    b. Détection et réponse a incident
    c. Modèle de réponse
    d. Investigation détaillée
    e. Découverte d'attaque
    f. Service de détection et réponse managé
        1. Lab 16 : Détection et investigation

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.