PROGRAMME DE FORMATION TREND MICRO – Vision One

Intitulé : **Formation TREND MICRO VisionOneCris**

Réseaux organisme de formation agréé N° 93130819313

Introduction :

Suite à cette formation, les participants vont acquérir des connaissances techniques pour utiliser TrendMicro VISION ONE.
Cette formation vous permettra :

- De décrire les avantages d'une solution XDR
- Connecter les produits Trend Micro à Trend Micro Vision One
- Collecter des données télémétriques à partir des points finaux, du courrier électronique, du Web et du réseau
- Intégrer des produits tiers à Trend Micro Vision One

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 Vision One et ses principales fonctionnalités.
A l'issue de cette formation, les participants seront capables :

- Déployer Vision One dans un environnement de production
- Configurer et administrer la solution
- Créer des playbooks pour rationaliser les activités de réponse aux incidents
- D'utiliser les outils de recherche pour localiser des informations

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 Vision 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 : Concepts XDR
    a. Collecte de données télémétriques
    b. Corrélation des données
    c. MITRE ATT&CK
2. Chapitre 2 : Trend Micro Vision One
    a. Comment Trend Micro Vision One s'intègre dans la plateforme Trend Micro One
    b. Capacités de base de Trend Micro Vision One
    c. Fonctionnalités de Trend Micro Vision One pour XDR
    d. Applications Trend Micro Vision One
3. Chapitre 3 : Connexion des produits Trend Micro
    a. Collecte d'événements de sécurité
    b. Connexion de Trend Micro Apex One™ as a Service
    c. Connexion de Deep Security™ Software
    d. Connexion de Trend Micro Cloud One™ - Endpoint & Workload Security
    e. Connexion de Cloud App Security
    f. Connexion de la passerelle de services (Service Gateway)
    g. Connexion de Web Security™
    h. Connexion de Deep Discovery™ Inspector
    i. Connexion de TippingPoint™ SMS

Jour 2

4. Chapitre 4 : Activation des capteurs XDR
    a. Installation de Endpoint Basecamp
    b. Création de groupes et de politiques de sécurité
    c. Activation des capteurs de points finaux
    d. Activation des capteurs de messagerie
    e. Activation des capteurs réseau
    f. Activation des capteurs web
5. Chapitre 5 : Intégration avec Produits Tierces-Parties
    a. Objectifs d'intégration
6. Chapitre 6 : Utiliser l'application XDR Investigation des Menaces
    a. Applications XDR
    b. Visualisation des données brutes d'événements et d'activités de sécurité
    c. Filtrage des événements de sécurité et des données d'activité
    d. Workbenches
    e. Actions du Workbenche
    f. Profils d'exécution
    g. Analyse du réseau
    h. Automatisation des réponses
    i. Détection d'attaques ciblées
    j. Gestion des réponses
    k. Managed XDR service

Jour 3

7. Chapitre 7 : Partage des renseignements sur les menaces
    a. Rapports de veille et rapports personnalisés
    b. Gestion des objets suspicieux
    c. Analyse des bacs à sable (Sandbox)
8. Chapitre 8 : Recherche dans le lac de données
    a. Syntaxe de recherche simple et complexe
    b. Conseils de recherche
    c. Listes de surveillance
9. Chapitre 9 : Répondre aux incidents à l'aide des Playbooks
    a. Modèles de Playbooks
    b. Déclencheurs de Playbooks
    c. Conditions du Playbook
    d. Actions du Playbook

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.