PROGRAMME DE FORMATION

TREND MICRO – VISION ONE
Security Operations (SecOps)

Cris Réseaux organisme de formation
N° Déclaration d'activité : 93130819313

Introduction :

Grâce à cette formation, les participants vont acquérir des connaissances techniques pour utiliser Trend Micro VISION ONE.
La formation est éligible aux financements par les OPCO.

Public :

Ce cours est conçu pour les VAD, partenaires, revendeurs et professionnels de l'informatique, responsables de la protection des réseaux.
Administrateurs Sécurité Système & Réseaux, Ingénieurs technique Avant-ventes, Techniciens Intégrateur de solution.

Modalités pédagogiques

-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.
-Ressources pédagogiques :
Afin de maintenir l'expertise du stagiaire, ce dernier peut consulter son support de cours en PDF.
Consulter les ressources sur le site de Trend Micro à partir de son compte personnel.
Il peut également consulter différentes ressources sur le site de Cris Réseaux:
https://www.cris-reseaux.com/service-technique/ressources/
Support technique Cris Réseaux : 04 84 47 42 25

Objectifs de la formation

A l'issue de la formation, les stagiaires auront acquis les compétences suivantes :

- Décrire les avantages d'une solution XDR
- Connecter les produits Trend Micro à Trend Micro Vision One
- Collecter la télémétrie provenant des **endpoints**, des **emails**, du **web** et du **réseau**
- Intégrer des produits tiers à Trend Micro Vision One
- Interpréter et naviguer dans les **Workbenches**
- Utiliser les outils de recherche pour localiser des informations dans le **data lake**
- Créer des **Playbooks** afin de rationaliser les activités de réponse

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/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.

Dans le cadre de nos formations, l'accueil des personnes en situation de handicap est possible après évaluation de la nature du handicap. Afin d'anticiper au mieux les besoins et étudier les compensations nécessaires, il est demandé de le signaler dès la prise de contact avec le service formation.

Modalités, délais d'accès et Tarifs :

Nous contacter.

Prérequis Technique :

Public issu du technique en réseau et informatique, avoir complété la formation Trend Vision One Security Operations Advanced

Prérequis Matériel :

Les prérequis matériels dépendent du format de la session.
En présentiel :
- PC portable avec une interface réseau filaire et un système d'exploitation Windows de préférence (physique ou virtuel en accès réseau par pont) avec droits d'administrateur ; et disposant des logiciels

suivants : Firefox, PuTTY (ou tout autre client SSH), WinSCP (ou client SCP équivalent), Wireshark, VirtualBox ou équivalent VMWare (VMWare Workstation Player ou Pro).
En distanciel:
- Navigateur web, en dernière version : Chrome ou Firefox ou Edge avec pour la réalisation des travaux pratiques (seuls ces navigateurs sont supportés).
- Accès internet avec un débit minimal de 2Mb/s - Un 2ème écran est fortement recommandé (22'' ou plus)
Pour les formations distancielles, les stagiaires doivent avoir une webcam et un micro fonctionnels, ainsi que les droits d'installation pour le logiciel de visio.

Description détaillée :

Présentation générale et tour de table
Chapitre 1 :

a. Concept XDR
b. Collecte de données télémétriques
c. Corrélation des données
d. MITRE ATT&CK

Chapitre 2 : Trend Micro Vision One

a. Fonctionnalités principales de Trend Vision One
b. Fonctionnalités de Trend Micro Vision One pour XDR

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 Trend Micro Apex One™ (on-premises)
d. Connexion de Trend Micro Cloud One™ - Endpoint & Workload Security
e. Connexion de Deep Security™ Software
f. Connexion de Cloud App Security
g. Connexion de la passerelle de services (Service Gateway)
h. Connexion de Web Security™
i. Connexion de TippingPoint™ SMS
    - LAB 1-2-3

Chapitre 4 : Activation des capteurs XDR

a. Décrire l'utilisation des capteurs Trend Vision One
b. Connexion des capteurs de point de terminaison
c. Connexion des capteurs de messagerie électronique
d. Connexion des capteurs réseau
e. Connexion des capteurs web
    - LAB-4

Chapitre 5 : Intégration avec Produits Tierces-Parties

a. Les différentes intégrations tierces disponibles avec Trend Vision One en rapport avec XDR
b. Connecter des applications tierces à Trend Vision One
    - LAB-5

Chapitre 6 : Utiliser l'application XDR Investigation des Menaces

a. Afficher les données brutes relatives aux événements et aux activités
b. Rétention de données
c. Filtrage des événements de sécurité et des données d'activité
d. Workbenches
e. Actions à partir du Workbench
f. Profils d'exécution
g. Analyse du réseau
h. Détection des attaques ciblées
i. Forensics
j. Gestion des réponses
k. Service managés
    - LABS 6-7

Chapitre 7 : Partage des renseignements sur les menaces

a. Décrire comment Threat Intelligence est utilisé dans Trend Vision One.
b. Rapports de veille et rapports personnalisés
c. Gestion des objets suspicieux
d. Analyse des bacs à sable (Sandbox)
    - LABS 8-9

Chapitre 8 : Recherche dans le lac de données

a. Syntaxe de recherche simple et complexe
b. Conseils de recherche
c. Listes de surveillance
    - LABS 10

Chapitre 9 : Répondre aux incidents à l'aide des Playbooks

a. Créer des playbooks
b. Exécuter les playbooks manuellement
c. Télécharger les résultats des playbooks
    - LAB 11

Modalités d'évaluation :

Pendant la formation : LAB et TP permettent d'évaluer l'acquisition des connaissances.
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.