FORMATION TEHTRIS FUNDAMENTALS

Ce cours est destiné aux administrateurs systèmes, analystes SOC, responsables sécurité et ingénieurs sécurité qui utilisent, déploient ou gèrent la solution TEHTRIS XDR.

OBJECTIF

Ce cours de 3 jours permettra de comprendre les concepts des solutions EDR/XDR et d'acquérir les compétences nécessaires pour déployer et gérer au quotidien la solution TEHTRIS XDR. Les différents workshops réalisés au cours de cette formation vous permettront d'utiliser les différents composants de la solution TEHTRIS, vous donnant ainsi les compétences au traitement d'un incident de sécurité.

CONTENU

La formation se présentera sous forme de présentation « slides » et de manipulation sur un environnement de lab.

Ce cours comprend :
- Support de formation au format électronique

Ce cours ne comprend pas :
- Frais d'hébergement
- Support de cours au format papier

PRE-REQUIS

Connaissances Système, connaissances réseaux et sécurité.
Formation eLearning:
- XDR
- SIEM
- SOAR
- Data Analytics

CERTIFICATION

Cette formation vous permettra d'acquérir les certifications XDR, SOAR et SIEM.

INSCRIPTION

Merci de nous contacter par mail: formation@ignition-technology.com

PRIX

TARIF PUBLIC: 2190,00€ HT

DURÉE ET LIEU

La formation dure 3 jours et commence à 9h le matin pour se finir vers 18h (17h le dernier jour).
La formation est disponible au format intra-entreprise et extra-entreprise.
Pour connaitre les dates des prochaines formations, merci de nous contacter par mail: formation@ignition-technology.com

AGENDA

JOUR 1:
- Introduction au concept de XDR
- Installation et Configuration des différents composants EDR (filtres, politiques de sécurité, Whitelists/Blacklists, Application Policy)

JOUR 2:
- Introduction à la CyberThreat Intelligence TEHTRIS
- Installation et configuration de la solution TEHTRIS EPP (mise en place de règles, exclusion, filtres, firewall)
- Configuration de la solution SIEM (Installation, Configuration, Investigations)/Mise en place de scénario SIEM
- Utilisation du composant Analytics (Discover, Visualize, Dashboard)
- Echange sur différents cas d'usage

JOUR 3:
- Mise en place de différents playbook d'orchestration au travers du module SOAR (Playbook email, Ticket, IOC Hunting)
- Exercice de traitement d'incidents de sécurité au travers de l'exploitation d'un scénario d'attaque