



Présentation

Code interne : IT320

Description

Donner aux élèves les fondamentaux pour intégrer des CERT & SOC.(Centre de réponse à incident / analyste de la menace). Avoir un apprentissage sur la connaissance de la menace et donner les capacités aux élèves de faire leurs premières « Threat Analysis ». On veillera à rendre le sujet pratique par la mise en place :

1. d'une plateforme OPENCTI
2. du développement de leurs plateformes DRSD : Détection Ransomware Surveillance Deep & DarkWeb.

Objectifs

Threat Intelligence :

1. Définition
2. Cycle de vie de la Threat Intelligence
3. Pratiquer la Threat Intelligence
4. Intelligence Source
5. Traffic Light Protocol

Les Acteurs de la menace et les modes opératoires :

1. Les acteurs et leurs motivations
2. Procédure d'attribution

Analyse de la menace : Tools & Procédures

1. Les outils { Data collection, Data processing, etc
2. YARA Rules
3. Analyses de LOG
4. Anatomie des Règles Sigma
5. MSTICpy

Heures d'enseignement

CI

Cours Intégrés

16h

Modalités de contrôle des connaissances

Évaluation initiale / Session principale

Type d'évaluation	Nature de l'évaluation	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'évaluation	Note éliminatoire de l'évaluation	Remarques
Contrôle Continu	Contrôle Continu			1		

Seconde chance / Session de rattrapage

Type d'évaluation	Nature de l'évaluation	Durée (en minutes)	Nombre d'épreuves	Coefficient de l'évaluation	Note éliminatoire de l'évaluation	Remarques
Projet	Rapport					