Module : Cyber Threat Intelligence				Code	
				ING-4-SSIR-S9-P4	
Période	**Semestre 1**	*Volume horaire*	**21h**	*ECTS*	**2**

Responsable	**Mohamed Aymen Karmous**	*email*	Mohamed.aymen.karmous@gmail.com
Equipe pédagogique	**Mohamed Aymen Karmous**		

1. Objectifs de Module *(Savoirs, aptitudes et compétences)*

Ce module porte sur : Cyber Threat Intelligence.

Acquis d'apprentissage :

A la fin de cet enseignement, l'élève sera capable de :

C1.1 Maitriser le rôle du renseignement sur les cybermenaces dans les opérations de cybersécurité

C1.1 Concevoir une réflexion critique pour faire face à des menaces persistantes et ciblées.

2. Pré-requis *(autres UE et compétences indispensables pour suivre l'UE concernée)*

- Se familiariser avec les bases de la mise en réseau
- Se familiariser avec la terminologie de la sécurité
- Pentesting
- Ligne de commande Linux

3. Répartition d'Horaire de Module

Intitulé de l'élément d'enseignement	*Total*	*Cours*	*TD*	*Atelier*	*PR*
Module : Cyber Threat Intelligence.	21h	12h	9h		

4. Méthodes pédagogiques et moyens spécifiques au Module

(pédagogie d'enseignement, ouvrages de références, outils matériels et logiciels)

- Supports de Cours
- Projecteur et Tableau
- Travaux dirigés

Bibliographie

Titre	Auteur(s)	Edition
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf https://www.giac.org/paper/gcih/27783/cyber-threat-intelligence-support-incident-handling/149720 https://www.sans.org/course/cyber-threat-intelligence		

5. Contenu *(Descriptifs et plans des cours / Déroulement / Détail de l'évaluation de l'activité pratique)*	Durée allouée	
Cyber Threat Intelligence		
Séance 1 : • Introduction to cyber security operations • Introduction au threat landscape • Comprendre le besoin d'une solution qui répond aux threats existantes • Partage du contenu du projet avec les étudiants	Cours	3H
Séance 2 : • Terminologie de base de Cyber Threat Intelligence • Exemple d'utilisation du Cyber Threat Intelligence	TD	3H
Séance 3 : • Cycle de renseignement et exemple de processus Cyber Threat Intelligence • Normes et protocoles Cyber Threat Intelligence	Cours	3H
Séance 4 : • Collection de données • Sources de collecte (internes et externes) • Exemples d'utilisations de la collection de données	Cours TD	1.5H 1.5H
Séance 5 : • Open Source Intelligence (OSINT) & scanners • Exemples existants	Cours TD	1.5H 1.5H
Séance 6 : • Modèles Cyber Threat Intelligence • Cyber Kill Chain framework • MITRE ATT&CK framework • Exemples d'utilisation des modèles	Cours TD	1.5H 1.5H
Chapitre 7 : • Présentation du project • Correction du projet	Cours TD	1.5H 1.5H

6. Mode d'évaluation de Module *(nombre, types et pondération des contrôles)*

Eléments d'enseignement	Coeff	DS	EX	TP	PR
Module – Cyber Threat Intelligence	1	40%	60%		

Pour valider le module, les étudiants passeront un examen dont le coefficient est de 60%, un DS (projet) dont le coefficient est de 40%.

La durée de tous les examens (Examen, DS…) est de 1h30.

Le DS est planifié dès le début début du module.

Quant à l'examen, il est planifié après l'écoulement des 7 semaines et portera sur toutes les thématiques enseignées tout au long des 21 heures.

Le module est validé si l'étudiant obtient une moyenne supérieure ou égal à 10 sur 20.