Cyber Awareness

Cyber Awareness	ECTS		4	SEMESTRE	S7
7KUCEN18	CM	TD	TP	EI	Travail personnel
	12h	24h	0h	0h	12h

Langues d'enseignement	Français
Responsable(s)	Laurent CIARLETTA blocked URL et interventions de E.Richard (Groupe La Poste), D. Szniten (Klee Group)
Mots clefs	Cybersécurité, Système d'Information / SI, Systèmes Cyber Physiques, IoT, Ingénierie-Sociale
Prérequis	Être motivé, bases de l'informatique, algorithmique, bon niveau en programmation (Python), connaissances générales scientifiques et managériales

Objectif pédagogique

De l'appréhension des risques liés à la cybersécurité à leur appréhension

Organisation et contenus

On peut constater que les ressources et infrastructures informatiques sont au cœur de nos quotidiens : depuis les sites industriels, nos entreprises, jusque dans nos véhicules et nos environnements domestiques. Ce phénomène s'intensifie, mais le corollaire est qu'on assiste à une augmentation constante des risques liés à la Sécurité de tous ces systèmes de systèmes Cyber (et Cyber-Physiques) : en nombre, variété et dans leur impact. Ainsi que ce soit dans notre vie quotidienne mais aussi professionnelle, une compréhension des enjeux et des techniques liées à la cybersécurité s'avère une nécessité. Il s'agit d'être préparé car la question devient quasiment non pas de savoir si cela va vous arriver mais quand...

1. « Cyber » ?
   a. Code, Programmation, Applications, Réseaux, Systèmes et S.I en accéléré
   b. Rappels et présentation des outils utilisés en réseaux et systèmes (autour de Python), mise à niveau
2. Cyber-sécurité pour les systèmes d'information (SSI), sur les principes de l'ANSSI Agence Nationale de la Sécurité des Systèmes d'Information (SecNumAcademie)
   a. Panorama de la SSI,
   b. Sécurité de l'authentification, sécurité sur Internet, sécurité du poste de travail et nomadisme,
   c. Pour surveiller, écouter, agir : créer ses propres outils avec Python,
   d. Le vocabulaire, et quelques outils sur étagère
   e. Au plus près de l'exécution du code
3. Systèmes Cyber-Physiques (de l'IoT au SCADA) :
   a. Panorama des technologies autour des objets connectés : IoT, SCADA, véhicules, robots et systèmes autonomes, immotique/domotique
   b. Les enjeux de leur sécurisation et méthodes pour leur sécurisation
   c. Mise en œuvre guidée sur divers systèmes
4. Autour de l'ingénierie sociale et ses enjeux :
   a. Phishing etc.
   b. Mise en œuvre sur un Serious Game

Outils et Plateformes :

Tech'Lab, Salle de Reverse Engineering, Matériel CoTS (WiFi Pinneapple, Bash Bunny, Packet Squirrel, O.M.G Cable), Logiciel (Kali Linux etc.), Jeux Sérieux

Compétences

Niveaux	Description et verbes opérationnels
Connaître	La réglementation, les bonnes pratiques, les principaux outils Le vocabulaire du domaine
Comprendre	Appréhender les risques liés au monde cyber (-physique), les parties prenantes, les méthodes de sécurisation
Appliquer	Prise en main guidé d'outils du marché
Analyser	Les risques présentés par des systèmes (S.I, CPS, sociaux)
Synthétiser	Exprimer des préconisations autour de la sécurité
Évaluer	Les principaux risques que posent un système

Contributions aux Objectifs de Développement Durable des Nations Unies

Modalités de contrôle des connaissances et compétences

Contrôle Continu	☑	Examen écrit	☐	Oral / Soutenance	☐	Rapport / Projet	☑