Annexe 1 – Description du contenu des cours ouverts (CC Cybersécurité) donnée à titre indicatif

1. CyberDefense and forensics 30 h cours 30 h HTPS

ACQUIS D'APPRENTISSAGE

- Identifier une attaque en cours
- Appliquer une analyse des risques en vue de limiter les dommages
- Être capable d'appliquer les méthodes de détection d'intrusions : IDS (intrusion detection systems)
- Appliquer les techniques de prévention : IPS (Intrusion prevention systems)
- Sécuriser les applications web et mobiles
- Renforcer un dispositif / système / réseau informatique (ou une partie critique) face à une attaque
- Appliquer des contre-mesures défensives ou offensives
- Analyser a posteriori les traces d'une attaque
- Récupérer une installation maximalement fonctionnelle
- Agir en professionnel éthique et responsable

CONTENU : DESCRIPTIF ET COHERENCE PEDAGOGIQUE

- Context-dependent risk and criticality analysis
- Pentesting and vulnerability assesment
- Intrusion detection and prevention
- Anomaly detection and identification
- Malicious activity detection and identification
- Side-channel Attacks detection
- Web and Mobile applications security
- Disaster Recovery
- Defense-in-depth
- Multiple independent levels of security (for example, in IoE)
- Countermeasures
- Security Incident and Event Management (SIEM) and dynamically enabled cyber-defense
- Data and system recovery
- Data mining for cyber-forensics

2. Cybersecurity 30 h cours 20 h (HTPS)

ACQUIS D'APPRENTISSAGE

- Connaissances théoriques de base en développement sécurisé d'applications
- Savoir que sécuriser, comment le faire, à quel moment, à quel coût
- Être conscient de la culture utilisateur de la cybersécurité

CONTENU : DESCRIPTIF ET COHERENCE PEDAGOGIQUE

- Introduction
- Contrôle d'accès
- Attaques par canal intermédiaire et rémanence de données
- Programmes set-uid
- Buffer overflow
- Race condition attacks

3. Ethical Hacking Project 10h

ACQUIS D'APPRENTISSAGE

- Mettre en œuvre des stratégies de cybersécurité pour les applications
- Mettre en place des méthodologies de sécurisation d'infrastructures IT
- Proposer, simuler et tester des méthodes d'attaques et de défenses d'infrastructures IT.
- Pratiquer de l'ethical hacking pour vérifier et valider un niveau de sécurité
- Agir en professionnel éthique et responsable

CONTENU : DESCRIPTIF ET COHERENCE PEDAGOGIQUE

voir point 2. Cybersécurité

4. Selected Topics in Cybersecurity (30h cours et 20h HTPS)

ACQUIS D'APPRENTISSAGE

Assurer activement une veille scientifique et technologique dans le domaine de la cybersécurité

CONTENU : DESCRIPTIF ET COHERENCE PEDAGOGIQUE

Contenus évolutifs, liés éventuellement aux activités de recherche, pouvant inclure :

- Quantum information science
- Post-quantum cryptography
- Blockchain
- Biometrics
- DevSecOps
- Virtualization
- Specificities of cybersecurity in some domain (healthcare, financial services, public safety, transportation...)
- Cybersecurity team management
- Cyber-criminology and law
- Mobile and Android malware
- AI and IoE security (e.g. Automotive hacking)
- Security of AI models
- Security and Big Data Analytics

- Cloud Computing Security
- Lightweight Cryptography
- Functional Safety