INTITULE DE LA MATIERE : **SECURITE ET OBJETS CONNECTES**

CODE : UE-64 SEMESTRE : 6
NOM DE L'ENSEIGNANT RESPONSABLE : PRESTIGIACOMO

NOMBRE D'HEURES ENCADREES CM : 40 (Deux formations distinctes) (DTD :
TP : A Définir – 2 EP distincts
NOMBRE D'HEURES DE TRAVAIL PERSONNEL DE L'ELEVE – estimation : 5

OBJECTIF GENERAL (pas plus de 5 lignes) :
Cette formation a pour objectif de :

Sur le plan opérationnel en 20h :
- Identifier les risques liés à la sécurité des applications de l'internet des objets
- Avoir un état de l'art des techniques nécessaires à la protection des données pour des solutions IoT
- Etre capable d'identifier les techniques, standards et architectures à déployer pour renforcer la sécurité des solutions IoT

Sur le plan du management en 20h :
- Comprendre et savoir mettre en œuvre un système de management de la sécurité des systèmes d'information – (Général) -Savoir mener une analyse de risques pour une solution IoT
- Avoir les outils méthodologiques, organisationnels pour intégrer la gestion de la sécurité dans les projets IoT
- Connaître le cadre réglementaire nécessaire à la protection des données personnelles traitées par les solutions IoT

CONTENU – PLAN DU COURS (pas plus de 15 lignes) :

VOLET I Sécurité opérationnelle des objets connectés (20H)
- Menaces et vulnérabilités des systèmes IoT (ex. Botnet Mirai) - Évolution des modes d'attaques
- Architectures de sécurité : standards et modèles – solutions de sécurité
- Cryptologie et protection des données : Symétrique, Asymétrique
- Association de la technologie Blockchain avec l'IoT - chiffrement et stockage distribué - Sécurité des API(s)
- Sécurisation du transport des données : protocoles et authentification des objets connectés
- Sécurisation du stockage des données – Intégrité et chiffrement des données - & sécurité dans le Cloud
- Patch Management IoT- Gestion des incidents

VOLET II Management de la sécurité des objets connectés (20H)
- Définition des objectifs de sécurité
- Gouvernance de la Cyber Sécurité - SMSI 27001 / 27002
- Gestion des risques par la pratique - Méthode EBIOS Risk Manager
- Normes et consortiums : IoT Cybersecurity Alliance, OWASP, NIST
- Protection des données personnelles / Violation de données : RGPD et IoT
- Intégrer la sécurité dans les projets IoT
- Certifications de sécurité pour les solutions IoT

FORME DE L'EVALUATION :
☐ Contrôle continu ☐ Contrôle terminal ☐ Mémoire/rapport ☐ Soutenance
préciser si nécessaire, nombre d'épreuves : 2 et type oral / écrit Oral et Ecrit

ACQUIS DE LA FORMATION ATTENDUS, ET QUI SONT EVALUES (5 à 10 items)

A l'issue de cet enseignement, l'élève est capable de :
VOLET I :

- Intégrer des mécanismes de sécurité dans les architectures IoT : Smart City – Smart Building – Smart Industrie
- Concevoir et mettre en œuvre des infrastructures de sécurité
- Communiquer avec des experts en sécurité dans les projets IoT

VOLET II

- Intégrer en amont dans les projets IoT, les enjeux de la sécurité grâce à une analyse de risque
- Mener une analyse de risques avec la méthode EBIOS d'un système d'information
- Définir et mettre en place un plan d'actions en sécurité des systèmes d'information
- Identifier les aspects réglementaires liés aux traitements de données à caractère personnel dans les projets IoT

PREREQUIS (pas plus de 5 lignes):
Avoir suivi le Volet opérationnel de la sécurité IoT avant le volet Management

REFERENCES, BIBLIOGRAPHIE (pas plus de 5 lignes) :
XXXXXXX