FC9CS07 2 470 € 3 jour(s)

[Formation] Sécurité des objets connectés et de l'internet des objets (IoT)

OBJECTIFS

- Identifier les risques liés à la sécurité des applications dans le monde de la mobilité et de l'internet des objets (IoT)
- Mettre en œuvre les technologies nécessaires à la protection des données, des applications en environnement mobile et des objets connectés

PROGRAMME

Introduction

Sécurité opérationnelle des objets connectés

- Historique et exemples d'attaques sur les objets connectés
- Problématique de confiance à distance
- Risques, menaces, vulnérabilités
- Évolution des modes d'attaques
- Organigramme typique d'une attaque
- Analyse d'un DDos – exemple MIRAI
- Observation des menaces : écosystème IoT, NFC, BLE
- Premiers conseils pratiques

Standards et modèles d'architectures

- Architecture, nommage, routage, piles protocolaires (6LoWPAN, 802.15.4, etc.)
- Architecture fonctionnelle et solutions IoT
- Standardisation réseaux, alliances industrielles
- Fonctionnalités et technologies IoT
- Domaines d'application des services
- Définition et mise en place d'une stratégie de sécurité associées aux projets IoT
- IoT et politiques de sécurité en entreprise

RGPD et autres règlementations

Protocoles de communication de l'internet

ATELIER AVANCÉ

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Cette formation s'adresse plus particulièrement aux personnes souhaitant comprendre la problématique de la sécurité des objets connectés et des applications associées et souhaitant acquérir les bases techniques pour la protection des données et la mise en place de solutions de sécurité adaptées.

Une connaissance des principes de base de la sécurité, de l'Internet et des applications mobiles sont souhaitables afin de tirer pleinement profit de la formation.

COORDINATEURS

Xavier AGHINA

Responsable de la Sécurité des Systèmes d'Information (RSSI) chez W-HA, avec l'objectif de garantir la sécurité, la disponibilité et l'intégrité du système d'information et des données. Il a développé une expertise en cybersécurité, par la conduite des projets techniques et un programme de recherche sur le paiement mobile et la protection des objets connectés.

MODALITES PEDAGOGIQUES

Des exemples illustrent les concepts théoriques.

des objets (IoT)

- Architectures d'accès IoT
- Protocoles de sécurité
- Exemple d'architectures sécurisées
- Sécurité des protocoles adaptés aux objets connectés (BLE, Zigbee, NFC, Z-Wave, etc.)
- Sécurité des réseaux longue portée (LoRa, Sigfox, LTE, etc.)
- Management de la sécurité
- Écosystème et généralités
- Sécurité du service dans l'IoT : cas d'usage
- Sécurité réseau dans l'IoT
- Sécurité des objets connectés
- Standards (IEEE, OneM2M, GSMA, etc.)

Cryptographie, protection des données en environnement IoT

- Rappels de cryptographie en contexte M2M (Machine to Machine) et internet des objets (IoT)
- Authentification des équipements connectés
- Chiffrement et intégrité des données collectées, stockées et transmises

Synthèse et conclusion