Programme de cours
IOT - Sécurité des objets connectés

Durée :	3 jours soit 21 heures	Référence :	IF-SECIOT

Public visé :

- Le profil type ciblé est un industriel (développeur ou intégrateur)

Pré-requis :

- Avoir une bonne connaissance générale en environnement linux nécessaire, ainsi que des notions en système.

Objectifs pédagogiques :

- Fournir suffisamment d'éléments techniques et de langage afin de permettre aux développeurs et aux intégrateurs de solutions communicantes de comprendre l'aspect multi vectoriel de la sécurité des systèmes embarqués avec notamment une approche de défense vis à vis d'une vision attaquante.
- Être en mesure d'évaluer une solution IoT en prenant en compte l'ensemble de la chaine de données, depuis sa production jusqu'à sa consommation. Sur l'ensemble de la formation, le profil type attaquant est un attaquant opportuniste.

Compétences acquises à l'issue de la formation :

- comprendre l'aspect multi vectoriel de la sécurité des systèmes embarqués avec notamment une approche de défense vis à vis d'une vision attaquante.
- Être en mesure d'évaluer une solution IoT en prenant en compte l'ensemble de la chaine de données, depuis sa production jusqu'à sa consommation. Sur l'ensemble de la formation, le profil type attaquant est un attaquant opportuniste.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Description / Contenu

Module 1 : Qu'est-ce que l'Iot ?

- Au cœur de la révolution industrielle et sociétale
- L'environnement IoT
- Cadre légal
- Analyse de risque
- Référentiels (ANSSI / GSMA / GIE / norme ISO / Internationale / NIST / CIS)
- Méthodologie test d'intrusion
- MITRE ATT&CK ICS
- PTES
- OSTMM
- OWASP

Module 2 : Caractéristiques spécifiques

- Contraintes spécifiques / contraintes d'encombrement
- Microcontrôleur vs CPU
- Notion d'architecture
- Système temps-réel
- Protocoles
- Attaque

Module 3 : Récupération d'information

- Lecture de documentation technique (ex. : DataSheet et cartographie)
- Suivi des pistes physiques (ex.: Gerber)
- Voyage dans le temps (ex. : Gitlog / timemachine)
- Fiches d'identité

Module 4 : Couche matérielle

- Liaison série (Synchrone et Asynchrone)
- Accès au microcode (port débogage / lecture mémoire)
- Accès indirect / Injection de fautes (DMA/DPA)
- Introduction aux radio fréquences (SDR)

Module 5 : Couche microcode

- Rétro-ingénierie ARM (ex. : R2 et Ghidra)
- Exploitation ARM (Emulateur, Debogueur, Montage des partitions de fichiers)
- Développement sécurisé
- Simulation d'une carte “alpha” (version de développement)

Module 6 : Couche concentrateurs

- Passerelles
- Modèle souscription/publication
- Modèle ad-hoc
- Gestion par événements
- Android
- Architecture
- Décompilation d'une archive applicative (APK)
- Interaction avec la pile d'exécution
- Analyse légale post-incident (Forensic)

Module 7 : Couche Internet

- Terminaison API / fonctions lambda
- Application Web
- Gestion des réseaux d'énergie / villes intelligentes

Module 8 : Défense

- Protection du matériel
- Développement sécurité par construction (Secure design)
- Sécurité périmétrique et surveillance (Parefeu, IDS/IPS, Gestion de journaux VS SIEM)