La sécurité des objets connectés (IoT)

DOMAINE : *Hacking étique*
CATEGORIE : *IoT*

MISE A JOUR LE 13/01/2025

Descriptif

De nos jours, on trouve les **objets connectés** (IoT) absolument partout. Que ce soit dans nos maisons, en entreprise (IIoT) ou même sur nous, les objets connectés occupent une place de plus en plus **importante** dans notre **quotidien**.

Les **hackeurs** ont compris notre dépendance croissante envers ce type de dispositif et n'ont pas tardé à élaborer toutes sortes d'**attaques** sur ces objets. Par conséquent, nous sommes tous **vulnérables**.

Cette formation offre un panorama complet des **menaces** et des **vulnérabilités** associées aux objets connectés (inclue les objets connectés industriels IIoT) et aux applications mobiles. Elle vise à préserver la **sécurité** des accès, l'intégrité des **applications** et des données, et à apporter des solutions concrètes pour se **prémunir** contre les **cyberattaques**.

Informations

Référence	**CY-HE-SIOT**

Publics concernés

Ingénieur en sécurité, développeur IoT, chercheure en sécurité

Formateur

Expert certifié en cybersécurité

Prérequis

Avoir les connaissances de bases en réseau et en programmation

Certification préparée

Aucune

Objectifs

- **Identifier** les **risques** liés à la sécurité des applications dans le monde des **IoT**.
- Mettre en œuvre les **technologies** nécessaires à la **protection** des données et des applications au sein des **équipement IoT**.
- Comprendre les principales **menaces** et typologies d'attaques sur les dispositifs **IoT**.
- Apprendre les bonnes pratiques de **sécurisation** des communications et des **équipements IoT**.

Type de session

Intra-entreprise, **inter-entreprise** (en présentiel ou à distance)

Durée	4 jours (28 heures)
Date	À la demande
Tarif	1.650 € H.T
Effectif	12 participants max
Niveau	**Intermédiaire**
Délai d'accès	**3 semaines**

Programme

1) Introduction à la sécurité des IoT

- L'environnement des IoT
- Les enjeux de la cybersécurité des IoT
- Modélisation des menaces
- Les attaques les plus courantes
- Les outils mis en œuvre
- Cadre légal et éthique

2) Sécurité des réseaux

- Les protocoles spécifiques des IoT (Zigbee, 5G, LORA)
- La sécurité des couches applicatives
- Étude de vulnérabilités et contre-mesures
- Test d'intrusion et sécurisation d'un broker MQTT

3) Le hacking des applications

- Méthodologie et exploitation des vulnérabilités
- Extraction et analyse de données
- Décompilation de binaire
- Analyse des interactions avec les périphériques
- Test d'intrusion sur un Firmware vulnérable
- Les contre-mesures (obfuscation, Secure boot)

4) Le hacking hardware

- Outillage et précaution d'usage
- Reconnaissance et analyse des circuits
- Exploitation de l'UART JTAG et SWD
- Hacking des Firmware

5) Radio hacking

- Introduction des communications radio
- Identification des vulnérabilités
- Techniques d'interception des données et analyse
- Techniques d'attaques par injection, brouillage et replay
- Les contre-mesures (authentification et chiffrement des communications)

6) Mise en situation réelle

- Présentation du laboratoire virtuel
- Hacking d'une Smart Home
- Analyse légale après incident (Forensique)
- Implémentation de sécurité

Ce programme peut être adapté pour des sessions plus courtes, plus longues ou selon des besoins spécifiques

Modalités pédagogiques

Nous mettons en œuvre des modalités pédagogiques **variées** afin de maintenir l'attention des participants. Cette formation s'appuiera sur :

- Une alternance théorie (35%) et pratique (65%).
- Des mises en situation réelle, études de cas et échanges de pratiques.
- Des mises à disposition d'outils numériques interactifs, collaboratifs et participatifs.

À la fin de la formation, toutes les ressources pédagogiques seront **mises à disposition** pour tous les participants via leur espace dédié.

Modalités d'évaluation et de suivi

Les acquis de l'action de formation sont **évalués** à partir des productions des participants lors des études de cas et à partir de quiz et exercices réguliers.

Un questionnaire **d'autoévaluation** au regard des objectifs de la formation vous sera transmis avant le début de la formation et à la fin de celle-ci, vous permettant ainsi de mesurer votre progression en fin de formation.

Information sur l'accessibilité

Nous remercions les personnes qui auraient des **besoins spécifiques** de nous le signaler dès leur inscription. Quel que soit le type de handicap, nous pouvons adapter certaines de nos modalités de formation en étudiant ensemble vos besoins. Pour toutes questions, merci de contacter notre **référent handicap** :

- Par mail à handicap@ghdeformation.fr
- Ou par téléphone au +33 06 78 84 71 24