

# Comment protéger vos produits connectés ?

Comprendre les attaques et appliquer les contre-mesures appropriées, du capteur jusqu'au cloud



3 jours



4 - 8 personnes



Valence

## Présentation

Apprenez à mettre en œuvre les contre-mesures liées à la sécurité des produits connectés et à vous assurer que leurs fonctions et données sont protégées. Vous découvrirez comment appliquer les principes de sécurité et de protection des données à chaque étape de la conception et de la mise en œuvre de projets connectés, de la sélection des composants à la validation des mises à jour logicielles.

Au terme de la formation, vous serez en mesure de comprendre les principales attaques à destination des appareils connectés et leurs conséquences éventuelles en vous basant sur une démarche éprouvée et sa mise en œuvre.



## Objectifs

- Comprendre les enjeux et impacts que peut avoir une cyberattaque sur un produit connecté
- Pratiquer les cyberattaques pour permettre de mieux s'appropriier le sujet
- Savoir identifier et mettre en œuvre les contre-mesures adaptées

## Public

Personnel ayant le besoin de mieux connaître les mécanismes d'intrusion sur les produits connectés, par la mise en œuvre des cyberattaques et de leurs contre-mesures appropriées.

## LES PLUS

- ✓ Prise en compte des bonnes pratiques et réglementations de cybersécurité les plus récentes
- ✓ Mise en œuvre d'une démarche de sécurisation d'un produit connecté représentatif
- ✓ + de 50% de la formation consacrée aux ateliers pratiques

# LE PROGRAMME

## JOUR 1

### Introduction sur la cybersécurité des dispositifs connectés

- Etude de cas basée sur des cyberattaques réelles
- Vulnérabilités particulières aux dispositifs connectés
- Détermination du périmètre de cybersécurité

### Atelier pratique : mise en œuvre détaillée d'une démarche de sécurisation d'un produit connecté

- Modélisation du produit sous test
- Modélisation de menaces (dont la méthode STRIDE et l'outil MS Threat Modelling Tool)
- Analyse de risque EBIOS
- Exigences normatives
- Identification et application d'un référentiel de sécurité approprié

## JOUR 2

### Cryptologie

- Méthodes et approches cryptologiques
- Identification des moyens cryptologiques à mettre en œuvre en fonction du cas d'usage du produit connecté

### Atelier pratique : Comment sécuriser physiquement le système connecté ?

- Mise en œuvre d'attaques physiques
  - Attaques sur canaux I2C, SPI, UART, JTAG, pour lecture mémoire, fuzzing, extraction de firmware, reverse engineering, etc.
- Identification et application des contre-mesures associées

## JOUR 3

### Comment se prémunir des attaques de haute expertise ?

- Analyse de risque
- Attaques en faute
- Attaques par canaux cachés

### Atelier pratique : Comment sécuriser les canaux radios ?

- Mise en œuvre d'attaques sans-fil
- Compromission de réseau wifi WPA2
- Attaque de l'Homme du milieu sur communication Bluetooth Low Energy (BLE)
- Identification et application des contre-mesures associées



En partenariat avec

**CCI Formation**



**CONTACT**



**Elodie Ferrier**

Conseillère formation

Tél : 04 75 75 87 72

e.ferrier@drome.cci.fr

www.esynov.fr