esynov
by Grenoble INP - Esisar, UGA

CCI Formation
CCI DRÔME

Cybersécurité des dispositifs connectés

Prévenir les risques et anticiper les obligations normatives européennes

2 jours | 4 - 8 personnes | Valence

Présentation

Apprenez à identifier et à gérer les risques liés à la sécurité des appareils 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 et d'expliquer les principales obligations normatives applicables à la cybersécurité et à la protection des appareils connectés, afin de garantir leur conformité aux exigences européennes requises pour leur mise en vente sur le marché européen au 1er août 2024.

Objectifs

- Comprendre les risques liés à la cybersécurité des dispositifs connectés et leurs conséquences pour les entreprises et les consommateurs
- Apprendre comment mener une analyse et une évaluation des risques liés à la cybersécurité d'un dispositif connecté
- Comprendre les exigences normatives de cybersécurité pour la mise en vente d'un produit sur le marché européen
- Mettre en place des mécanismes de sécurité pour protéger les dispositifs connectés

Public

Personnel ayant le besoin de mieux connaître les obligations normatives de cybersécurité pour les dispositifs connectés et leur application à un produit.

LES PLUS

- Prise en compte des bonnes pratiques et réglementations de cybersécurité les plus récentes
- Couverture de l'ensemble des domaines d'un produit connecté : Système embarqué, réseaux sans fil, mobile, Cloud

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

Comprendre les nouvelles normes

- Introduction aux normes de cybersécurité
- Cadre européen (CyberSecurity Act)
- Référentiel ETSI EN303645
- Référentiel Industriel IEC62443-4-2
- Directive RED & Cyber Resilience Act, se préparer pour 2024

Comment mener une analyse de sécurité d'un dispositif connecté ?

- Application d'une démarche de sécurisation complète d'un dispositif connecté
- Prise en main des méthodes et outils de modélisation de menaces
- Détermination de la surface d'attaque
- Analyse de risque
- Contre-mesures et remédiations

JOUR 2

Comment sécuriser les communications radios ?

- Etude des attaques sans-fil : brouillage, usurpation, Man-in-the-Middle
- Application sur les canaux les plus répandus : Wifi, Bluetooth Low Energy (BLE)
- Méthodes de sécurisation et contre-mesures

Comment sécuriser physiquement le dispositif connecté ?

- Etude des attaques physiques : Lecture mémoire, fuzzing, extraction de firmware, reverse engineering, fuite de secret
- Etude sur les canaux les plus répandus : JTAG, SPI, UART, I2C
- Méthodes de sécurisation et contre-mesures

Comment sécuriser les communications avec une application mobile ou un service Cloud ?

- Etude de la sécurité des interfaces mobiles
- Etude de la sécurité des interfaces Cloud
- Méthodes de sécurisation et contre-mesures

En partenariat avec

CCI Formation

CCI DRÔME

CONTACT

Elodie Ferrier
Conseillère formation
Tél : 04 75 75 87 72
e.ferrier@drome.cci.fr