FONDAMENTAUX
NIVEAU 1
NIVEAU 2

NEW

LES FORMATIONS INDISPENSABLES TOUT AU LONG DE LA VIE

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS
MODULE 2 : APPROFONDISSEMENTS ET TECHNIQUES AVANCÉES

PUBLIC ET PRÉ-REQUIS :

- **Public cible** : ingénieurs, techniciens, chefs de projet, responsables sécurité, ou toute personne impliquée dans le développement ou l'évaluation des systèmes embarqués.
- **Prérequis** : avoir suivi le Module 1 (les fondamentaux) ou disposer de connaissances solides en cybersécurité et systèmes embarqués. Connaissances en programmation C, C++, ou ASM recommandées. Connaissances souhaitées des environnements Linux.

DURÉE DE LA FORMATION
3 jours (21 heures)
avec alternances
théorie/pratique

LIEU
En présentiel à
Saint-Quentin-en- Yvelines
(78)

PRIX
2 250 €
Modules 1 et 2 : 4 410 €

DATES
16, 17, 18 juin 2025
et 7, 8, 9 juillet 2025

INTERVENANTS

Jean-Pierre BRUANDET
Consultant et formateur
expert en cybersécurité
des systèmes embarqués et
en gouvernance cyber.

OBJECTIFS PÉDAGOGIQUES

- Approfondir les concepts avancés de cybersécurité des systèmes embarqués
- Expérimenter les techniques d'exploitation de vulnérabilités
- Implémenter les bonnes pratiques de sécurisation
- Utiliser et appliquer les référentiels de bonnes pratiques
- Évaluer et renforcer la sécurité des systèmes embarqués

PROGRAMME

Sécurisation de la couche logicielle

Objectifs : maîtriser les faiblesses logicielles et les techniques de sécurisation du code et des applications.
- Introduction : vulnérabilités courantes, sécurisation de la supply chain logicielle
- Sécurisation des binaires
- Sécurisation de la mémoire
- Gestion des types et des exceptions
- Gestion des dépendances et des bibliothèques
- Protection de la propriété intellectuelle (PI) et furtivité
- Mise en place et gestion d'une PKI

Sécurisation de la couche matérielle

Objectifs : comprendre les menaces et protections spécifiques au matériel et intégrer la sécurité dès la conception.
- Security by Design et intégration sécurisée
- Reconnaissance matérielle
- Attaques par injection
- Exploitation des canaux auxiliaires
- Sécurisation de la supply chain matérielle
- TPM (Trusted Platform Module) et HSM (Hardware Security Module

MOYENS PÉDAGOGIQUES

- Supports de cours détaillés,
- Environnements de tests pour l'expérimentation et les démonstrations des techniques d'exploitation et de protection,
- Analyse d'études de cas réels,
- Documentation technique sur les référentiels et standards de sécurité.

SUIVI ET ÉVALUATION

- **Suivi** : évaluation continue à travers des exercices pratiques et des études de cas.