Formation **Cybersécurité des systèmes embarqués**

Acquérir une maîtrise complète sur la sécurisation des systèmes embarqués

Plongez au cœur de la cybersécurité des systèmes embarqués avec notre formation conçue pour les professionnels aspirant à maîtriser les défis de sécurisation dans un monde connecté. De la compréhension des menaces à l'application de stratégies de défense avancées, en passant par la cryptographie et le développement sécurisé, ce programme intensif vous outille avec les compétences clés pour protéger vos systèmes contre les vulnérabilités. Transformez les risques en opportunités et devenez un acteur clé de la sécurité informatique dans votre organisation ! Cette formation peut être adaptée à des profils non-techniques, contactez-nous pour nous détailler votre besoin.

Durée

3 jours

Objectifs pédagogiques

- Identifier et analyser les menaces et vulnérabilités des systèmes embarqués
- Implémenter des techniques cryptographiques pour la protection des données
- Développer des systèmes embarqués sécurisés suivant une approche Secure by Design
- Utiliser des outils de rétro-ingénierie pour évaluer la sécurité des systèmes

Public

Développeurs, architectes, RSSI...

Prérequis

Une expérience dans le développement de systèmes embarqués.

96 Boulevard Vivier Merle +33 (0)4 78 22 10 38
F-69423 LYON Cedex 03 demande@sparks-formation.com www.sparks-formation.com

Sparks - Société par Actions Simplifiées au capital de 50 000 euros I Siret 48528157000039 I APE 8559A I N° de déclaration d'activité 82 69 09848 69

Programme de formation

Introduction à la formation Cybersécurité des systèmes embarqués
Vue d'ensemble des vulnérabilités courantes et impératifs de sécurisation : protection réseau, sécurité physique, et propriété intellectuelle.
Analyse des différences en termes de sécurité entre MCU et MPU.
Examen des obstacles techniques et opérationnels à la sécurisation.

Catégorisation et analyse des attaques
Exploration de vulnérabilités connues, outils de rétro-ingénierie matérielle et logicielle.
Méthodologies d'analyse passive et active, techniques d'exploitation : RF, réseau, logicielles, attaques physiques.
Exemple d'activités pratiques : sécurisation de la clé Wookey.

Élaboration de stratégies défensives
Aperçu des principales régulations et normes de sécurité.
Définition des problèmes de sécurité, analyse des risques.
Exemple d'activités pratiques : création d'une cible de sécurité pour des applications spécifiques.

Principes de cryptographie
Techniques et algorithmes de cryptographie symétrique et asymétrique : AES, RSA, ECDSA.
Utilisation des algorithmes de hachage et de MAC, gestion et diversification des clés.

Secure by Design ARM
Sécurité intégrée dès le cycle de vie du produit, mécanismes de sécurité : attestation, démarrage sécurisé, mise à jour sécurisée.
Configuration d'un serveur écho sécurisé avec MbedTLS et Zephyr OS.
Exemple d'activités pratiques : établissement d'une connexion TLS.

Meilleures pratiques de développement sécurisé
Adoption de pratiques de développement sécurisé, utilisation de MCUboot pour la gestion de firmware.
Exemple d'activités pratiques : configuration de MCUboot.

Sécurité avancée avec ARM TrustZone
Sécurisation des applications avec les extensions TrustZone pour Cortex M, provisionnement des clés et services de sécurité intégrés.

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.