+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 19/01/2026

S'inscrire

Formation Secure by Design pour systèmes embarqués

2 jours (14 heures)

Présentation

Le concept de Secure by Design ne consiste pas seulement à respecter des normes, mais à intégrer la sécurité au cœur même du cycle de développement logiciel (SDLC). Pour les systèmes embarqués, souvent déployés pour des années sans possibilité de patch facile, la qualité du code est la première ligne de défense.

Notre formation "Développer Secure by Design" s'adresse aux ingénieurs qui conçoivent et codent les systèmes embarqués. Elle vise à transformer les pratiques de développement pour anticiper les menaces dès la phase de design et d'implémentation. Vous apprendrez à identifier les failles critiques en C/C++ (débordements de mémoire, race conditions), à appliquer les standards de codage sécurisé (CERT C, MISRA) et à utiliser les outils d'analyse statique et dynamique.

À l'issue de la formation, vous serez capable d'intégrer la sécurité dans vos pipelines CI/CD et de livrer un code robuste, conforme aux exigences du Cyber Resilience Act.

Objectifs

- Comprendre les principes du Secure SDLC (Cycle de développement sécurisé).
- Maîtriser les règles de codage sécurisé en C/C++.
- Savoir identifier et corriger les vulnérabilités classiques (Buffer Overflow, Integer Overflow).
- Mettre en œuvre des mécanismes de défense (Secure Boot, Chiffrement, TEE).
- Utiliser des outils d'audit de code (SAST) et de tests (Fuzzing).

Public visé

- Développeurs C/C++ embarqué
- Architectes logiciels

- Lead Developers / Tech Leads

Pré-requis

- Bonne maîtrise du langage C ou C++.
- Connaissance de l'environnement Linux ou RTOS est un plus.

Pré-requis techniques

- Machine virtuelle Linux fournie avec chaîne de compilation (GCC/Clang) et outils d'analyse (Cppcheck, Flawfinder, AFL++).

Formation Secure by Design pour systèmes embarqués

[Jour 1 - Matin]

Introduction et Secure SDLC

- Le paysage des menaces sur l'embarqué (Top 10 OWASP IoT/Embedded)
- Le coût de la dette technique de sécurité
- Intégrer la sécurité dans le cycle en V ou Agile (DevSecOps)
- Principes de conception : Moindre privilège, Défense en profondeur, Surface d'attaque réduite
- Atelier pratique : Analyse d'un code vulnérable (Bug Bounty simplifié) pour identifier les failles évidentes.

[Jour 1 - Après-midi]

Codage Sécurisé en C/C++

- Gestion de la mémoire : le cauchemar du C
- Comprendre et prévenir les Buffer Overflows (Stack & Heap)
- Les failles de format (Format String Vulnerabilities)
- Gestion sécurisée des entiers (Integer Overflows/Underflows)
- Les standards de codage : MISRA C et SEI CERT C
- Atelier pratique : Exploitation d'un Buffer Overflow et correction via code défensif.

[Jour 2 - Matin]

Architecture et Protection des Données

- Stockage sécurisé : ne jamais coder de clés en dur (Hardcoded credentials)
- Principes de cryptographie appliquée à l'embarqué (AES, ECC, Hashing)
- Mécanismes hardware : Secure Boot, TrustZone (TEE), TPM
- Sécurisation des communications (TLS, MQTT sécurisé)
- Atelier pratique : Implémentation d'un stockage chiffré de configuration sensible.

[Jour 2 - Après-midi]

Outillage et Validation (Testing)

- L'analyse statique de code (SAST) : Cppcheck, SonarQube, CodeQL
- L'analyse dynamique (DAST) et instrumentation (Valgrind, Sanitizers)
- Introduction au Fuzzing (AFL++) pour tester la robustesse
- Gestion des dépendances et SBOM (Software Bill of Materials)
- Atelier pratique : Mise en place d'un pipeline d'analyse automatique sur un projet Git.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.