C C++ Secure Coding

Objectifs :

- sensibiliser les développeurs sur la sécurité du code
- connaître le rôle des acteurs et la classification des risques
- connaître les bonnes pratiques à appliquer
- connaître les principes de chiffrement et d'authentification

Durée : 3 jours

Public : développeurs, chefs de projets

Prérequis :

- pratique du langage C++

Démarche pédagogique :

- présentation des concepts, démonstrations et ateliers

Programme détaillé :

- Introduction
  - les risques liés au développement
  - les traces laissés par les développeurs
    - mémoire, journaux, …
  - les attaques
  - les différents acteurs : CERT, PCI, CWE, OWASP, …
  - codage sécurisé d'une application
- Classification des risques CERT
  - domaine
    - integer, string, floating point, array, …
  - sévérité, priorité, ...
  - guidelines
- Coder de manière à sécuriser le code
  - structuration du code
  - les macros
  - environnement
  - déclarations et initialisations
  - es entiers, les réels...
  - gestion des chaînes de caractères
  - validation des entrées
  - gestion de la mémoire
  - les entrées - sorties
  - les privilèges et permissions
  - bonnes pratiques POO
  - gestions des traces :

        - journaux, état de la mémoire, logs, …
    - la revue de code
- Introduction au chiffrement
    - les nombres aléatoires
    - le chiffrement symétrique
    - le chiffrement asymétrique
    - réseau et SSL
    - authentification
        - codes Hash, échange de clés
    - infrastructure PKI
        - certificats, X.509