C C++ Secure Coding

Objectifs :

- sensibiliser les développeurs sur la sécurité du code
- connaître le fonctionnement de la pile
- savoir repérer les erreurs dans le code
- connaître le rôle des acteurs et la classification des risques : CERT, CWE, OWASP
- connaître les bonnes pratiques à appliquer

Durée : 1 journée

Public : développeurs, chefs de projets

Prérequis :

- pratique des langages C C++

Démarche pédagogique :

- présentation des concepts, démonstrations et ateliers
    - utilisation de POC (Proof of Concept) et discussion sur les corrections
    - mise en oeuvre des bonnes pratiques

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
    - domaines
        - integer, string, floating point, array, …
    - sévérité, priorité, ...
    - guidelines
- Les langages C et C++
    - modèle mémoire
    - compilation
    - comprendre les appels de fonction
        - structure de la pile
- Coder de manière à sécuriser le code
    - quelques exemples de code
    - les chaînes de caractères
    - les pointeurs
    - gestion de la mémoire

    - les entiers
    - les sorties formatées
    - les fichiers
- Les bonnes pratiques
    - bonnes pratiques de codage
        - macro et inline
        - gestion de la mémoire : new, free, gestion des erreurs
        - structure des classes
        - passer à C++14
            - généralités : nullptr, enum, deleted fonctions
            - utilisation des smart pointers
    - les standards de sécurité
    - vérification du code
- Conclusion