Programme de cours
C/C++ Secure coding

Durée :	2 jours soit 14 heures	Référence :	IF-C++SEC

Public visé :

Cette formation est destinée aux développeurs C/C++ et aux ingénieurs de développement C/C++.

Pré-requis :

Pour suivre cette formation les apprenants doivent :

- avoir pratiquer du C/C++
- avoir suivi la formation "C++ : Avancé"

Objectifs pédagogiques :

Adopter une culture du développement sécurisé
Connaître les vulnérabilités courantes en C/C++
Intégrer des techniques de protection mémoire
Implémenter du code préventif pour circonscrire les attaques
Restreindre la surface d'exposition du programme

Compétences acquises à l'issue de la formation :

- Adopter une culture du développement sécurisé
- Connaître les vulnérabilités courantes en C/C++
- Intégrer des techniques de protection mémoire
- Implémenter du code préventif pour circonscrire les attaques
- Restreindre la surface d'exposition du programme

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant
- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Description / Contenu

Module 1 : Vue d'ensemble

- Etat des lieux de la sécurité applicative
- Standards : PCI, OWASP, OWASP Mobile, CWE Top 25 et CERT
- Responsabilisation de l'équipe de développement
- Radiographie d'une application C/C++

Module 2 : Contournements

- Entiers, réels : Dépassements
- Pseudo-aléatoire / Cryptosafe
- Chaînes : Injections, PFS, DTV
- Ressources et secrets
- Séquences et accès : Race conditions, TOCTOU, ...

Module 3 : Corruption mémoire

- Cartographie de la mémoire d'un programme C/C++
- Structure de la pile et conventions d'appel
- Hors limites : pointeurs, indices
- Débordements (Overflows)

Module 4 : Bonnes pratiques

- Validation des entrées : format, nettoyage, checksum
- Gestion de la complexité de l'unicode
- Prévention des injections : SQL, Commandes, ...
- Traitement des exceptions et erreurs
- Impact sur les tests

Module 5 : Protections

- Types sécurisés : strings, smart pointers, ...
- Hachages et chiffrements
- Zones non exécutable : NX
- Protection de la pile : SSP
- Adressage aléatoire : ASLR