Formation Cybersécurité

Durée : 3 jours

Date : Sur demande

Type : Inter et Intra-entreprise

Niveau : Confirmé en informatique

Support de cours : Français (Anglais disponible sur demande préalable)

Lieu : Dans nos agences ou sur site

Attestation : en fin de stage

Nos engagements

- ✓ Des interventions personnalisées
- ✓ Une offre améliorée selon nos retours d'expériences et notre veille technologique du marché
- ✓ Des intervenants issus de l'ingénierie ayant une expérience opérationnelle éprouvée
- ✓ Une formation orientée sur la pratique
- ✓ Plus de 30 ans dans l'ingénierie et le conseil en logiciel technique, industriel et électronique

Plus d'informations

conseil_formation@medianesysteme.com

Description

Devenez opérationnel et concevez des produits industriels répondants à vos contraintes de cybersécurité. Cette formation vous permettra d'acquérir les bonnes pratiques de cybersécurité à adopter face au contexte actuel et de développer votre esprit d'analyse.

Participants / Prérequis

Développeur, chef de projet ou architecte logiciel disposant d'un niveau intermédiaire dans un langage de programmation.

Objectif pédagogiques de la formation

Le cursus a pour objectifs d'apprendre aux participants :

- ✓ Les pratiques usuelles de cybersécurité et le contexte actuel associé (méthodologie, contexte normatif et réglementaire, …).
- ✓ Les bonnes pratiques d'analyse, de conception et de développement dans le contexte des produits industriels.
- ✓ Les principales menaces et catégories d'attaques, ainsi que les parades ou précautions associées
- ✓ Les points communs et les différences entre les pratiques de Maintien en Condition de Sécurité (MCS) et celles de Maintien en Condition Opérationnelle (MCO).

Programme

Cybersécurité d'un système industriel - vue d'ensemble

Introduction à la cybersécurité
Les systèmes d'information industriels
Sensibilisation aux risques
Normes et cybersécurité
Appréhender les risques
Stratégie de sécurisation
Cycles de développement sécurisé
Vulnérabilités classiques des produits
Défense en profondeur & composants

Implémentation technique de la cybersécurité dans un logiciel embarqué

Rôle du hardware
Couches logicielles
Sensibilisation à la cryptographie
Gestion des communications
Stratégies et techniques de durcissement
Configuration de la génération
Tests et preuves
Déploiement et configuration sécurisés
Maintien en condition de sécurité

Boîte à outils

Guide *Les best-practices de la cybersécurité* offert aux participants en fin de cursus.