Cybersécurité des systèmes industriels

Identifier les points faibles pour renforcer le niveau de Cybersécurité

3 jours / 21 heures | **Valence** | **Ref : INDUS1**

PRÉSENTATION

L'avènement de l'industrie du futur, ou industrie 4.0, impose de nouveaux challenges en terme de connectivité, de communication et d'exposition sur des réseaux non sécurisés tel qu'internet. Les environnements critiques industriels offrent alors des vulnérabilités aux cyber-attaques. Si elles ne sont pas identifiées et corrigées, elles exposent les systèmes industriels à des impacts physiques, environnementaux et/ou financiers importants. Cette formation vise ainsi à sensibiliser les acteurs du monde industriel aux différentes menaces et vecteurs d'attaques qui pèsent sur leurs systèmes et aux besoins de cybersécurité qui en découlent.

Automate programmable

SCADA

Vulnérabilités

OBJECTIFS DE LA FORMATION

COMPRENDRE les enjeux liés à la Cybersécurité des systèmes industriels et les particularités de ce domaine
IDENTIFIER les vulnérabilités de ces systèmes et les points clés à examiner lors de leur conception
ACQUÉRIR la méthodologie pour renforcer le niveau de Cybersécurité des systèmes existants et les points clés pour concevoir de nouveaux systèmes
MAÎTRISER les outils d'analyse des risques applicables aux environnements industriels

PUBLIC VISÉ

Personnes en charge de la conception, du développement, de l'intégration ou de l'exploitation et de la maintenance de systèmes industriels (maîtrise d'ouvrage, maîtrise d'oeuvre, exploitants, etc.)

Personnes amenées à réaliser des audits ou à accompagner des clients dans leurs projets de renforcement de la Cybersécurité des systèmes industriels

PRÉREQUIS

Connaissance de base en réseau
Connaissance de base en système informatique ou en contrôle / commande

POUR ALLER PLUS LOIN..

Cybersécurité : Les fondamentaux [Ref : SECU1]
Cloud Computing : Les fondamentaux [Ref : CLOUD1]

LES + DE LA FORMATION

OUVERTURE
à deux publics : les automaticiens et les informaticiens

PRATIQUE
Formation basée sur des démonstrations et des travaux pratiques

RETOURS D'EXPÉRIENCES
d'experts en Cybersécurité des systèmes industriels

Programme

JOUR 1

JOUR 2

JOUR 3

Module automaticien

- Définition de la Cybersécurité et principaux concepts
- Enjeux
- Attaques classiques (MITM, spoofing, ingénierie sociale, déni de service, détournement de sessions, DDOS, APT, Vers)
- Grands principes pour déployer un projet cybersécurité (analyse de risque, DEP, PSSI, etc)
- Bonnes pratiques
- Panorama des normes et standards (2700X, certification de produits, etc.)
- Introduction à la cryptographie

Module informaticien

- Introduction au monde des systèmes industriels et à leurs spécificités
- Les différents types de systèmes industriels
- L'architecture, la composition et les langages d'un système industriel
- Les protocoles et l'héritage qu'ils portent
- Introduction à la sûreté de fonctionnement
- Panorama des normes et standards

Module principal

- Enjeux propres à la cybersécurité des systèmes industriels
- État des lieux et historique, contraintes liées au contexte d'emploi, conséquences en termes de vulnérabilités et faiblesses et conséquences liées à l'interconnexion avec les systèmes informatisés
- Dualité/différences entre la sûreté de fonctionnement et la cybersécurité
- Exemples d'incidents sur des installations industrielles et illustration des impacts
- Focus sur les vulnérabilités et les vecteurs d'attaques classiques sur des installations industrielles
- Panorama des normes et standards liés à la cybersécurité des systèmes industriels
- Les initiatives étatiques en France : la Loi de Programmation Militaire, le projet de cybersécurité des systèmes industriels
- Les recommandations (aussi bien techniques qu'organisationnelles) pour aller vers l'état de l'art : présentation des bonnes pratiques et de leurs objectifs ainsi que les moyens pour les mettre en œuvre

Illustrations pratiques

- Présentation sur systèmes cyber-physiques industriels
- Analyse des configurations
- Analyse des vulnérabilités
- Démonstrations d'attaques sur système cyber-physique réel, analyse des conséquences
- Sécurisation