

## Cybersécurité des systèmes Industriels (DI-CYBER)

### Présentation

30% Théorie, 70% Pratique

Cette Formation ne fait pas l'objet d'une évaluation formelle des acquis.

Elle permet à un public d'automaticiens d'acquérir les bases de la cybersécurité des systèmes industriels et d'en connaître les solutions de protections de bases.

La formation n'a pas vocation à faire des stagiaires des experts de ce domaine.

### Objectifs

A l'issue de la formation le stagiaire sera capable de :

- Identifier les failles et vulnérabilités courantes des SI industriels
- Proposer de mettre en place les principales mesures de protections des SI industriels
- Configurer les protections automatées
- Mettre en place un cloisonnement des réseaux
- Mettre en place un système de détection d'incidents

### Groupes cibles

Toute personne en charge de la conception, du développement, de l'intégration, de l'exploitation ou de la maintenance de systèmes industriels (maîtrise d'ouvrage, maîtrise d'œuvre, exploitants, intégrateurs, etc.).

### Programme / Contenu

Introduction à la cybersécurité (Pratique)

- Enjeux
- Besoins de sécurité (Disponibilité, Confidentialité, Intégrité,...)
- Définitions (Chiffrement, Signature, Hash,...)
- Les menaces
- Normes et standards
- Présentation du guide d'hygiène de l'ANSSI

Cybersécurité des systèmes industriels (Pratique)

- Le contexte des systèmes industriels
- Exemple d'incidents industriels cyber
- Vulnérabilités courantes
- Bonnes pratique et principales mesures
- Défense en profondeur (Cloisonnement des réseaux et détection d'incidents)

Mise en application des solutions (Pratique)

- Présentation d'un SI industriel et prise en main (Bancs de test)
- Identifications des vulnérabilités et chemins d'attaques possibles
- Réflexion sur les solutions à mettre en place

Application des protections automatées (Pratique)

- Présentation du S7-1500 qualifiée (Configuration évaluée, recommandations d'usage, Fonction de sécurité)
- Activation des protections S7-1500
- Activation des mots de passe utilisateurs
- Activation du mot de passe de l'afficheur
- Protection des blocs de programme
- Configuration des coupleurs S7-1500 et S7-300

Cloisonnement des réseaux (Pratique)

- Présentation du XM-400 certifiée
- Configuration du XM-400
- Routage inter-vlan
- Mise en place des ACL
- Mise en place du filtrage MAC
- Configuration d'un S615
- Filtrage réseaux
- VPN

Détection d'incidents (Pratique)

- Présentation des SIEM
- Présentation d'ELK
- Configuration de la remontées d'informations
- Observation de la remonté d'information

Pour aller plus loin (Théorie)

- DMZ
- Station de décontamination
- Sondes de détection d'incidents

- Bastion

---

**Prérequis**

---

Un minimum de compétence en terme d'automatisme et d'administration réseaux.

---

**Remarque**

---

N° d'existence du centre de formation SITRAIN : 11 93 00 205 93

Compétences formateur :

- Réalisée par des experts assurant au quotidien des missions techniques auprès des entreprises, formés et qualifiés à la pédagogie des adultes avec un suivi et une actualisation de leurs compétences théoriques, pratiques, et pédagogiques.

Remarques complémentaires :

- -

Matériel Pédagogique (à titre indicatif) :

Réseau pour le groupe constitué de :

- console de programmation
- API S7-300 et S7-1500
- Switch manageable Scalance X300

---

**Type**

---

Formation en salle

---

**Durée**

---

3 Jours

---

**Langue**

---

fr

---

**Prix**

---

2 260 EUR

Prix en EURO HT par personne (repas compris)