Réseaux

Cybersécurité Industrielle

IDENTIFICATION

CODE : TC-5-S1-EC-CSI
ECTS : 2.0

HORAIRES

Cours : 32.0 h
TD : 0.0 h
TP : 0.0 h
Projet : 0.0 h
Face à face
pédagogique : 32.0 h
Travail personnel : 0.0 h
Total : 32.0 h

ÉVALUATION

SUPPORTS PÉDAGOGIQUES

LANGUE D'ENSEIGNEMENT

Français

CONTACT

M. BECHKIT Walid
walid.bechkit@insa-lyon.fr
Tel. : 0472438069

OBJECTIFS RECHERCHÉS PAR CET ENSEIGNEMENT

L'objectif de cette session pédagogique est d'explorer les concepts de cybersécurité dans le contexte de l'industrie. Les participants auront l'opportunité d'adopter à la fois la perspective d'une équipe d'attaquants (Red Team) et celle d'une équipe de défenseurs (Blue Team) afin de mieux appréhender les menaces qui ciblent les systèmes industriels, ainsi que les mesures de sécurité pouvant être mises en œuvre pour les contrer. Cette formation se basera sur des simulations d'attaques physiques et logiques au moyen d'une maquette virtualisée. De plus, des exemples de remédiation à la suite d'incidents seront également présentés pour une compréhension complète du processus de protection des systèmes industriels.

*** Cette session pédagogique est assurée par M. Alexis TASSE de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en collaboration avec M. Walid Bechkit de l'INSA de Lyon. ***

PROGRAMME

*** Module 1: Introduction aux systèmes industriels ***

- Contexte des systèmes industriels
- Le modèle de Purdue : une approche hiérarchique
- Les équipements industriels et leur fonctionnement
- Les protocoles de communication courants : Modbus, S7comm, OPC UA
- Introduction à l'IIOT (Industrial Internet of Things) et son impact sur les systèmes industriels

*** Module 2: Sécurité informatique des systèmes industriels ***

- Les menaces courantes : étude de cas de Stuxnet, Triton, Black Energy
- Méthodes de sécurisation des systèmes industriels
- Analyse des risques avec la méthode EBIOS RM
- Traitement des risques : mesures techniques et organisationnelles
- Mesures techniques :
 - Durcissement des systèmes d'exploitation
 - Segmentation réseau (VLAN, filtrage IP, filtrage applicatif)
 - Chiffrement des communications (IPSEC, TLS)
 - Détection des intrusions (utilisation de sondes comme suricata)
- Durcissement du matériel
- Sécurité physique périmétrique
- Mesures organisationnelles
- Évaluation des produits de sécurité
- Compréhension des certifications de sécurité
- Analyse d'une cible de sécurité

*** Module 3: Réponse aux incidents ***

- Compréhension de la chaîne d'attaque ICS (MITRE ATT&CK® Matrix for ICS)

PRÉ-REQUIS

Bases en Réseau (3TC-IP)

Bases en virtualisation légère (ex : Virtualbox)

INSA LYON

Campus LyonTech La Doua

20, avenue Albert Einstein - 69621 Villeurbanne cedex - France
Tel. +33 (0)4 72 43 83 83 - Fax +33 (0)4 72 43 85 00

www.insa-lyon.fr