

CYBERSÉCURITÉ DES CHAÎNES DE PRODUCTION

Cybersécurité industrielle (OT / SCADA / ICS) - Certificat IFALP



LIEUX DE FORMATION

L'IFALP - Institut Français des Achats et de la Logistique Publics
55, avenue du Président Wilson, 94230 CACHAN

EXECUTIVE EDUCATION

MODULE SPÉCIALISÉ – CYBERSÉCURITÉ INDUSTRIELLE (OT / ICS / SCADA)

OBJECTIFS

Les chaînes de production industrielles - automobile, énergie, agroalimentaire, pharmaceutique, défense - reposent sur des systèmes industriels (ICS, SCADA, automates, IoT industriel) longtemps isolés et désormais largement interconnectés. Cette convergence IT/OT crée une surface d'attaque inédite : Stuxnet, Triton, Industroyer, ransomwares ciblant les usines (Norsk Hydro, Honda, JBS) sont autant d'illustrations. Le programme forme les responsables industriels, RSSI/RSSI-OT, ingénieurs méthodes, automaticiens et acheteurs industriels à protéger leurs sites de production. Il couvre la cartographie des SI industriels, l'analyse de risques EBIOS RM appliquée à l'OT, la sécurisation des architectures (modèle Purdue, IEC 62443), la détection sur réseaux industriels et la conduite d'incidents.

PROGRAMME (PRÉVISIONNEL)

Le programme de formation est conçu selon une hybridation des meilleures pratiques en cybersécurité issues des secteurs public et privé. Les apprenants acquièrent une double compétence opérationnelle et stratégique.

	Fondamentaux	Mise en application industrielle
FONDAMENTAUX OT / IT	- Différences IT vs OT : contraintes, sûreté de fonctionnement - Architecture industrielle : modèle Purdue - Composants : automates (PLC), IHM, SCADA, DCS, historians	- Protocoles industriels : Modbus, OPC-UA, Profinet, EtherNet/IP - IoT industriel et Industrie 4.0 - Convergence IT/OT et impacts cyber
CADRE NORMATIF & RÉGLEMENTAIRE	- IEC 62443 (familles 2-1, 3-3, 4-2) - ANSSI : guide de cybersécurité des SI industriels - LPM / OIV / OSE et NIS2 industrielle	- ISO 27019, NIST CSF, NIST 800-82 - Sectoriels : ISA-99, NERC CIP (énergie), TS 50701 (ferroviaire) - Conformité et homologation des systèmes industriels
MENACES SUR LES CHAÎNES DE PRODUCTION	- Études de cas : Stuxnet, Triton, Industroyer, Colonial Pipeline - Ransomwares industriels : Norsk Hydro, Honda, JBS, Clorox - Compromission supply chain logicielle (SolarWinds, MOVEit)	- Sabotage, espionnage industriel, État-nations - Attaques sur l'IoT et les jumeaux numériques - Threat intelligence industrielle (Dragos, Claroty, Nozomi)
ANALYSE DE RISQUES & ARCHITECTURE	- EBIOS RM appliquée à un site industriel - Cartographie des actifs OT (passive scanning) - Zones et conduits (IEC 62443-3-2)	- Segmentation, DMZ industrielle, diodes, firewalls OT - Sécurisation des accès distants (mainteneurs, OEM) - Hardening des automates et postes IHM
DÉTECTION & RÉPONSE À INCIDENT INDUSTRIEL	- Sondes OT (Claroty, Nozomi, Dragos, Sentryo) - SOC industriel et corrélation IT/OT - Forensics sur automates et systèmes embarqués	- Plan de réponse à incident industriel - Continuité d'activité et reprise de production - Exercices de crise (war games OT)
ACHATS, FOURNISSEURS & SOUVERAINETÉ	- Clauses cyber dans les marchés industriels et MOE/MOA - Évaluation cyber des équipementiers et intégrateurs - Maintenance, télémaintenance, accès tiers	- Souveraineté : équipements et composants critiques - Sécurisation de la supply chain logicielle (SBOM) - Pilotage du cycle de vie des équipements OT

COMPÉTENCES CIBLÉES

- Cartographier un SI industriel (IT et OT)
- Conduire une analyse EBIOS RM sur site industriel
- Concevoir une architecture sécurisée IEC 62443
- Sécuriser les accès distants des mainteneurs
- Détecter les attaques sur réseaux OT
- Conduire la réponse à incident industriel
- Rédiger des clauses cyber dans les marchés industriels
- Piloter la conformité (LPM, NIS2, IEC 62443)



PROFILS CONCERNÉS

- RSSI, RSSI-OT, responsables cybersécurité industrielle
- Ingénieurs méthodes, automaticiens, responsables maintenance
- Directeurs d'usines, responsables d'opérations industrielles
- Acheteurs industriels, acheteurs publics OIV / OSE
- Consultants en cybersécurité industrielle et auditeurs

LES RESPONSABLES SCIENTIFIQUES DE L'IFALP



Irène FOGLIERINI
Responsable académique
Campus Cachan
Professeure Associée, Phd.
ifoglierini@gip-cei.com



Hind ABOUSSIKINE
Ingénieur, Phd, responsable
de la filière Cybersécurité
Industrielle, GIP CEI
haboussikine@gip-cei.com



Dr Thierry SAUVAGE
Directeur de recherche en Achats et Supply Chain,
PhD, HDR
tsauvage@gip-cei.com

VOTRE RESPONSABLE FORMATION



Sylvia DÉSIGNÉ
Responsable Formation
Continue
sdesigne@gip-cei.com

MEMBRES DU COMITÉ DE LABELLISATION

- Direction des Achats de l'Etat
- France Travail
- Conseil National des Achats
- Ministère de l'Intérieur
- Ministère des Armées
- Direction des Achats de l'APHP
- Département des Hauts-de-Seine

CONDITIONS D'ADMISSION ET PRÉREQUIS

Expérience professionnelle dans l'industrie, l'automatisme, la maintenance, la sécurité des SI ou les achats industriels.
Une connaissance des SI industriels (PLC, SCADA) est un plus.

CANDIDATURES

ADMISSION SUR DOSSIER ET ENTRETIENS

Dossier à compléter en ligne sur : www.gip-cei.com

Formation accessible aux personnes en situation de handicap, contacter le Pôle handicap du GIP CEI : handicap@gip-cei.com

MÉTHODES ET MOYENS MOBILISÉS

- Pédagogie centrée sur une approche participative et pragmatique
- Travaux pratiques en laboratoire de cybersécurité industrielle
- Études de cas réelles : Stuxnet, Norsk Hydro, Colonial Pipeline
- Wargame de réponse à incident industriel
- Corps professoral : enseignants académiques et experts cyber industriels

DATES IMPORTANTES

Ouverture des candidatures : toute l'année

Rentrée : janvier 2027

DURÉE

12 jours répartis sur une année (6 sessions de 2 jours).

COÛT

Le prix de la formation est de 7 000 €*.

- Plan de développement des compétences
- Plan de formation continue
- Financement personnel
- Compte Personnel de Formation (CPF)

** les membres du consortium sont invités à prendre contact avec l'IFALP*

Le GIP CEI / ESLI – ESTI a obtenu, le 12 juillet 2021, la certification du référentiel national de qualité Qualiopi.



La certification qualité a été délivrée au titre des catégories d'actions suivantes :
ACTIONS DE FORMATION
ACTIONS PERMETTANT DE VALIDER LES ACQUIS DE L'EXPÉRIENCE
ACTIONS DE FORMATION PAR APPRENTISSAGE

CONTACT POUR LA FORMATION CONTINUE

06 10 10 63 24
sdesignne@gip-cei.com



www.gip-cei.com