Cybersécurité des Systèmes Critiques – Quali-SIL - CYB

SIS - CYB

Quali-SIL INERIS

SÉCURITÉ & SÛRETÉ
QUALITÉ

Objectifs :

- Intégrer les exigences de cybersécurité dans le management et les étapes du cycle de vie des Systèmes Instrumentés de Sécurité.
- Savoir identifier et analyser les risques de cybersécurité pour concevoir et maintenir des systèmes résilients aux menaces afin de préserver la sécurité des installations industrielles critiques.
- Faire le lien avec tous les acteurs du cycle de vie et instaurer une démarche commune dans le domaine de la sécurité fonctionnelle.

Public :

Responsables projet et leaders techniques (automaticiens, info. Indus., HSE, sécurité des procédés, BE, intégrateurs de SIS, direction de service technique) ayant des responsabilités dans une des phases du cycle de vie de sécurité.
La formation est conçue pour les utilisateurs (propriétaires d'actifs) et intégrateurs.

Méthode Pédagogique :

- Un programme exclusivement focalisé sur la cybersécurité des systèmes critiques liés à la sécurité des installations industrielles, bâti sur le cycle de vie de la norme CEI 61511.
- Intégration des exigences réglementaires (ANSSI) et normatives (CEI 62443) dans le cycle de vie de la sécurité fonctionnelle (CEI 61508, CEI 61511)
- Des exercices de mise en pratique dans le prolongement de ceux des formations SIS-ING ou SIS-TECH (même procédé étudié sous l'angle cybersécurité).

Prérequis :

- Connaissances de base en cybersécurité ou avoir suivi le stage CYB – Cybersécurité des systèmes industriels – OT
- Connaissance en sécurité fonctionnelle ou avoir suivi le stage SIS-ING ou SIS-TECH. (Titulaire d'un certificat Quali-SIL ING ou CIM en cours de validité pour la certification Quali-SIL Cyb).

Programme :

CADRE ET VOCABULAIRE

- Rappels vocabulaire, définitions, notions fondamentales et spécificités des systèmes industriels de sécurité (IT/OT, CIA, Sécurité/Sûreté, …)
- Compréhension du cyberrisque (menaces, vulnérabilités, attaquants, propriétés CIA, …).
- Historique et actualités (dates clés, évolutions des menaces, CERTs, …)
- Besoins de cybersécurité des systèmes de contrôle-commande industriels dédié à la sécurité;

REGLEMENTATION, NORMES ET GUIDES DE REFERENCE

- Cadre réglementaire (LPM, directive NIS, arrêtés relatifs aux secteur d'activités d'importance vitale, ICPE et OIV, …).
- Normes et guides (CEI 61 511 et série CEI 61508, ISO/CEI série 27 000, CEI 62 443, NIST, ANSSI, …)
- Principes & concepts fondamentaux et lignes directrices (SMS, défense en profondeur, …).

APPRECIATION DES RISQUES DE CYBERSECURITE

- Principe du cycle de vie, inventaire et cartographie
- Evaluation initiale des risques de cybersécurité (High-Level Risk Assessment)
- Appréciation détaillée des risques de cybersécurité
- Critères d'évaluation des risques – Graphe des cyberrisques – probabilités d'attaque (menaces, attaquants, scénarios/vecteurs de menace et vulnérabilités)
- Architecture et segmentation, identification et exigences relatives aux zones et conduits – Détermination des SL-T, Identification des contre-mesures et facteur de réduction du risque.

SPECIFICATIONS DES EXIGENCES DE CYBERSECURITE (CSRS)

- Fonctions essentielles, architectures et indépendances, contremesures compensatoires, ...
- Spécifications des exigences fondamentales et SL-T, vecteur par zone et conduit
- Exigences de contrôle d'identification et d'authentification (IAC), de Contrôle d'utilisation (UC), d'intégrité du système (SI), de confidentialité des données (DC), de Flux de données réduit (RDF), de réponse en temps réel aux événements (TRE), de disponibilité des ressources (RA).

CONCEPTION ET MISE EN OEUVRE DE LA CYBERSECURITE

- Certification produits, Niveau de cyber capabilité (SL-C), SAV fournisseur.
- Design préliminaire, évaluation des contre-mesures et moyens alternatifs de réduction des risques.
- Analyse et comparaison des architectures possibles et bonnes pratiques
- Composants réseaux, conception détaillée, détails des zones et conduits, choix de protocoles de communication répondant aux exigences de sûreté et sécurité

INSTALLATION, MISE EN SERVICE ET VALIDATION

- Tests d'intégration, PEN tests. FAT et SAT de cybersécurité et liaison avec la sécurité fonctionnelle.
- Pre-Startup Review – Audit de configuration.

EXPLOITATION ET MAINTENANCE

- Gestion des accès : sécurité physique, accès et communications non autorisés.
- Gestion des essais (bypass, Proof Test). Détection et contrôle des intrusions (IDS, IPS).
- Evénement de menace (plans de réponse aux incidents et de remédiation, PCA/PCS)
- Evaluation et métrique de cybersécurité

INSPECTION – AUDIT – MOC – DECOMMISSIONING

- Veille sur les vulnérabilités (gestion des alertes, analyse des correctifs)
- Implémentation des mises à jour / correctifs - analyse d'impact sur l'intégrité (SIL) / requalification.
- Gestion de l'obsolescence (HW & SW plus supportés) et des mises au rebut

SYSTÈME DE MANAGEMENT DE LA CYBERSECURITE

- Politique, planification, organisation, programme de sécurité (62443-2-1)
- SMC (modèle de maturité, processus, évaluation, vérification, …)
- Sensibilisation et compétence du personnel
- Formation, compétence, responsabilité et indépendance.

Institut de Régulation et d'Automation

Durée
4jours / 25h

Horaires
mardi 9h00 - vendredi 12h00

Niveau d'acquis
Maitrise

Nature des connaissances
Perfectionnement des connaissances

Modalités d'évaluation
Quali-SIL Cyber ou FS-CYB

Certification
Quali-SIL Cyber

Participants
Mini : 2 - Maxi : 12

Responsable
Fabien CIUTAT

Dates, Prix & Certification

Consulter notre site internet : www.ira.eu

Formation disponible en INTRA à la demande.

Informations Complémentaires :

Formateur expert en Sécurité Fonctionnelle, Automatismes et réseaux industriels

Certification des compétences : Modalité : dossier + examen (QCM) durée 2 h. Certification de compétence QUALI-SIL-CYBER délivrée par INERIS (pour les personnes déjà certifiées Quali-SIL ING (voir stage SIS-ING) Certification valable 5 ans.*

Les repas sur Arles vous sont offerts.

*Dossier de candidature à remplir et à remettre avant l'entrée de stage

Travaux dirigés / Études de cas