Programme de la formation Cybersécurité des Systèmes Critiques - Préparation à la certification *Quali-SIL* CYBER

(4 Jours)

CADRE ET VOCABULAIRE

- Rappels vocabulaire, définitions, notions fondamentales et spécificités des systèmes industriels de sécurité (IT/OT, CIA, Sécurité/Sûreté…).
- Compréhension du cyber-risque (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 (SIS, SCS…).

REGLEMENTATION, NORMES ET GUIDES DE REFERENCE

- > Cadre réglementaire (LPM, directive NIS, arrêtés relatifs aux secteurs d'activités d'importance vitale, ICPE et OIV…).
- Normes et guides (IEC 61 511 et série IEC 61508, ISO/IEC série 27 000, IEC 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 cyber-risques – 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 contremesures et facteur de réduction du cyber-risque.

SPECIFICATIONS DES EXIGENCES DE CYBERSECURITE (CSRS)

- Fonctions essentielles, architectures et indépendances, contremesures compensatoires, moindre privilège.
- 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 (CSRS)

- Certification produits, Niveau de cyber capabilité (SL-C), SAV fournisseur.
- Design préliminaire, évaluation des contremesures 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 (Contournement, bypass, Proof Test).
- Détection et contrôle des intrusions (IDS, IPS).
- Evénement de menace (plans de réponse aux incidents et de remédiation, plan de continuité d'activité / continuité de la sécurité) Gestion des Alertes Cybersécurité.
- Evaluation et métrique de cybersécurité.

INSPECTION – AUDIT – MOC – DECOMMISSIONING

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

SYSTÈME DE MANAGEMENT DE LA CYBERSECURITE

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