Cybersécurité des installations Industrielles IEC 62443

Ref. ***CYB-10***
Durée : 5.0 jour(s) / 35.0 heures

La cybersécurité dans le monde industriel est un des enjeux majeurs de l'industrie 4.0.
La famille des normes 62443 permet d'appréhender les divers aspects liés à ce contexte.
Comprendre l'ensemble de ces normes est indispensable pour pouvoir mettre en place un système de management adéquate, apprécier les niveaux de maturité associés et adopter les mesures de sécurité adaptées aux risques évalués

Avertissement : La cinquieme journée est destinée au passage de la certification. (Inclus dans le tarif)

Le stagiaire peut suivre la formation sur 4 jours sans passer la certification

Pré-requis :

Connaissance du fonctionnement managérial et organisationnel d'une structure et connaissance de base en sécurité de l'information et des systèmes industriels.

Personnes concernées :

Responsable de projet sécurité industrielle
Architecte sécurité industrielle,
Concepteur produits pour industrie,
Ingénieur cyber sécurité,
Consultant sécurité
DSI.
RSSI.
Risk Manager

Objectifs :

Identifier les exigences et la structure des normes IEC62443
Dialoguer avec le vocabulaire adapté
Réaliser une évaluation de maturité des processus
Réaliser une évaluation de niveau des mesures de sécurité
Choisir les certifications adaptées à la stratégie de l'entreprise
Identifier les risques liés aux installations industrielles

Programme :

JOUR 1
Cybersécurité industrielle
- Panorama cybersécurité
- Les enjeux et contraintes
- Les principes de sécurité
- Vocabulaire
- Architecture et composants
- Les protocoles usuels
- L'écosystème
- Les typologies de menaces
- Les attaques courantes

- IT vs OT
- Pourquoi mettre en place un programme de cybersécurité industrielle
Exercices sur les attaques, quizz sur les notions théoriques essentielles et vocabulaire

62443 series: overview et préparation du CSMS
- Les concepts
- Les 7 exigences fondamentales (62433-1-1)
- SL, SL-A, SL-C SL-T
- Niveaux de maturités
- Les certifications
- Rôles et responsabilités
- Les actifs
- Les risques
- Les phases du CSMS
- Les politiques et procédures
- Les zones de sécurité
- Les conduits
- Les niveaux de sécurité
- Les modèles
- Ensemble d'exigences pour aborder le CSMS
Exercices à partir d'études de cas, réflexion et préparation du projet d'implémentation d'un CSMS

JOUR 2
Composition du CSMS
- Les éléments
- Gestion des risques
- Lien entre risques et CSMS
- Les catégories
- Les mesures
- Implémentation
- Surveillance et amélioration
- Réaliser une analyse de maturité des processus
- Réaliser une analyse du niveau de sécurité
Travaux Dirigés / Exercices : analyse des écarts

JOUR 3
62443 et les fournisseurs de services IACS
- 62443 2-4 overview
- Propriétaire vs fournisseur : différentes façons d'utiliser la norme
- Intégration des services
- Maintenance
- Overview des exigences
- Gestion de la maturité
Travaux Dirigés : Etude de cas

JOUR 4
Gestion des développements des produits sécurisés
- La défense en profondeur
- Management de la sécurité
- Exigences de sécurité : spécifications
- Secure by design
- Implémentation sécurisée
- Vérification et test de validation
- Gestion des écarts
- Mise à jour
- Pratiques de sécurité
- Niveaux de sécurité
- Évaluation du niveau de sécurité d'un produit
Exercices : à partir d'une étude de cas, réalisation d'une évaluation du niveau de sécurité et proposition d'amélioration.

JOUR 5
Préparation certification : Quizz global. Etude de cas
Examen final : Qcm sur la cybersécurité industrielle, vocabulaire,63443 ; Mise en situation sur analyse des écarts, développement, SL, étude de cas

Démarche pédagogique :

Exposés avec illustrations
Etudes de cas
Tables rondes et échanges

La formation est animée par un formateur disposant d'une qualification spécifique de formateur selon les procédures de qualification de Bureau Veritas justifiant d'une expérience terrain confirmée dans le domaine concerné.

Evaluation et validation :

EXAMEN : PASSAGE DE LA CERTIFICATION DE PERSONNES :

- Partie théorique et pratique
- Le temps destiné au passage de la certification est de 3H.
- L'examen est composé de 3 parties : QCM, mise en situation sur points spécifiques, mise en situation sur cas concrets.
- Il se déroule sur une plateforme à distance.

L'examen valide des domaines de compétences en relation avec les profils métiers identifiés par l'European union agency for cybersecurity via l'European Cybersecurity Skills Framework