Cybersécurité des systèmes industriels selon la norme IEC 62 443

Cybersécurité des systèmes industriels selon la norme IEC 62 443

Formation | 1 session disponible | Attestation de présence

Formation présentielle | 21 heures

Référence de la formation: FR-SysInd

Version: 21.11.2024. Vous trouverez toutes les informations actuelles sur https://academie-fr.tuv.com/s/FR-SysInd

Face aux cybermenaces croissantes des systèmes industriels, les entreprises sont aujourd'hui toutes concernées, quels que soient leur taille ou secteur d'activité. Les cyberattaques peuvent entrainer un malfonctionnement, voire un arrêt complet des installations industrielles, mais aussi entraver à la sécurité des biens et des personnes. La norme IEC 62443 définit un cadre pour la gestion des risques de cybersécurité des systèmes industriels.

Plongez dans la cybersécurité des systèmes industriels et la norme IEC 62443 à travers des ateliers interactifs, des démonstrations et le partage de connaissances de formateurs experts. Découvrez des stratégies de défense en profondeur et apprenez à évaluer les risques selon les directives de la norme IEC 62443. Équipez-vous des compétences nécessaires pour auditer, protéger et renforcer vos systèmes industriels.

Les objectifs

Cette formation est principalement destinée aux architectes de produits et systèmes.

Elle a pour objectif de :

- Reconnaître les enjeux, difficultés, limitations et défis liés à la cybersécurité,
- Identifier leur impact sur leur quotidien (responsabilités, activités, résultats…).

Le public ciblé

Amateurs et professionnels en électronique ou sécurité IT, intéressés par le design d'architecture dans le milieu industriel (développeur, architecte, intégrateur, concepteur hardware, chef de projet).

Les prérequis

Aucune expérience en sécurité informatique n'est requise. Cependant, des connaissances en systèmes industriels ainsi que quelques notions en informatique, électronique, logiciel embarqué sont souhaitables.

- Un PC / MAC avec l'outil Teams d'installé ainsi qu'un accès non restreint à internet.

Si en distanciel :

- Un accès internet stable via Ethernet ou Wi-Fi avec un débit correct (1.2 Mb/s en débit descendant minimum est recommandé).

Le contenu de la formation

Introduction et normes de sécurité

- Introduction avec des concepts clés et des différences entre les environnements IT et OT
- Panorama des menaces et analyse des risques liés à la cybersécurité industrielle
- Introduction à la norme IEC 62443 méthodologie et évaluation des risques
- Ateliers pratiques sur la définition d'un SuC (Système under consideration) et l'évaluation de risque selon la norme IEC 62443
- Concepts clés de la norme IEC 62443 (zones, conduits et méthodologies d'analyse de risque)
- Défense en profondeur et les différentes couches de sécurité (organisationnelle, physique, périmétrique)
- Démonstration : sécurité des systèmes d'accès, exemple avec la technologie Mifare

Sécurité réseau et cryptologie

- Sécurité des systèmes et les principes de base de sécurité réseau
- Démonstration d'une attaque par force brute sur un réseau WPA2
- Introduction à la cryptologie : présentation des concepts clés (chiffrement symétrique et asymétrique, hash, sel et poivre)
- Démonstration exploitation d'une faille sur des fichiers Python précompilés contenant des secrets

Sécurité des produits et architecture sécurisée

- Cycle de vie sécurisé des logiciels (SDLC) et les bonnes pratiques pour le développement de logiciels sécurisés
- Sécurité des hôtes et des applications:
- Démonstration des vulnérabilités affectant des ports USB mal protégés avec personnel non sensibilisé aux attaques provenant des dispositifs apparemment inoffensifs
- Démonstration d'une attaque par rejeu mettant en œuvre des exploits sur un tableau d'affichage
- Sécurité des données
- Ateliers pratiques sur l'évaluation détaillée des risques, estimation des risques et définition des niveaux de sécurité selon la norme IEC 62443
- Méthodes pour identifier et traiter les vulnérabilités
- Présentation des bonnes pratiques pour concevoir une architecture robuste et sécurisée

JOUR 1

Introduction

Cybersécurité dans le monde industriel

- Comprendre la cybersécurité dans le contexte industriel
- Menaces et méthodologies d'attaques
- Divergence et convergence IT / OT

Norme ISA/IEC 62443

- Comprendre les concepts de la norme
- Processus d'évaluation des risques
- Évaluation initiale des risques détaillés
- Acceptation et comparaison des risques

Ateliers

- WS1 – Définir le système considéré
- WS2 – Effectuer l'évaluation initiale des risques
- WS3 – Partitionnement des Zones et conduits

JOUR 2

Norme ISA/IEC 62443

- Processus d'évaluation détaillée des risques

Défense en profondeur

- Systèmes - Sécurité physique
- Systèmes – Sécurité périmétrique
- Systèmes - Sécurité interne des réseaux

Démonstration

- Cas classique de Mifare
- Attaque par Brute force WPA2 et usurpation ARP
- Crypto : Mauvaise implémentation du chiffrement

Cryptographie

- Symétrique et asymétrique
- Certificat et PKI (Infrastructure à clés publiques)
- Fonction de hachage avec “sel” et “poivre”

Ateliers

- WS4 – Évaluation des risques détaillée (1/2) – Scénarios de menaces

JOUR 3

Norme ISA/IEC 62443

- Cycle de vie du développement d’un produit sécurisé
- Exigences fondamentales

Défense en profondeur

- Produit – Sécurité de l’hôte
- Produit – Sécurité des applications
- Produit – Sécurité des données

Démonstration

- Rubber Ducky – Attaque USB
- Radiofréquence – Attaque par rejeu

Ateliers

- WS5 – Évaluation des risques détaillée (2/2) – Estimation des risques
- WS6 – Définition des niveaux de sécurité
- WS7 – Spécification des exigences de cybersécurité

Détails sur les vulnérabilités

- MCS, CVE & CVSS

Méthodes pédagogiques

- Alternance d'exposés théoriques, d'illustrations par des cas concrets, d'exercices individuels ou en groupes de travail et de jeux de rôle.

Modalités d'évaluation :

- Exercices individuels, en binôme, en groupe,
- Débriefing par les groupes,
- Débriefing par le formateur,
- Evaluation des compétences acquises via un questionnaire en fin de formation.

Informations importantes

Ce cours est proposé en partenariat avec SERMA Safety & Security.

Si vous êtes en situation de handicap, nous vous remercions de bien vouloir nous contacter avant de procéder à l'inscription en envoyant un mail à formation@fr.tuv.com. Nous mettrons tout en œuvre pour répondre à votre besoin de formation.

Aperçu des dates et réservation

Réservez dès maintenant la date de votre choix directement en ligne sur https://academie-fr.tuv.com/s/FR-SysInd et profitez de ces avantages :

- Processus de réservation rapide
- Compte client personnel
- Réservation simultanée pour plusieurs participant(e)s.

Vous pouvez également utiliser le formulaire de commande pour commander par e-mail.

Formulaire de commande Page 1/3

Je m'engage par ce document présent à m'inscrire à la formation suivante:

Cybersécurité des systèmes industriels selon la norme IEC 62 443

Référence de la formation: FR-SysInd

Veuillez sélectionner votre session:

☐ **10/12/2024 - 12/12/2024**, Vandœuvre-lès-Nancy | Référence de la session: FR-SysInd-SysInd - décembre 2024
2 700,00 € Prix HT 3 240,00 € Prix TTC

Vous trouverez toutes les informations complémentaires sur les dates sous https://academie-fr.tuv.com/s/FR-SysInd.

Veuillez nous envoyer **toutes les pages** du formulaire par e-mail pour commander le séminaire susmentionné.

E-mail:
formation@fr.tuv.com

Veuillez saisir vos données de commande sur la page suivante.

Formulaire de commande Page 2/3

☐ Je commande en tant que consommateur (client privé)

☐ Je commande en tant qu'entreprise / administration (client professionnel)

Adresse de facturation

Nous utilisons ces données pour la confirmation de commande et la facturation.

Nom de l'entreprise ou de l'administration: _____

Département (optionnel): _____

Rue et numéro: _____

Code postal: _____ Ville: _____

Votre numéro de commande interne: _____

Numéro de TVA (optionnel): _____

vous pouvez indiquer ici un numéro de commande interne (numéro SAP, etc.) défini par votre entreprise. Nous indiquerons ce numéro sur la facture.

Vos coordonnées

Nous utilisons ces données pour la confirmation de commande et la facturation.

Civilité: _____ Prénom: _____ Nom de famille: _____

Adresse e-mail: _____

Numéro de téléphone (optionnel): _____

Formulaire de commande Page 3/3

Informations sur les participants

☐ Je participerai moi-même au séminaire (coordonnées, comme indiqué ci-dessus).

☐ La personne suivante doit participer au séminaire:

A ne remplir que si vous ne participez pas vous-même, mais qu'une autre personne participe.

Civilité: Prénom: Nom de famille:

Adresse e-mail: Numéro de téléphone (optionnel):

Date de naissance (optionnel): Lieu de naissance (optionnel):

Méthode de paiement: Facture

Pour les consommateurs, les informations sur le droit de rétractation s'appliquent et sont disponibles sous les CGV ci-jointes.

☐ J'accepte par la présente les conditions générales de l'organisateur (https://academie-fr.tuv.com/conditions-generales-vente) décrites ci-après.

Lieu, date Signature

Veuillez nous envoyer **toutes les pages** du formulaire par e-mail pour commander le séminaire susmentionné.

E-mail:
formation@fr.tuv.com