SIEMENS

Keep it cyber secure with OT & IT security (WS-I-SEC)

Présentation

Les réseaux de production (OT) et les réseaux de bureaux (IT) sont de plus en plus connectés. Cette intégration offre de nombreux avantages : plus de données, des processus numérisés, une intervention plus rapide en cas d'immobilisation et une collaboration entre entreprises dans les écosystèmes. Un inconvénient de taille : vous êtes plus vulnérable aux cyberattaques. Une attaque bien ciblée entraîne instantanément l'arrêt de toutes vos activités.

Objectifs

Le nombre de cyberattaques augmente chaque jour. En cybersécurité, attendre qu'il soit trop tard peut vous coûter une fortune. De plus, en raison de la nouvelle directive européenne sur la sécurité des réseaux et de l'information (NIS 2), pratiquement toutes les entreprises seront bientôt obligées de prendre des mesures de cybersécurité.
Heureusement, vous n'êtes pas seul. Dans notre atelier, vous découvrirez le concept « defense in depth » de Siemens, avec lequel nous abordons à la fois la sécurité de votre production, de vos systèmes informatiques et de votre réseau. Attendez-vous à une véritable immersion dans la sécurisation des réseaux, de la segmentation à la surveillance en passant par un accès à distance sûr.
L'après-midi, nous nous attelons en pratique à la sécurisation dans TIA Portal. Pensez au User Management & Access Control (UMAC), aux certificats, à la sécurisation des projets et à la communication cryptée. De cette manière, c'est vous qui bénéficiez des avantages de la numérisation, et non les hackers malveillants.

Programme / Contenu

avant-midi:
Qu'est-ce que NIS2 (Network and Information Security Directive), la directive européenne sur la cybersécurité ? Comment Siemens peut-elle vous aider ?
La norme internationale de cybersécurité IEC62443
Comment Siemens aborde-t-elle cette question par le biais du concept de « défense en profondeur » ?
- Sécurité de l'installation
- Intégrité du système
- Sécurité du réseau

Approfondissement de la sécurité du réseau :
- Segmentation de votre réseau
- Quel firewall utiliser ?
- Accès à distance en mode sécurisé
- Quels outils logiciels peuvent surveiller votre réseau ?
- Comment détecter les « vulnérabilités et anomalies » ?
- Possibilités d'évaluation

UMC (gestion centrale des utilisateurs)
Exercices pratiques avec les firewalls.
après-Midi:
Approfondissement de la sécurité des contrôleurs Simatic et du portail TIA.
Exercices pratiques sur :
- UMAC (User Management & Access Control) : les rôles des utilisateurs et leur influence sur la gestion de projet et l'automate (nouveau dans V3.1).
- La gestion des certificats dans le portail TIA
- La sécurité du projet dans TIA Portal et l'unité centrale Simatic S7
- Communication cryptée

Prérequis

L'atelier dure une journée entière.

Remarque

Pour un atelier, vous payez 220 euros (hors TVA). Si vous combinez 2 ateliers d'une journée complète, vous payez 370 euros (hors TVA) pour les deux. Un bénéfice de 70 € !

Type

Formation en salle

Durée

1 Jour

Langue

mu