Cybersécurité des systèmes industriels : analyse et enjeux

Comprendre la cybersécurité des environnements industriels et ses spécificités ainsi que les principaux risques associés

Stage pratique
Sécurité

Code :
CYBOT

Durée :
1 jour(s) (7,00 heures)

Exposés : **40 %**
Cas pratiques : **40 %**
Echanges d'expérience : **20 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 990,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

DESCRIPTION

Les systèmes industriels (OT) sont aujourd'hui confrontés à des menaces croissantes, susceptibles d'avoir des impacts critiques sur la production et la sécurité des opérations.

Cette formation propose une compréhension claire des spécificités de la cybersécurité des environnements industriels, en mettant en lumière leurs différences avec les systèmes IT ainsi que les principaux risques associés.

Les participants disposent d'une vision des clés nécessaires pour sécuriser les architectures industrielles, déployer des mesures adaptées aux contraintes opérationnelles et pour intégrer la sécurité dans les projets comme dans l'exploitation des systèmes OT.

OBJECTIFS PEDAGOGIQUES

- Comprendre les spécificités des systèmes industriels et les différences entre environnements OT et IT Identifier les principales menaces et vulnérabilités propres aux systèmes industriels
- Connaître les référentiels et normes clés (notamment IEC 62443 et NIST)
- Identifier les bonnes pratiques de sécurisation des environnements OT

PUBLIC CIBLE

- Ingénieur
- Responsable maintenance / production
- RSSI / équipes cybersécurité
- Chef de projet OT

PRE-REQUIS

Connaissances de base en informatique (IT) et en sécurité des systèmes d'information (SSI) recommandées.

METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique des formateurs, complétés

de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci. Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

COMPRÉHENSION DES ENVIRONNEMENTS OT ET SCADA ET DE LEURS SPÉCIFICITÉS

- Définir les systèmes industriels (ICS, SCADA, DCS, PLC) et leurs spécificités
- Identifier les différences entre priorités IT (Confidentialité, Intégrité, Disponibilité) et OT (Sécurité des personnes, continuité opérationnelle)
- Expliquer les enjeux liés à la convergence IT/OT et les risques associés

PRINCIPAUX RISQUES ET VULNÉRABILITÉS DANS L'OT ICS

- Analyser les menaces spécifiques aux environnements industriels : obsolescence, absence de segmentation réseau, accès distants
- Comprendre les impacts des cyberattaques sur la production, la sécurité physique et l'environnement
- Présenter les standards et référentiels (IEC 62443, ISO 27001, NIST 800-82)

NORMES ET CADRES DE RÉFÉRENCE (IEC 62443, NIST, ANSSI)

- Comprendre les principes clés des principaux référentiels de cybersécurité industrielle
- Réaliser un mapping entre les environnements IT

BONNES PRATIQUES DE SÉCURISATION OT TELLES QUE :

- Gouvernance et politiques de sécurité
- Politique de cybersécurité adaptée aux systèmes industriels et rôles et responsabilités (RSSI, ingénieurs OT, équipes MRO)
- Intégration de la cybersécurité dans les processus de gestion du changement et de maintenance

SÉCURISATION DES ARCHITECTURES ET DES PROTOCOLES

- Mettre en œuvre des mesures de protection : segmentation réseau, durcissement des systèmes, contrôle des accès.
- Intégrer la sécurité dès la conception (« SecurityByDesign »)
- Implémenter des mécanismes de protection physique et logique
- Concevoir des architectures industrielles robustes
- Renforcer la sécurité opérationnelle des équipements et sécuriser les protocoles industriels (modbus, DNP3..)
- Déployer des solutions de surveillance et détection (IDS/IPS, SIEM adaptés à l'OT)
- Gérer les correctifs et mises à jour dans des environnements critiques

GESTION DES INCIDENTS ET CONTINUITÉ

- Élaborer des plans de réponse adaptés aux environnements OT
- Simuler des scénarios de crise pour tester la résilience et la coordination
- Intégrer la cybersécurité dans les plans de maintenance et d'exploitation des systèmes industriels

CONCLUSION

- Synthèse de la journée
- Rappel des messages clés
- Évaluation finale

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com