SWARM
innovation & transformation center

CYBERSÉCURITÉ EN ENVIRONNEMENT INDUSTRIEL

#10

LES OBJECTIFS :

- Prendre conscience des enjeux et des vulnérabilités propres aux systèmes cyber-physiques
- Faire converger vos compétences IT et OT et les mobiliser autour d'une vision partagée.
- Expérimenter une démarche pragmatique pour mettre en œuvre votre plan d'action.
- Initier votre propre feuille de route pour augmenter la cyber-résilience de vos actifs industriels.

LE PARCOURS :

CREATIVE LAB.

1 DÉCODER

COMPRENDRE LES ENJEUX PARTAGER LA VISION

- Le réseau industriel et le système de contrôle-commande sont ils des cibles ? Sont-ils davantage vulnérables?
- **Escape Game** : « Nos moyens de production sont attaqués »
  - Saurons-nous détecter ce qui cloche ?
  - Allons-vous réussir à vous protéger sans ralentir la production ?
  - Parviendrons-nous à limiter l'impact de l'attaque et reprendre l'activité ?
- Pourquoi la **collaboration IT-OT** est indispensable ?
- Que devons-nous protéger? Quel objectif réaliste et raisonnable se fixer?
- Quelle norme peut nous aider ? Quelles bonnes pratiques suivre pour progresser?
- Pourquoi utiliser l'approche ZeroTrust?

TRANSFO LAB.

4 SIMULER

PARTAGER ENTRE LES FONCTIONS OT ET IT EXPÉRIMENTER PROGRESSER PAR ETAPE

- **Identifier** : connaître les éléments spécifiques de l'IT et de l'OT en jeu pour construire une culture commune entre nos équipes.
  Explorer les outils pour cartographier les connexions, les échanges de données, les flux transportés, les protocoles spécifiques et établir les zones et conduits.
  Comprendre les méthodes d'analyse de risques et de classification pour prioriser les actifs industriels à protéger en priorité contre les cyber-attaques.
- **Défendre** : regrouper nos objets IOT et nos machines par zone de confiance.
  Organiser/segmenter nos flux applicatifs et de données. Déployer une politique de sécurité efficace et équilibrée pour préserver la performance et l'agilité des actifs industriels.
- **Répondre** : detecter les comportements anormaux , distinguer les tentatives d'attaques des évènements classiques de production. Contenir et traiter les menaces.

TRANSFO LAB.

FAIRE LE POINT ET CONSTRUIRE SA FEUILLE DE ROUTE

3 CONCEVOIR

- Qu'avons nous decouvert ? : notre rapport d'étonnement, notre prise de conscience
- **Quelle priorité** d'action pour nous? : nos urgences à traiter
- Quelle trajectoire pragmatique pour **faire progresser notre cybersécurité industrielle** sans diminuer notre performance opérationnelle ?
  - Nos étapes
  - Notre demarche de co-construction
  - Nos critères de réussite
- La **gestion du facteur humain**

DESCRIPTION :

Comprendre les enjeux, partager la vision.	1 jour
Partager, expérimenter, progresser par étape	3 jours
Faire le point et construire la feuille de route	1 jour
BUDGET	7500 € HT *

*** Parcours labellisé Région Auvergne, Rhône-Alpes :**
Subventionné à 50% sur dépose de dossier auprès de la région AURA
et sous réserve d'acceptation par la commission Région

AGENDA :

1 DÉCODER

JOUR 1 :
Comprendre les enjeux
Partager la vision
(Direction Générale + Responsables OT & IT)

4 SIMULER

JOUR 2, 3 et 4 :
Partager
Expérimenter,
Progresser par étape
(Responsables OT & IT)

3 CONCEVOIR

JOUR 5 :
Faire le point et construire sa feuille de route
(Direction Générale + Fonctions OT & IT)

A mi-parcours, 2h de respiration, de mise en action autour d'une démonstration Fasttrack + afterwork

PARCOURS OPÉRÉ PAR :

CISCO

nxo

SWARM vous accompagne dans la réalisation du dossier :

- Rédaction après analyse avec le client des besoins et projets de l'entreprise
- Procédure de dépose de dossier