INFORMER

LES OPÉRATEURS DE SYSTÈMES INDUSTRIELS SUR LES MENACES ET LES SOLUTIONS DÉJÀ EXISTANTES

PLATEFORME DE DÉMONSTRATION **CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS**

INDUSTRIE DU FUTUR

INTERNET INDUSTRIEL

SYSTÈMES DE CONTRÔLE COMMANDE

SURVEILLANCE ET DÉTECTION

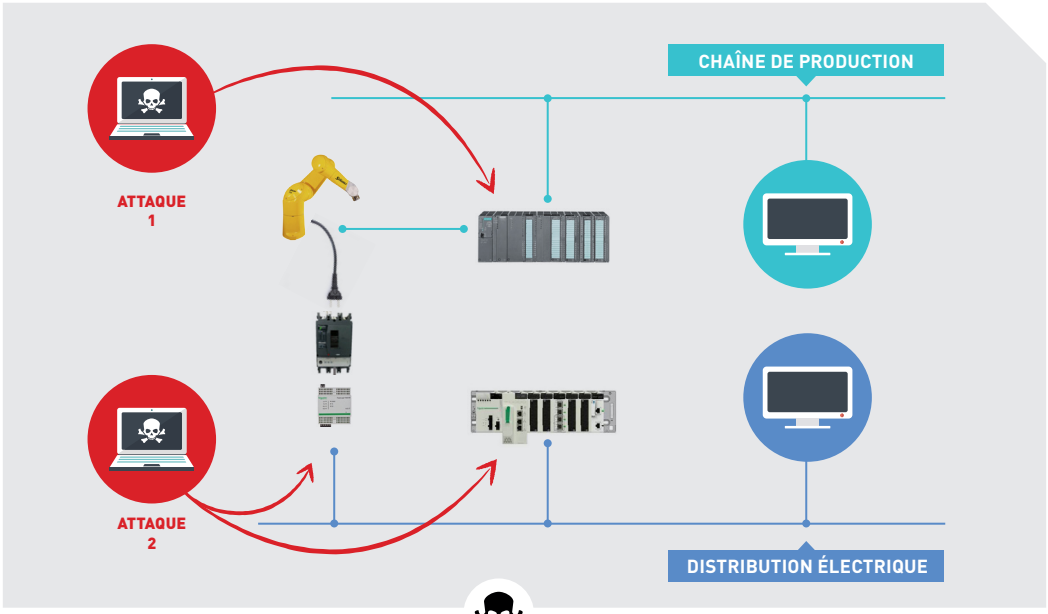
INTÉGRITÉ ET SÉCURITÉ

LE 1ER COLLECTIF EUROPÉEN DÉDIÉ À LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS ET URBAINS

ONLYLYON

DESCRIPTION
DU DÉMONSTRATEUR

Une chaîne de production s'appuie sur des robots pour la fabrication. L'alimentation électrique de l'usine est pilotée par des disjoncteurs communicants.



MENACES Le numérique est au cœur de vos installations industrielles. Nombre d'entre elles ont été conçues de façon à répondre à des besoins de disponibilité / continuité / qualité de service et n'intègrent aucune mesure de cybersécurité.

IMPACTS Disponibilité, fiabilité, sûreté et intégrité sont les véritables enjeux de la cybersécurité : une attaque réussie met à mal tous ces critères !

VULNÉRABILITÉS EXPLOITÉES
Tous les équipements du système industriel sont accessibles sans protection.

ATTAQUE 1

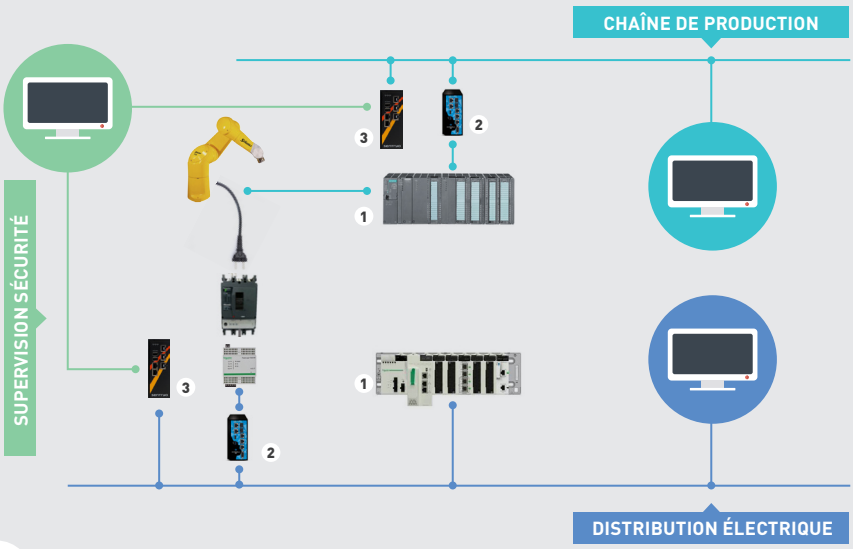
Une pièce jointe, contenant un malware, est ouverte sur un PC de maintenance par un automaticien.
Le code contenu dans le malware ouvre le disjoncteur pilotant le circuit d'alimentation.
C'est donc au travers de l'envoi d'une commande de déclenchement du disjoncteur sur le circuit d'alimentation de votre site que toute la chaîne de production se retrouve hors tension.

ATTAQUE 2

Un autre malware déclenche cette fois une commande pour changer la vitesse des robots de votre usine.
La commande fait diminuer la vitesse du robot : votre productivité chute. La commande envoyée fait accélérer le robot : la qualité des pièces produites est dégradée.

COMMENT SE PROTÉGER
ET ÊTRE ALERTÉ D'UNE ATTAQUE ?

**Pour limiter la surface d'attaque de vos installations, des bonnes pratiques et solutions techniques existent : cloisonnement, pare-feu, contrôle d'accès, etc.
Vous pouvez retrouver ces mesures dans les guides publiés par l'ANSSI.**



SÉCURISATION

La sécurisation du système industriel s'appuie sur des mesures techniques et organisationnelles. Nous ne présentons ci-dessous que les mesures techniques.

→ Les automates de nouvelle génération ❶ disposent de fonctions de cybersécurité : chiffrement entrela supervision et l'automate, authentification pour la lecture et l'écriture de blocs, etc.

→ L'installation d'un pare-feu ❷ permet de protéger les éléments critiques : le disjoncteur et le robot. Ce pare-feu filtre les échanges entre les différents équipements. Un équipement non autorisé ou un contenu malveillant ne pourra traverser cet équipement.

→ L'installation de sondes réseau ❸ permet d'identifier les flux de données et points d'accès inutiles voire dangereux. La connexion d'un équipement non autorisé ou un trafic inadapté sera détecté et vous serez alerté au travers d'un outil de supervision.

→ Ces mesures techniques doivent s'accompagner de mesures organisationnelles pour garantir une protection efficace et un maintien en condition de sécurité. Ces mesures se retrouvent dans les guides de l'ANSSI.

→ L'ANSSI a par ailleurs mis en place un référentiel des exigences pour les prestataires d'intégration et de maintenance de systèmes industriels afin de garantir le niveau de service adapté.

Pour plus d'informations : www.ssi.gouv.fr/systemesindustriels

DE GRANDS NOMS DE L'INDUSTRIE SE RÉUNISSENT **POUR PROMOUVOIR LA CYBERSÉCURITÉ DES SYSTÈMES INDUSTRIELS ET URBAINS**

Pour relever les défis liés à la cybersécurité des systèmes industriels et urbains (industrie connectée, smart building, réseaux de transport, smart grid, IoT industriel...), la Métropole de Lyon s'est associée à de grands noms de l'industrie, des PME et des start-up technologiques pour promouvoir ce thème majeur. De cette rencontre est né le premier collectif dédié en Europe.

6 MEMBRES DU COLLECTIF S'ASSOCIENT POUR PROPOSER CETTE PLATEFORME DE DÉMONSTRATION

ai automatique & industrie

INTÉGRATEUR Coordination et intégration globale maquette cyber /conception maquette robotique

axians

INTÉGRATEUR Intégration et fourniture de solutions réseaux industriels

Schneider Electric

CONSTRUCTEUR Conception maquette distribution électrique / Fourniture automates

SIEMENS

CONSTRUCTEUR Fourniture équipements réseaux industriels et automates

sentryo

CONSTRUCTEUR Sonde réseau et supervision de cybersécurité

STORMSHIELD

CONSTRUCTEUR Pare-feu industriel / développement des attaques

AVEC LE SOUTIEN DE :

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION AUVERGNE-RHÔNE-ALPES

DIRECCTE Auvergne-Rhône-Alpes
Direction Régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi

GRANDLYON la métropole

CONTACT :
Métropole de Lyon
Délégation Développement Économique, Emploi & Savoirs
THIBAUT BANIÈRE - *Chef de projet innovation*
tbaniere@grandlyon.com

ONLYLYON

Merci à Stäubli pour le prêt du robot