

A photograph of a modern industrial factory floor. Several yellow robotic arms are visible, positioned over a production line. The floor is covered with large, blue, grid-patterned panels. The background shows a complex network of white and blue structural beams and overhead lighting. The overall scene is brightly lit and clean.

Cybersécurité industrielle : de la visibilité à la résilience IT/OT

Teodor Chabin

Cyberlead

Cyril Vailler

Spécialiste Réseaux et
Cybersécurité industriels

Risques

La Cyber Résilience et la Cyber Sécurité



Impact sur le réseau
industriel



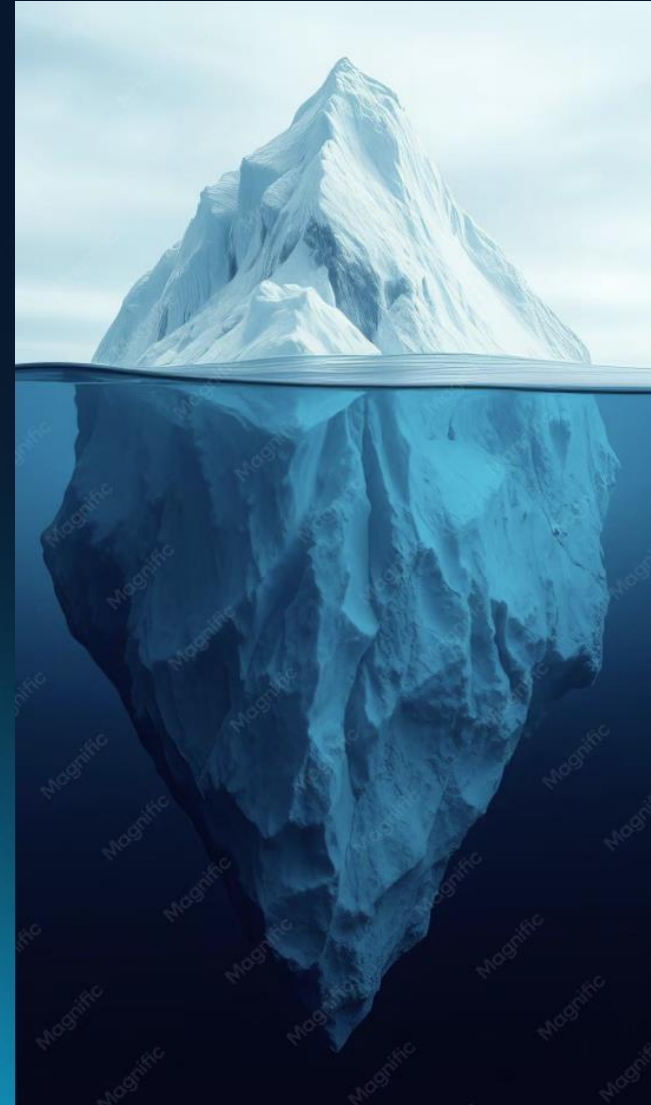
Risques Cyber



Collaboration IT/OT

Visibilité

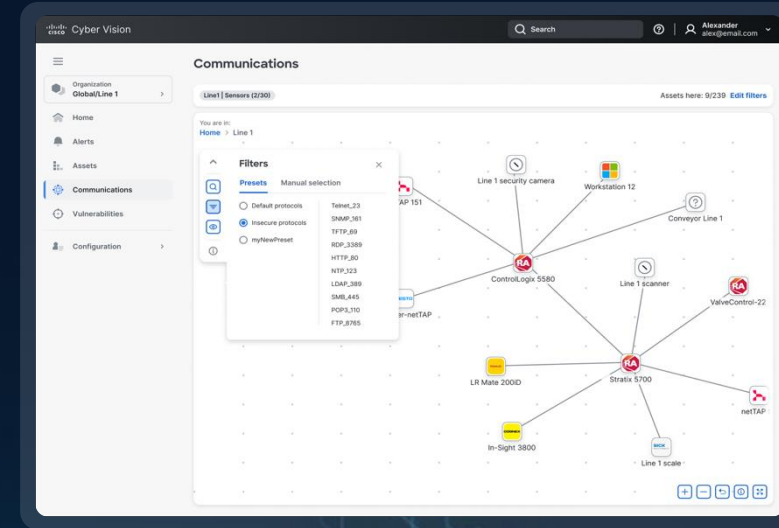
Avoir connaissance de ce
qui est connecté et
communiquant



Visibilité intégrée

- Analyse au niveau des commutateurs
 - ✓ Pas besoin de hardware supplémentaire
 - ✓ Pas besoin de copier le trafic vers un point central
- Listes des assets
 - ✓ Fournisseurs, versions, vulnérabilités
- Matrice de communications
 - ✓ Détection de passerelle 4G...

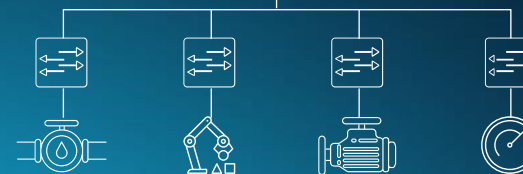
Cyber Vision Center



Seul 3% à 5% du trafic total est transmis au center



Cisco
Commutateur
ou Routeur Industriel



Détection

Une approche silotée n'est pas suffisante pour l'industriel
Détecer les menaces nécessite aussi une visibilité entre plusieurs environnements et contextes

OT, IT, et le Cloud sont des domaines **interconnectés**

Les attaques proviennent de l'IT ou des accès distants pour l'OT de manière malveillante ou no,

Une **visibilité** unifiée interdomaines est clef pour la detection et l'arret des attaques



A well-tailored email causing a user to click....



Which goes to a questionable website....



Which downloads malware to the users' machine....



Allowing a bad actor to log into the OT network



Causing unusual activity in the OT....

Infrastructure



Des documents de design validés et testés pour des infrastructures standardisées , sécurisée, résilientes, disponibles



Déploiements plus rapide



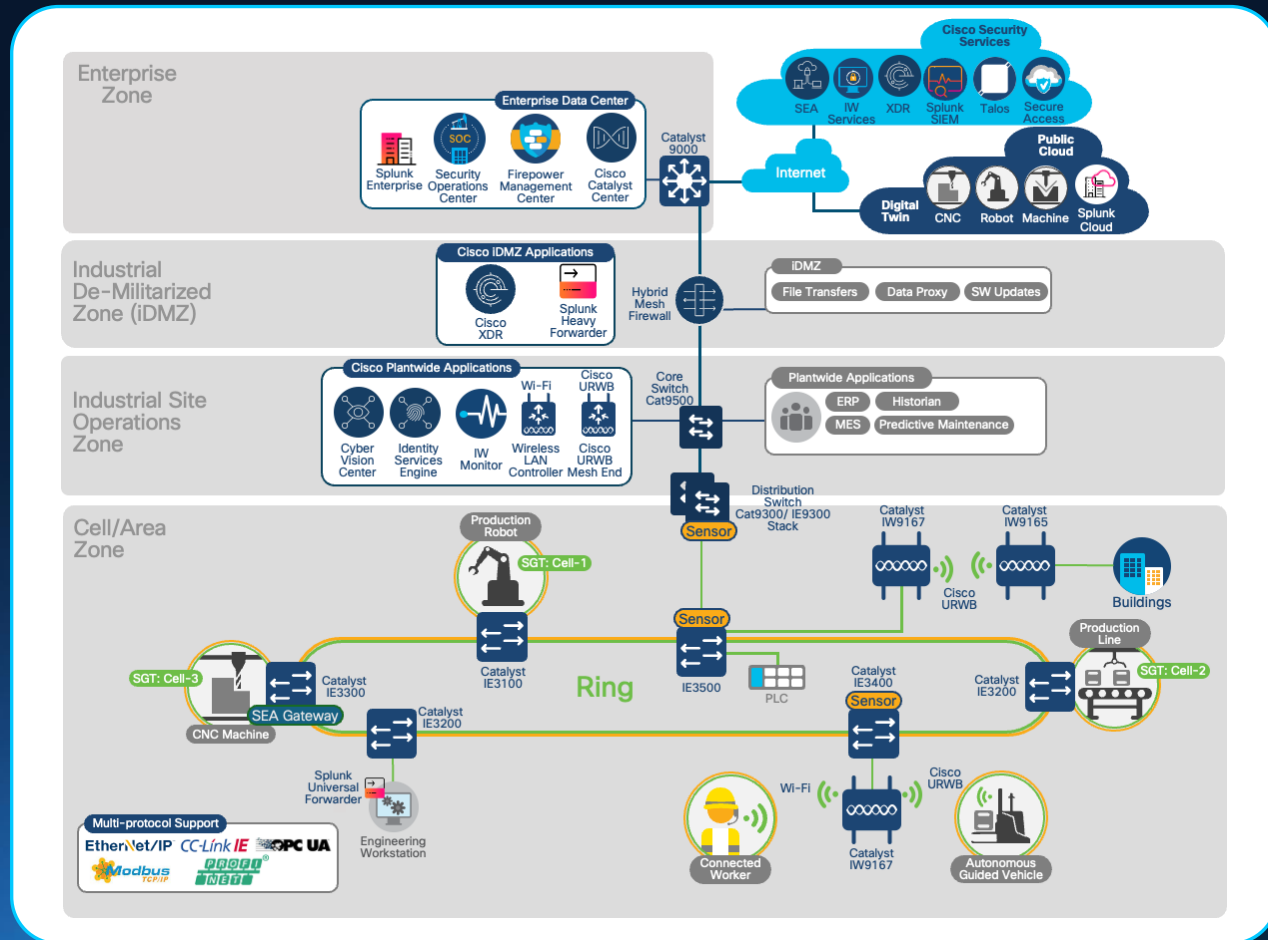
Moins de risques



Predictabilité améliorée



Design de bout en bout



Par où commencer ?

Gérer le risque comment par un assesement

Ce n'est pas une photo, c'est un process en continu

Quelle est votre tolerance au risque ?

Est ce que votre tolerance est alignée avec votre assesement

Quel risque etes vous prêt à accepter ?

L'acceptation du risque ne se défini pas une fois pour toute, il peut évoluer dans le temps

En conclusion



**Évaluer les risques
les impacts métiers**



**Avoir de la visibilité
Avoir la connaissance**



**Détecter
Être vigilant**



**Infrastructure
Le socle**

Merci



Une démarche

Secure remote access
to OT assets



SOC monitoring for
your OT network



Visibility to your risk
exposure



Segmentation to limit
the blast radius