



BAROMETRE CYBER ET ACCOMPAGNEMENTS FINANCIERS

»»» Les Bénéfices de la Sécurité Economique



**La protection de la
Propriété Intellectuelle**



**La Différenciation Technique
Et Commerciale**

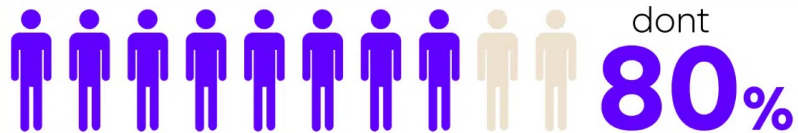


**L'anticipation des
Contraintes Réglementaires**

➤➤➤ Niveau de Maturité des Dirigeants Observés

7/10
dirigeants

n'ont pas de budget, comité de pilotage et assurance dédié à la cybersécurité



dont

80%

sont des entreprises avec moins de 50 salariés



57%

des PME/ETI ont **un référent cybersécurité**

»»» Les Pratiques Constatées

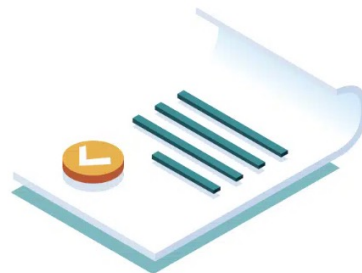


55%

des PME/ETI **sensibilisent leurs collaborateurs**

46%

des entreprises **ont une charte informatique**



➤➤➤ Niveau de protection du SI

1 PME/ETI sur 4 n'a pas de système de sauvegarde externalisée

2 entreprises sur 3 ne disposent pas de solution de protection de ses applications web

dont :

50%

inférieur à 50 salariés

39%

entre 51 et 300 salariés

1 PME/ETI sur 2 n'a pas de solution de protection antivirus de dernière génération

4 PME/ETI sur 5 ne font pas de tests d'intrusion

DONT



51%

inférieur à 50 salariés

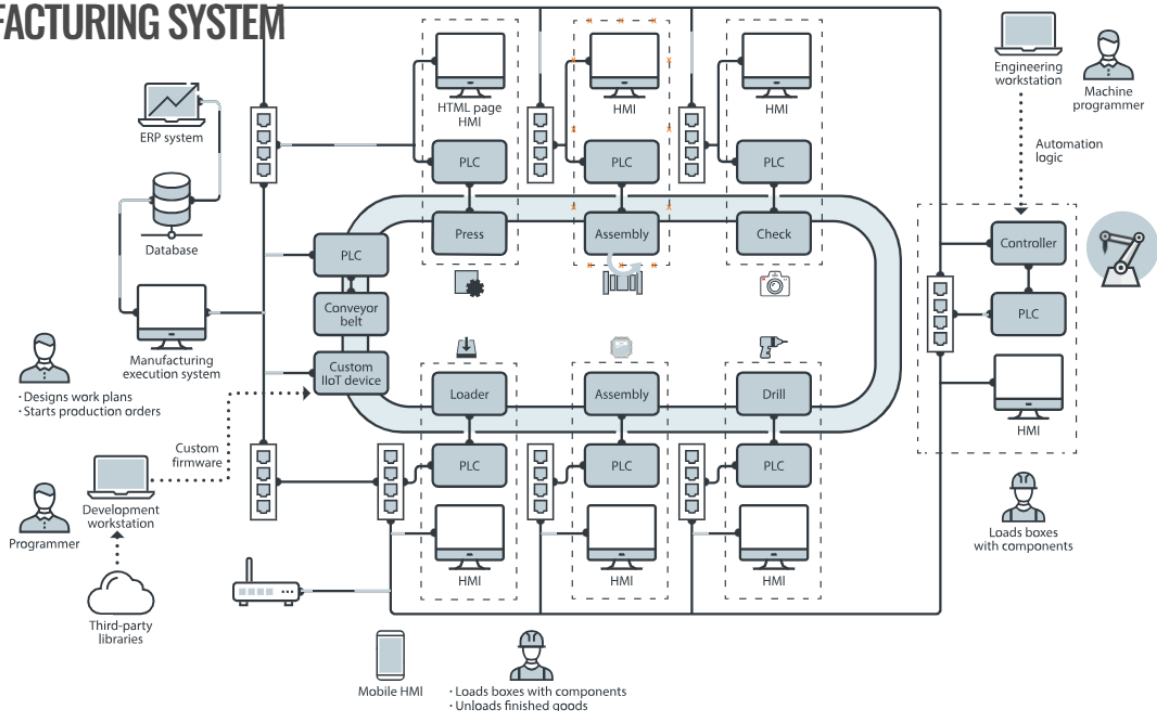
41%

entre 51 et 300 salariés

»»» La complexité de l'OT rend le système vulnérable

Les risques spécifiques à l'informatique industrielles et l'OT

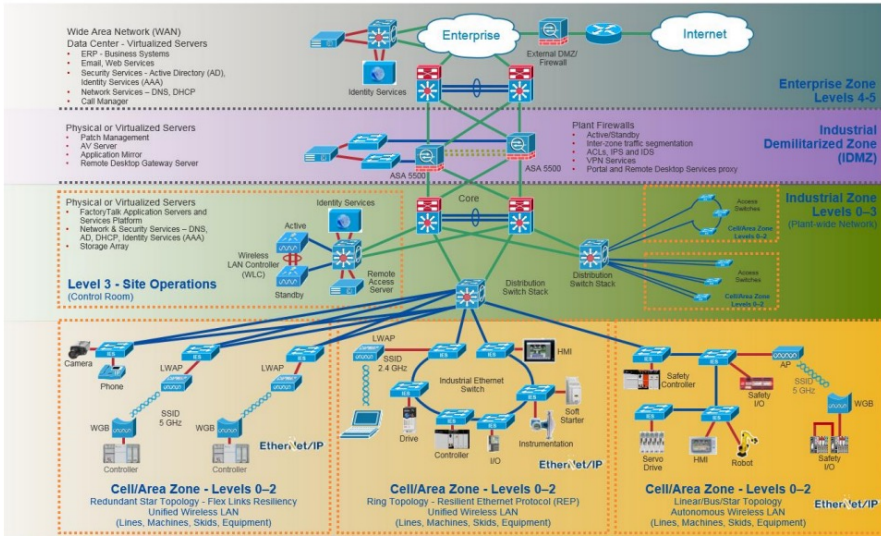
THE SMART MANUFACTURING SYSTEM



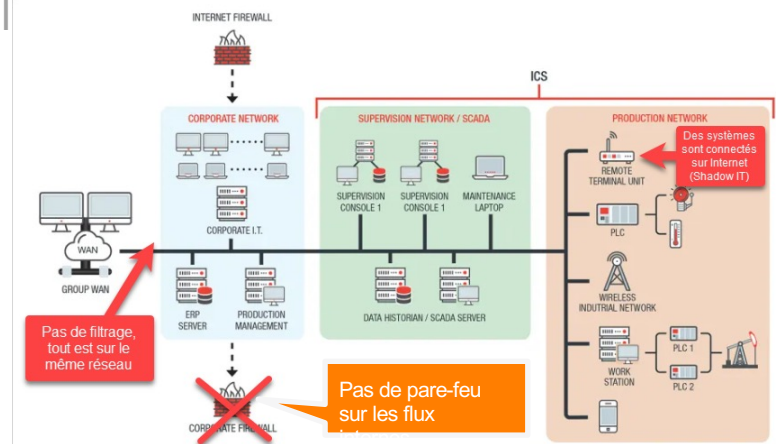
De la théorie à la pratique

Les risques spécifiques à l'informatique industrielle et I

La théorie : cloisonnement des réseaux et collaboration IT/OT

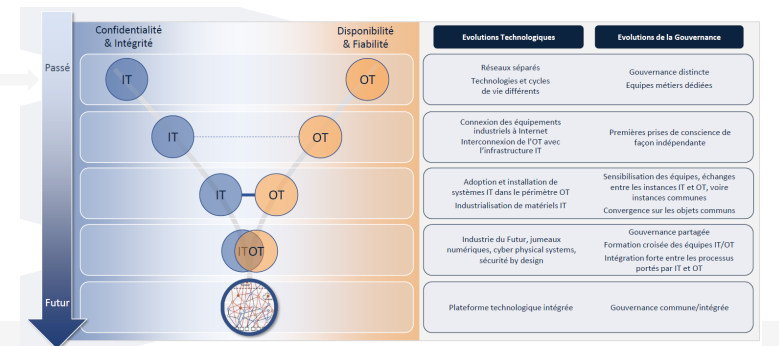


La pratique : aucun cloisonnement réseau et shadow IT



CLOUDSEC 2018 - William Malik, vice-président de la stratégie d'infrastructure chez Trend Micro

La pratique : les équipes IT et OT ont du mal à travailler ensemble



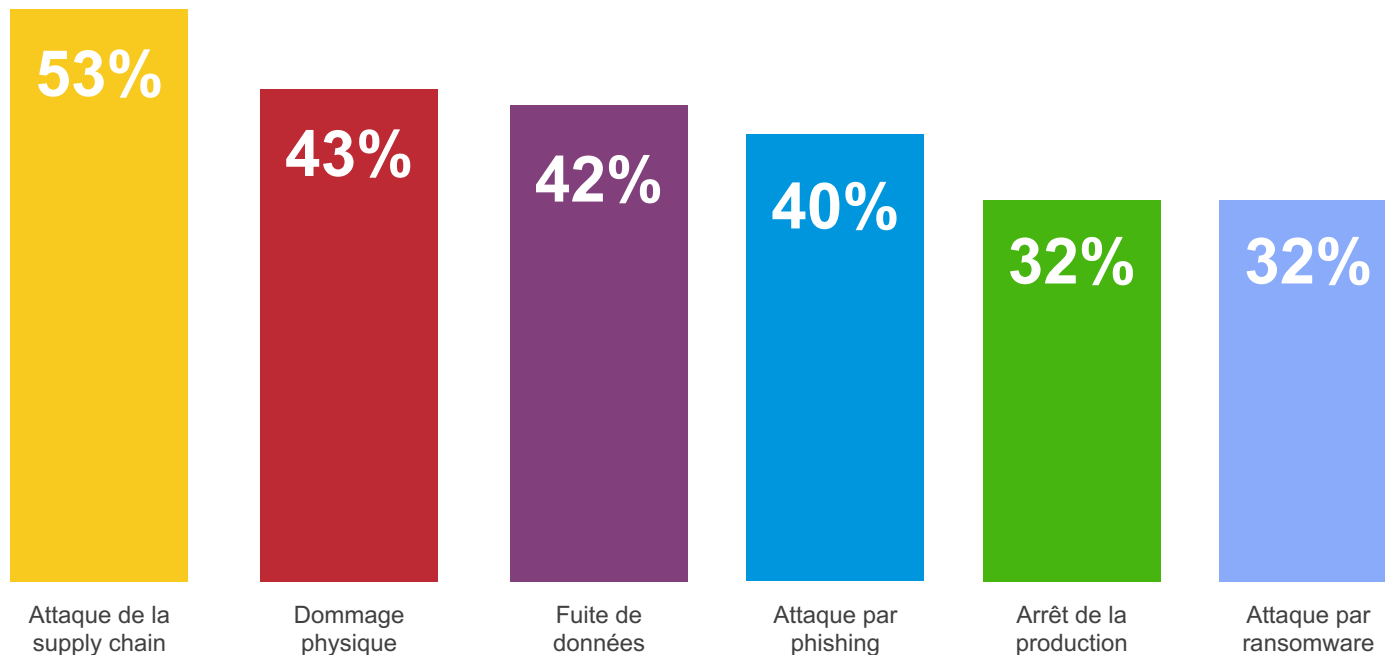
IT and OT Convergence - Recommendations for Building an IoT-Ready Manufacturing Network
ODVA 2017 Industry Conference & 18th Annual Meeting

La convergence n'est pas encore entamée



Les principales préoccupations sur l'OT

Les risques spécifiques à l'informatique industrielles et l'OT



Source : OTARIO 2022 OT Cybersecurity Survey Report



Les 10 mesures essentielles pour une P

Comment se protéger ?

1. Faire des sauvegardes « offline » et testez-les régulièrement
2. Sensibiliser les employés pour qu'ils deviennent des pare feux humains
3. Mettre en place des antivirus performants de type EDR et des systèmes de protection de la messagerie. Traiter les alertes
4. Mettre à jour les logiciels et l'infrastructure SI
5. Mettre en place le Multi Facteur Authentication et des mots de passes robustes
6. Limiter les comptes administrateurs locaux
7. Chiffrer les disques durs des postes de travail
8. Surveiller la surface externe et cloisonner votre réseau
9. Mettre en place une procédure de gestion d'incident
10. Faire des « pentests » internes régulièrement

Être accompagné pour monter progressivement en compétence cybersécurité.



»»» Les outils de financement de la maturité Cyber



Start-up et PME



50% de prise en charge
2,5 k€ d'aide

PME / PMI



50% de prise en charge
max 16 k€ d'aide

Start-up et PME défense



80% de prise en charge
max 11 k€ d'aide

Antoine CAMUS
Directeur Pole Cybersécurité
MINALOGIC

0671836606
Antoine.camus@minalogic.com