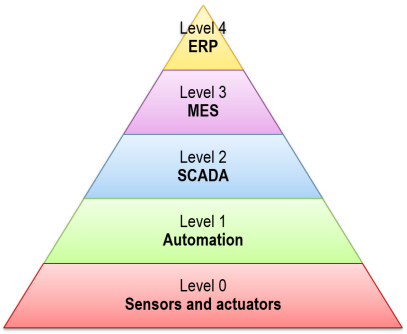
ÉTUDE DE CAS PME

SÉCURISER SON SI ET RÉDUIRE SES COÛTS IT/OT : LA MÉTHODE GAGNANTE

1 INTRODUCTION

Contexte des entreprises industrielles

Dans l'industrie, la digitalisation accélère et l'interconnexion des systèmes de gestion (ERP, CRM…), des infrastructures IT et des équipements de production (SCADA, MES, automates…) augmente.



Cette convergence IT/OT apporte des gains de productivité, mais expose aussi à de nouveaux risques :

- Vulnérabilités cyber sur les réseaux industriels et bureautiques
- Difficulté à piloter l'ensemble des coûts IT/OT
- Complexité de la gestion de la donnée entre production et SI d'entreprise

Objectif du document

Montrer comment une approche globale, intégrant IT & OT, permet d'améliorer la sécurité et de maîtriser durablement les budgets, tout en optimisant la performance.

2 DIAGNOSTIC INITIAL

Situation classique rencontrée dans les PME industrielles

- **Informatique d'entreprise (IT)**
  - ERP vieillissant, absence de PRA/PCA, serveurs disparates, sauvegardes peu fiables
  - Données métiers dispersées, absence de gouvernance claire
  - DMZ inexistante ou mal configurée, réseaux bureautiques mêlés aux accès industriels
- **Informatique industrielle (OT)**
  - Réseaux SCADA/MES isolés mais parfois connectés sans contrôle au SI
  - Automates anciens, non patchés, documentation lacunaire
  - Absence de supervision centralisée ou de gestion de flotte d'automates

Conséquences

- Risques de propagation de cyberattaques entre IT et OT
- Difficulté à tracer et à sécuriser les flux de données
- Multiplication des incidents : interruptions de production, pertes de données, surcoûts cachés

Chiffres types observés dans l'industrie

- Surcoûts IT/OT : jusqu'à 30 % du budget SI
- Incidents annuels liés à la convergence : 3 à 8
- Temps de reprise après incident : plusieurs heures à plusieurs jours

3 Approche & Solutions

La méthode Digital Compass – Double compétence IT/OT

1. **Audit croisé IT/OT**
    - Cartographie des flux entre ERP, DMZ, systemes industriels
    - Analyse des points de contact et des vulnérabilités croisées
2. **Déploiement d'une architecture sécurisée**
    - Séparation stricte des réseaux (VLAN, firewalls, DMZ)
    - Renforcement des accès distants (VPN, authentification forte)
    - Centralisation des sauvegardes de données métiers ET de production
3. **Optimisation opérationnelle**
    - Rationalisation des licences logiciels, maintenance centralisée des serveurs
    - Déploiement de solutions de supervision des applications avec gestion des alertes centralisé et unifié
    - Mise en place d'un plan de gestion des mises à jour des logiciels et des automatismes
4. **Accompagnement au changement**
    - Formation des équipes (IT et industriel)
    - Gouvernance partagée des projets de digitalisation

Le + Digital Compass

Une vision globale, de l'infrastructure IT au réseau d'usine, pour garantir cohérence, sécurité et performance.

4 Exemple d'action : Sécurisation des flux entre OT et IT via une DMZ

Problématique

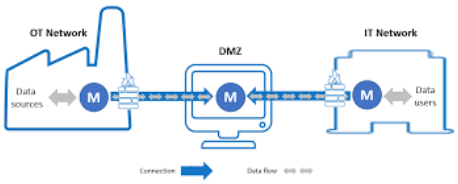
Dans de nombreuses PME industrielles, les réseaux de production (OT) et les réseaux bureautiques (IT) communiquent de façon directe, ouvrant la porte à des cyberattaques et à la propagation de menaces d'un environnement à l'autre.

Solution mise en œuvre

Nous avons déployé une **DMZ (zone démilitarisée)** dédiée, jouant le rôle de "sas sécurisé" entre l'usine (OT) et les services administratifs (IT).

Grâce à l'architecture illustrée ci-contre :

- **Séparation stricte des flux** : les échanges de données passent par la DMZ, protégée par des firewalls et des contrôles d'accès renforcés.
- **Contrôle et traçabilité** : chaque transfert de données entre l'atelier et le SI est surveillé et journalisé.
- **Réduction drastique du risque** : une attaque sur l'IT ne peut plus se propager jusqu'aux automates ou systèmes industriels, et inversement.



Bénéfices constatés

- Diminution des incidents de sécurité IT/OT
- Meilleure visibilité sur les flux de données
- Conformité accrue aux référentiels industriels

5 RÉSULTATS & ROI OBTENUS (MOYENNES OBSERVÉES)

- **Réduction du risque cyber** : quasi élimination des points de passage non contrôlés entre IT et OT
- **Baisse des coûts IT/OT** : jusqu'a -30 % sur 12 mois (rationalisation infrastructure et licences, moins d'incidents)
- **Productivité** : meilleur disponibilité des moyens de production, données mieux valorisées (meilleure traçabilité, reporting temps réel)
- **Réactivité** : temps de reprise après incident divisé par 4

Témoignage d'un dirigeant industriel

> *« La convergence IT/OT était un vrai casse-tête. Grâce à une approche globale, nous avons sécurisé nos flux, simplifié la maintenance, et retrouvé une vision claire de notre budget SI. »*

6 POINTS CLÉS À RETENIR

Conseils pour les industriels

1. **Cartographiez vos flux IT/OT pour identifier les risques**
2. **Séparez physiquement et logiquement les réseaux de gestion et de production**
3. **Centralisez la gouvernance de la donnée, du bureau à l'atelier**
4. **Mettez en place des procédures de mise à jour et de sauvegarde sur l'ensemble du périmètre**

Les erreurs à éviter

- Laisser des accès distants non maîtrisés entre OT et IT
- Négliger la formation des équipes de production aux enjeux cyber
- Reporter la mise en place d'une DMZ industrielle

7 PASSEZ À L'ACTION

Vous êtes une PME industrielle confrontée à ces enjeux ?

👉 [Lien ou QR code]

Demandez votre interview IT/OT offert (60 min)

Contact : contact@digitalcompass.fr
www.digitalcompass.fr