Digital Risk: Remote-Monitoring, IoT Sensors and Data Integrity Stats and Facts – French



FAITS

- **La fiabilité d'un capteur dépend de la qualité de ses données:** un capteur mal étalonné, compromis ou défectueux ne signale pas une situation dangereuse – il ne fait que fournir un chiffre. Les travailleurs qui agissent sur la base de données erronées s'exposent à des dangers invisibles jusqu'à ce qu'ils se traduisent par des blessures.
- **L'accès à distance est une porte à double sens:** les systèmes qui permettent aux utilisateurs autorisés de surveiller les conditions à distance peuvent également être accessibles à des personnes non autorisées. Sans authentification adéquate ni pare-feu, l'accès à distance constitue une porte ouverte vers tous les systèmes critiques pour la sécurité auxquels il est connecté.
- **L'intégrité des données est un enjeu de sécurité:** des lectures de capteurs altérées ou falsifiées peuvent masquer des conditions dangereuses – faibles niveaux d'oxygène, concentrations élevées de produits chimiques, défaillances d'équipement – jusqu'à ce qu'il soit trop tard pour qu'un travailleur puisse réagir.
- **Les appareils de l'IdO sont souvent non gérés:** de nombreux capteurs industriels de l'IdO ne reçoivent pas régulièrement de correctifs et ne font pas l'objet d'une surveillance visant à détecter tout comportement anormal, ce qui crée des vulnérabilités persistantes dans les systèmes dont dépendent les travailleurs pour obtenir des renseignements sur la sécurité.
- **L'automatisation peut échouer en silence:** un système de sécurité compromis ou mal configuré peut continuer à sembler fonctionnel tout en n'offrant aucune protection réelle. Un voyant vert sur un tableau de bord n'équivaut pas à une condition de sécurité confirmée.

STATISTIQUES

- Selon une étude sur la cybersécurité industrielle, le coût moyen d'une violation de données dans le secteur manufacturier a atteint 4,97 millions de dollars en 2024, sans compter les amendes réglementaires et les pertes

liées à l’interruption des activités.

- Selon une étude du secteur de la sécurité OT/IoT, 77 % des entreprises industrielles en sont encore aux premières étapes de la mise en œuvre de la sécurité OT, et aucune n’est entièrement sécurisée.
- On prévoit que 15,14 milliards d’appareils IoT seront installés à l’échelle mondiale d’ici 2029, ce qui élargira considérablement la surface d’attaque dans les environnements où la sécurité est critique.
- Le 5 février 2021, un pirate informatique a obtenu un accès à distance non autorisé à l’usine de traitement de l’eau d’Oldsmar, en Floride, et a augmenté la concentration d’hydroxyde de sodium de 100 à 11 100 parties par million — un niveau susceptible de causer de graves brûlures chimiques, voire la mort. Un employé vigilant s’en est aperçu et a annulé la modification avant que l’eau n’atteigne les consommateurs.
- Selon GuidePoint Security, le secteur manufacturier a été le plus ciblé par les rançongiciels en 2025, avec une augmentation de 58 % d’une année sur l’autre du nombre de victimes parmi les organisations industrielles.
- 34 des 39 vulnérabilités de l’Internet des objets (IdO) les plus fréquemment exploitées sont connues depuis plus de trois ans en moyenne — ce qui signifie que la plupart des attaques réussies exploitent des failles déjà documentées et évitables, selon le rapport 2024 d’Asimily sur la sécurité des appareils IdO.