WALLIX
TRACE, AUDIT & TRUST

NOUS PROTÉGEONS VOS INFRASTRUCTURES SENSIBLES
NOUS COMPRENONS VOS MÉTIERS

INDUSTRIE
RÉSILIENCE / SCADA / OIV

Les systèmes industriels se différencient des systèmes d'information de gestion « classiques » par le fait qu'ils pilotent des installations physiques (unités de chaîne de production, infrastructures et réseaux de distribution smartgrids…). **Ils utilisent également abondamment les technologies de l'information alors qu'ils n'ont pas été conçus pour faire face aux menaces qu'elles introduisent.** Les interconnexions des systèmes industriels aux réseaux IP et au Système d'Information véhiculent de nouveaux risques dont les conséquences peuvent être critiques pour leur propre activité ou vitale pour les utilisateurs ou clients.

RÉGLEMENTATIONS

- **NERC CIP**
- **SP-800-82**
- **ISO 27000**
- **NIS / Opérateurs d'importance vitale (OIV)**
- **RGDP**

La solution WALLIX ADMINBASTION SUITE (WAB Suite) permet de contrôler, tracer et gérer les accès des utilisateurs internes et externes au réseau de technologie opérationnelle. Les Systèmes de Contrôles Industriels (SCI) sont extrêmement vulnérables aux menaces dont certaines peuvent avoir des conséquences critiques sur le marché des opérateurs d'importance vitale (OIV). La sûreté de fonctionnement et la résilience sont parties intégrantes des contraintes qui pèsent sur les outils industriels.

CAS D'USAGE

La solution WALLIX ADMINBASTION SUITE protège les comptes à privilèges des SCI et systèmes SCADA et détecte les vulnérabilités inhérentes à la connectivité entre les SCI, les environnements IT, l'Internet et les utilisateurs à distance.

- **Optimiser la configuration avec l'auto-découverte** de tous les comptes à privilèges Windows et Linux,
- **Contrôler et protéger les accès aux équipements, aux automates et aux bus de terrain :** gestion des identifiants, accord de connexion sur certains équipements et selon certaines fréquences,
- **Appliquer une politique granulaire** de connexion des utilisateurs internes et externes (prestataires externes),
- **Sécuriser et gérer la rotation automatique des mots de passe et des clés SSH**, en particulier ceux des utilisateurs à distance avec le SCI,
- **Isoler les systèmes critiques** par le contrôle d'accès à des serveurs de rebond,
- **Alerter en temps réel** le département IT, les responsables de la technologie opérationnelle et l'équipe en charge de la sécurité afin de détecter, réagir automatiquement et stopper la progression d'une attaque en cours, réduisant ainsi au minimum les perturbations et les éventuels dommages causés à l'entreprise,
- **Tracer et enregistrer** les connexions, bénéficier d'un audit en temps réel et de reportings complets.