HEXATRUST

CYBERSECURITY & DIGITAL TRUST

SECURISATION DES SYSTEMES INDUSTRIELS

Sécuriser les systèmes de production industrielle, les grandes infrastructures critiques et l'Industrial Internet Of Things (IIoT)

Au cœur de notre appareil productif, les systèmes industriels, les opérateurs d'importance vitale (OIV) et les grandes infrastructures publiques garantissent le bon fonctionnement de notre économie. Pourtant, ils ont longtemps été le parent pauvre de la politique de Cyber Sécurité des entreprises et des Etats, du fait de leurs caractéristiques et contraintes spécifiques, mais aussi de leur position relativement à l'écart du reste de l'informatique.

Or la digitalisation, et notamment l'IIoT, a pour effet d'intensifier l'interconnexion des entreprises industrielles avec leurs fournisseurs, partenaires et clients, augmentant la fréquence des risques et l'impact des attaques ciblant ces systèmes. « La Cyber Sécurité des systèmes de contrôle / SCADA est au cœur de nombreux processus industriels et est un domaine en croissance qui va présenter des opportunités commerciales et industrielles », a déclaré ainsi Udo Helmbrecht, Directeur Exécutif de l'ENISA (European Network and Information Security Agency).

VISION PAC

A CXP GROUP COMPANY

A l'instar d'autres pans de notre économie, **les systèmes industriels se digitalisent**. Quelque 75% des entreprises industrielles se sont lancées dans une approche de transformation numérique (*source : enquête PAC Global CxO 3000, 2015*). Vu les perspectives de gains d'efficacité et d'innovation qu'elle ouvre, la transformation digitale de leurs systèmes est devenue une **préoccupation majeure** pour les acteurs de l'industrie et des infrastructures.

Toutefois, la transformation digitale multiplie les facteurs de vulnérabilité et devient un vecteur de choix pour les **cyberattaques**. En protégeant la digitalisation, la Cyber Sécurité constitue un catalyseur critique de ce processus.

Les attaques sont de plus en plus **fréquentes**. Surtout, leur impact peut prendre un caractère systémique par le biais de la digitalisation. Les systèmes de sécurité « *classiques* » ne sont plus adaptés à ces nouvelles contraintes et les dispositifs de contrôle utilisés pour les infrastructures critiques et pour les installations industrielles s'avèrent de moins en moins efficaces.

D'où la **préoccupation** désormais centrale des acteurs de l'industrie, de l'énergie, des transports et de l'infrastructure : se prémunir contre les attaques sur les systèmes de production, devenues l'**une des trois menaces** que ces entreprises redoutent le plus (*source : enquête PAC Global CxO 3000, 2015*).

Le témoin de cette prise de conscience est le durcissement de la réglementation et le renforcement des investissements.

Le **manque de visibilité** que les entreprises ont de leurs systèmes industriels est la principale barrière à une protection efficace. Comment réagir en temps réel sans une bonne maîtrise des interrelations entre modules ? Comment anticiper les attaques sans une bonne vision de l'évolution des systèmes dans le temps? La clé d'une cybersécurisation optimale des systèmes est donc d'assurer une **supervision globale** de tous les éléments pour détecter les comportements anormaux et, de ce fait, les attaques.

Chaque réseau industriel, du fait des machines et des logiciels spécifiques qui le composent, se distingue par des caractéristiques qui lui sont propres (protocoles, mémoire, processus critiques) qu'il faut prendre en compte dans leur sécurisation. Ceci explique la **rareté** des solutions de Cyber Sécurité spécifiques aux systèmes industriels et, par extension, capables de répondre aux exigences de l'IIoT.

RÉPONSE D'HEXATRUST

HEXATRUST
CYBERSECURITY & DIGITAL TRUST

Les membres d'**HEXATRUST** proposent des solutions qui adressent des problématiques cruciales et complémentaires pour les systèmes industriels : la **surveillance**, l'**isolation** et le **continuum de sécurité logique-physique**.

La protection d'un système, d'une installation, d'une chaine de production industrielle, nécessite une **surveillance complète** de l'ensemble de ses modules et de leurs interactions. Cette surveillance doit être adaptée aux contraintes spécifiques des métiers de ces entreprises et de leurs systèmes de production.

L'**isolation** quant à elle est un élément fondamental de la gestion des systèmes industriels et des infrastructures critiques. C'est la condition *sine qua non* pour éviter la contagion des attaques les plus dangereuses entre les modules composant le réseau. Cette isolation ne doit pas se faire au détriment des activités de l'entreprise et doit préserver la fluidité des interactions.

La surveillance physique des installations critiques étant également un impératif, le **continuum de sécurité logique-physique** consiste à faire remonter des alertes de Cyber Sécurité vers les PC Sécurité des sites industriels pour pallier à des cyberattaques visant les protections d'accès au site, préalables à de potentielles intrusions physiques.

POSITIONNEMENT ET AVANTAGE D'HEXATRUST

Deux types de solutions sont actuellement disponibles sur le marché. D'un côté, les **solutions embarquées** issues du milieu industriel, développées à l'origine en spécifique et liées à un type de plateforme ou de constructeur (Siemens, ABB, Kubota, etc.). Les **solutions** issues de **l'informatique de gestion** ne répondent pas ou très partiellement aux contraintes des systèmes industriels. Elles sont souvent **intrusives**, ne supportent pas les standards du monde industriel et sont conçues pour être gérées par des informaticiens et non par des **automaticiens**, c'est en particulier le cas des principaux Firewall ou IDS.

Les solutions proposées par les membres d'**HEXATRUST** sont précisément conçues pour la **protection et la surveillance des réseaux industriels**.

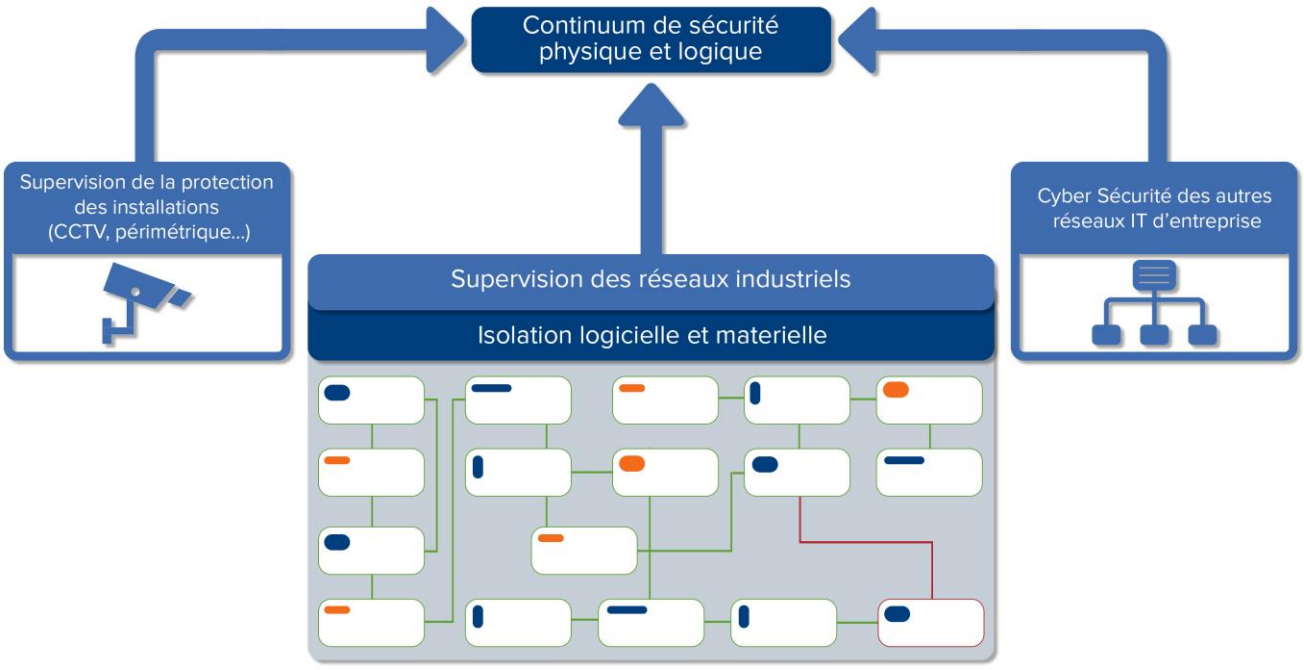
Au niveau protection elles permettent l'isolation stricte des différentes composantes du réseau, le contrôle des personnels chargés de l'administration et l'identification des vulnérabilités.

Au niveau supervision elles permettent d'une part la surveillance du réseau et la détection de comportements anormaux mais aussi la gestion de la surveillance physique des installations industrielles.

Ce **continuum** entre cyber sécurité et gestion de la sécurité physique des installations apporte une **réponse globale** aux problématiques de groupes industriels qui sont ou seront tôt ou tard confrontés à des **attaques « hybrides »**, mêlant malveillance informatique et pénétration non autorisée sur sites sensibles.

HEXATRUST apporte ainsi la réponse européenne optimale aux besoins de cybersécurisation de vos systèmes industriels.

SÉCURISATION DES SYSTÈMES INDUSTRIELS



L'Association HEXATRUST : HEXATRUST est née de la volonté commune de PME et ETI françaises, acteurs complémentaires experts de la sécurité des systèmes d'information, de la cyber sécurité et de la confiance numérique.

10 bis, Avenue Ampère
78180 Montigny-le-Bretonneux – France
Tél : +33 1 39 30 62 50
www.bertin-it.com
contact@bertin-it.com

Bertin IT propose une gamme complète pour la défense en profondeur des infrastructures critiques. Sa plateforme de cyber intelligence permet de détecter les signes précurseurs de cyber attaques ou de toute autre opération malveillante ciblant un OIV. Ses solutions basées sur son hyperviseur certifié EAL 5+ assurent quant à elles la neutralisation des menaces USB, la sécurisation des interconnexions réseaux et le cloisonnement des données sensibles au sein de postes multi-domaine.

86 rue de Paris
91400 Orsay – France
Tél : +33 1 77 93 21 27
www.egidium-technologies.com
contact@egidium-technologies.com

La tenue de situation qui s'adapte à vos impératifs de sécurité présents et futurs. Egidium fournit un logiciel de supervision de la sécurité physique qui prend aussi en compte les cyber alertes.

40 avenue Théroigne de Méricourt
34000 Montpellier – France
Tél : +33 4 11 93 08 59
www.seclab-solutions.com
contact@seclab-solutions.com

Constatant que la sécurité logicielle est insuffisante pour les systèmes critiques, notre offre se base sur une approche de défense en profondeur implémentée dans l'électronique. **DENELIS** est une gamme de passerelles réseau filtrantes bidirectionnelles dont le cloisonnement réseau est assuré par une carte électronique.
SCOOP protège les ordinateurs et automates de toute attaque USB, des couches électriques aux couches logicielles. **Pocket Pass**, est une solution de gestion et de distribution de mots de passe aux exploitants et aux intervenants en milieu industriel.

Bâtiment CEI-1
66 boulevard Niels Bohr
CS 52132, 69603
Villeurbanne Cedex – France
Tél : +33 9 70 46 96 94
www.sentryo.net
contact@sentryo.net

Sentryo est un pionnier de la protection des réseaux M2M et des systèmes industriels critiques. Sentryo ICS CyberVision surveille le réseau, détecte les comportements anormaux et permet de répondre aux incidents en évitant les dommages. Sentryo s'adresse aux opérateurs d'infrastructure critique dans l'énergie, le transport ou l'environnement et à toutes les entreprises industrielles qui relèvent le défi de l'industrie du futur.

250 bis, rue du Faubourg Saint-Honoré, 75008, Paris France
Tél : +33 1 53 42 12 90
www.wallix.com
sales@wallix.com

Wallix AdminBastion Suite permet de sécuriser les infrastructures SCADA via le contrôle, la traçabilité et l'enregistrement de tous les accès à ces infrastructures. En complément, le mécanisme de SSO de WAB Suite évite d'avoir à transmettre les mots de passe de l'infrastructure SCADA à d'éventuels prestataires externes.