Sécurisation d’infrastructures industrielles : retour d’expérience

Yann BOURJAULT, Directeur Département Transformation Digitale France
Network Engineering & Cybersecurity : FR-NEC@schneider-electric.com

Schneider Electric, spécialiste mondial de la gestion de l'énergie et des automatismes

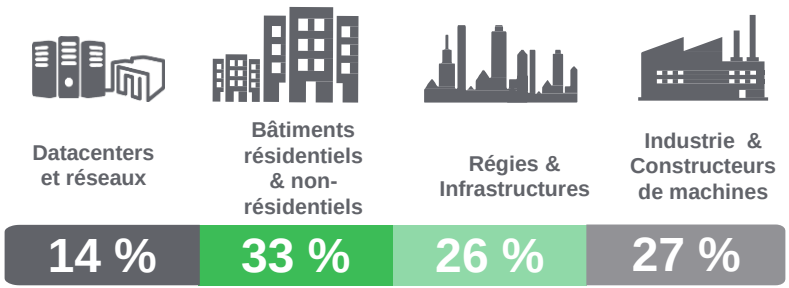
€25 milliards
CA 2016

~5%
du CA investi en R&D

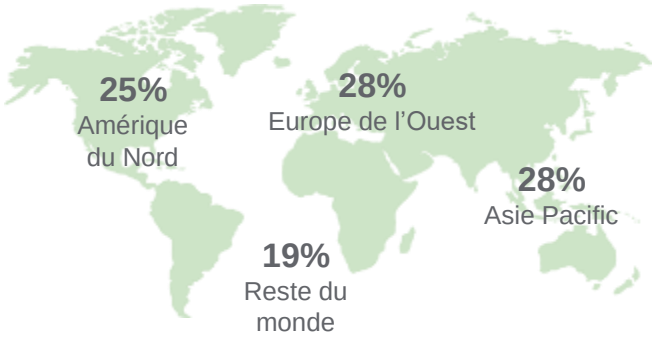
43%
du CA en solutions

~160,000
employés dans +100 pays

Marchés finaux diversifiés – CA 2016



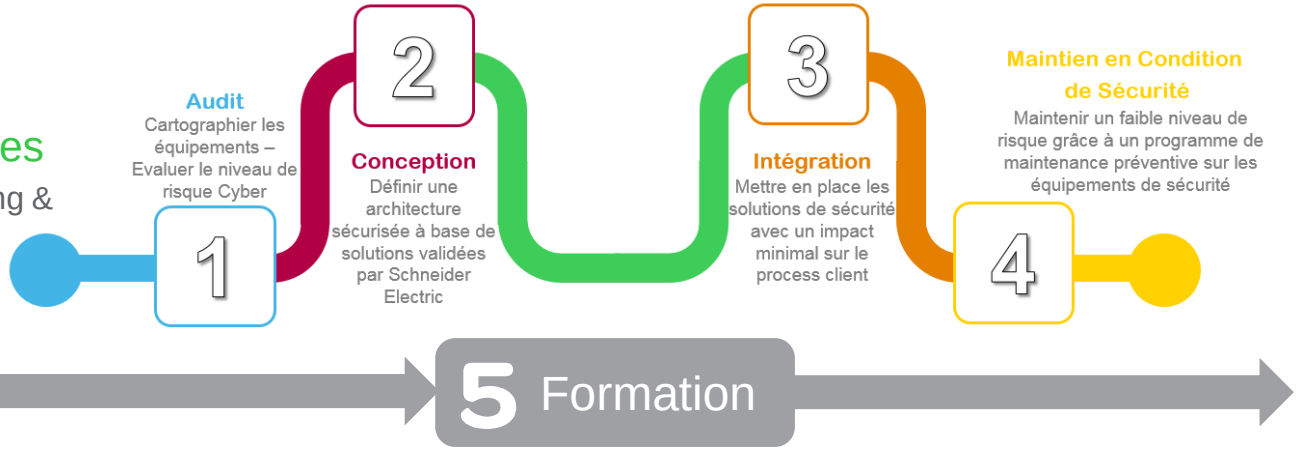
Répartition géographique – CA 2016



Schneider Electric – Programme Cybersécurité

1 – Projets & Services

NEC : Network Engineering & Cybersecurity



2 – Produits / Logiciels

Cybersécurité intégrée dans le cycle de développement :

- Contrôleur M580, FCP280
- Disjoncteur MasterPact MTZ,
- Système de protection PACIS,
- Relais de protection Easergy,
- Micro Data center Smart Bunker,
- Wonderware, EcoBuilding,

EcoStruxure

3 – Partenariats

Produits et logiciels validés dans les solutions Schneider

STORMSHIELD

THALES

McAfee

WALLIX TRACE, AUDIT & TRUST

KUB

sentryo

NEC : l'équipe France

Network Engineering & Cybersecurity

Notre expérience

10 ans d'expérience dans les métiers de l'informatique industrielle
5 ans de collaboration avec l'ANSSI dans la cybersécurité industrielle

Nos compétences

Analyse de risque, Conception d'architecture
Intégration de solutions
Audit, Conseil, Formation

Nos certifications

GSEC, GCIA, GCIH, Hirschmann, Stormshield Network Security,
Microsoft, Vmware, Wallix Admin et Expert,
Cisco, Checkpoint

Nos moyens

3 équipes (Lyon, Nantes et Lille) , des relais répartis ailleurs en France
1 plateforme de test et démonstration à Lyon

Nos labels

NEC : Une reconnaissance nationale

> Janvier 2018 – WALLIX

Schneider Electric reçoit de WALLIX le Prix Spécial de l'Innovation, thématique Industrie du Futur, pour son offre IPAM développée en 2017

> Janvier 2018 - HEXATRUST

H E X A T R U S T

CLOUD CONFIDENCE & CYBERSECURITY

Schneider Electric rejoint Hexatrust, consortium qui regroupe les entreprises numériques de confiance

> Janvier 2018 – Label France Cyber

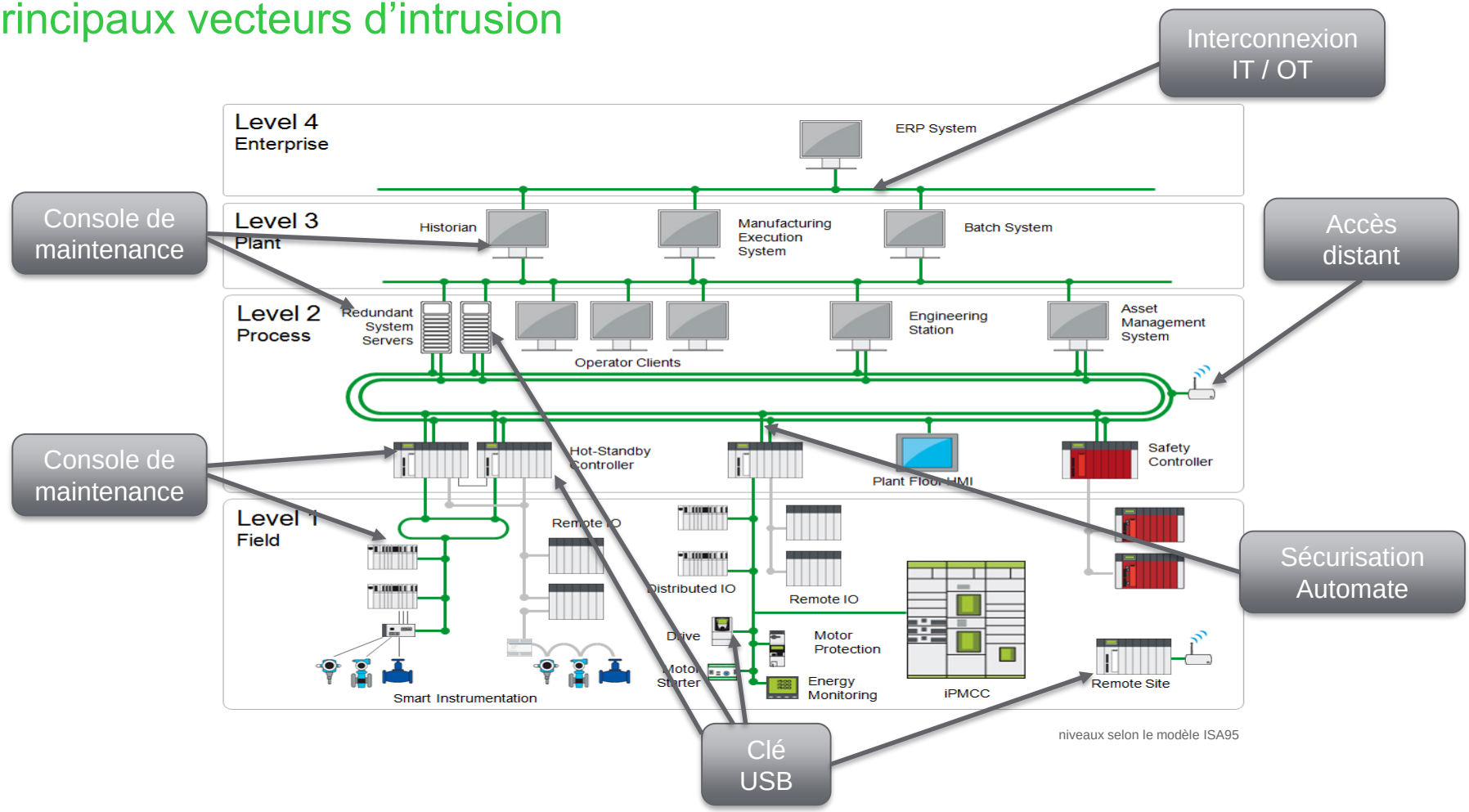
Schneider Electric reçoit le Label France Cyber 2018 de Mounir MAHJOUBI, Secrétaire d'Etat en charge du numérique, pour son offre de Services en Cybersécurité industrielle

> Août 2018 – Label ANSSI Formation continue SecNumEdu

Schneider Electric reçoit la labellisation SecNumEdu de l'ANSSI pour sa formation continue CYBINDUS de 3 jours

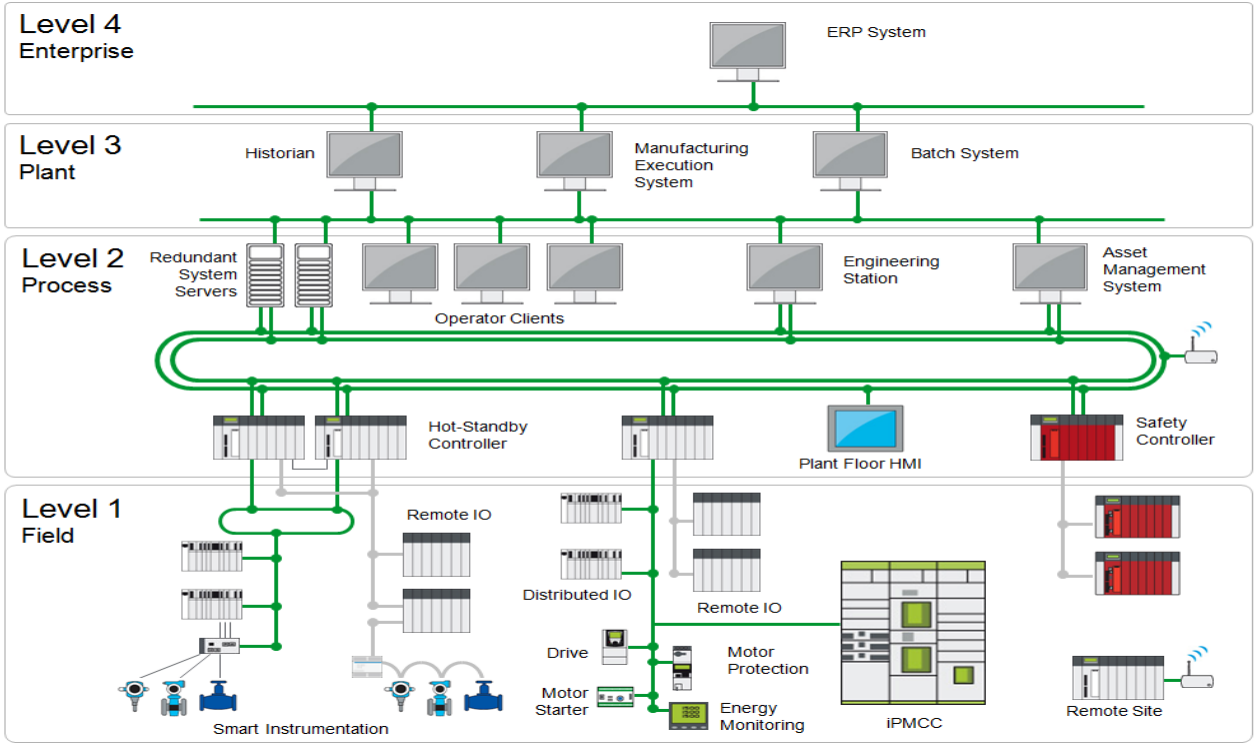
Exemple de solutions déployées en environnement industriel

Principaux vecteurs d'intrusion



Notre offre Cybersécurité industrielle

1. Audit & évaluation
2. Conception
3. Intégration
4. Exploitation MCS
5. Formation



niveaux selon le modèle ISA95

Notre offre Cybersécurité industrielle

1 Audit & évaluation

2 Conception

3 Intégration

4 Exploitation MCS

5 Formation

	Production maintenance	Ingénierie, travaux neufs	Administration RSSI
SENCYB (1j) Sensibilisation du personnel. Les bonnes pratiques au sein de l'entreprise	☑	☑	
CYBINDUS (3j) Spécificités et protection des systèmes de contrôle-commande industriels	Labellisée ANSSI	☑	☑

REX formation CYNBINDUS (labellisée SecNumEdu)

- La formation répond bien aux attentes sur la réglementation (LPM, directive NIS)
- Les acteurs IT et OT sont satisfaits des TP et notamment le cas d'usage de sécurisation d'une installation industrielle
- Les acteurs IT et OT sont satisfaits du niveau de compétences des formateurs

- Les intégrateurs de systèmes veulent aller plus loin dans l'implémentation des solutions => nouveau module CybExpert de 3 jours à partir de Juin 2019
- Bémol fait sur le fait d'aborder assez peu l'IEC 62443 versus le guide des mesures détaillés de l'ANSSI

Console de maintenance Sécurisée Cybertec Win10

Console de maintenance sécurisée

Vous souhaitez

- Une solution de durcissement de vos postes de maintenance
- Une solution validée par le constructeur sur ses logiciels catalogue

Notre solution

Console de maintenance sécurisée CyberTec

- Paramétrage du système d'exploitation selon le guide CIS et les recommandations de l'ANSSI
- Validation Schneider sur les logiciels de programmation au catalogue (Unity Pro, Vijeo Designer, …)
- Adaptation aux besoins client (logiciels tiers, politique de sécurité…)

Description	Politique Operateur	Politique Administrateur
Périphériques USB, Wifi, Bluetooth, lecteur CD, port parallèle LPT	INTERDIT	AUTORISE
Clef USB dédiée et drivers validés (identifiée par numéro de série)	AUTORISE	AUTORISE
Exécution d'application depuis la clef USB	INTERDIT	AUTORISE
Exécution d'application non présente dans la liste blanche	INTERDIT	AUTORISE
Modification, mise à jour des applications installées	INTERDIT	AUTORISE
Modification des fichiers système Windows	INTERDIT	AUTORISE
Connexion internet	INTERDIT	AUTORISE
Modification des politiques de sécurité	INTERDIT	AUTORISE
Surveillance d'applications (HIPS)	ACITVE	ACTIVE
Chiffrement de surface du disque dur	ACTIVE	ACTIVE

REX Console de maintenance Cybertec

- La validation de l’ensemble des logiciels Schneider pour automatismes de gamme actuelle et ancienne
- Le niveau de sécurité jugé très satisfaisant par des acteurs majeurs de la Cybersécurité
- L’adoption d’un tel outil par les utilisateurs au regard des risques cyber (fini le PC perso avec accès internet)

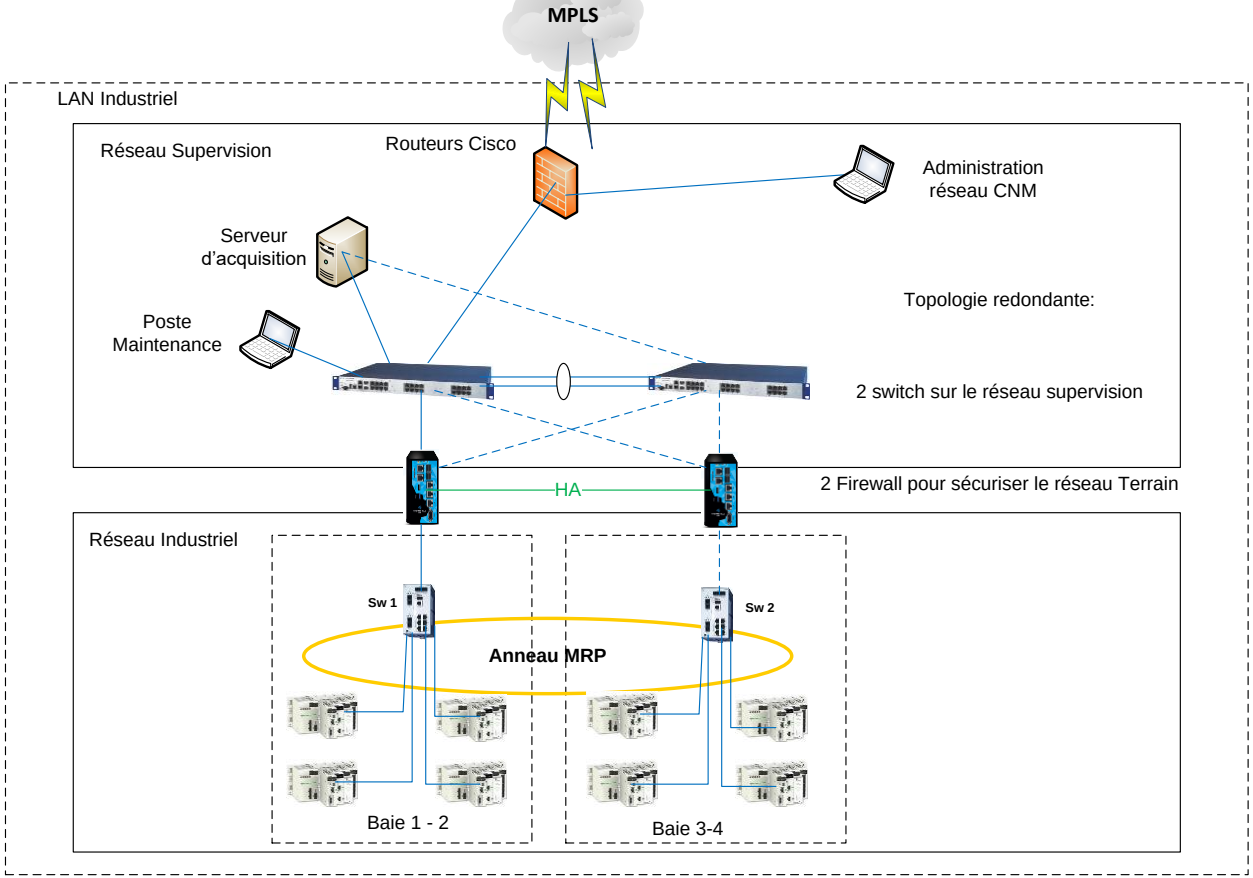
- L’opérateur de maintenance souhaite encore conserver sa propre machine car il a sa propre version des logiciels, ses patchs, ses drivers, … et tout en étant admin de son poste !
- Difficulté d’imposer de passer par le bureau de la DSI pour récupérer une console
- Qui achète la console ? Le client final et il la met à disposition des intervenants extérieurs ? Les intervenants extérieurs directement ? Sur le budget du projet (non prévu initialement) ?

Pare-feu SNi40 : Adapté aux contraintes industrielles

- STORMSHIELD : Une expérience de 15 ans dans la cyber sécurité réseau
- Développé dans le cadre du projet NG-IUTM, partenariat Stormshield/Schneider Electric commandité par l'ANSSI
- Certifié et Qualifié CSPN
- Une formation et certification unique IT/OT
- Solution de détections des vulnérabilités réseaux
- DPI des Protocoles Industriels:
  - Modbus, S7, OPC UA, IEC104, OPC DA, Ethernet/IP

Depuis Mai 2016 :
+ de 20 OIV équipés et formés

Exemple d’architecture : Sécurisation Interconnexion IT/OT



REX segmentation et implémentation routage / filtrage protocoles industriels

- Facilité de mise en œuvre
- Réactivité du support lorsqu'on poste un ticket
- Prix vs performance et nombre de ports
- Filtrage des protocoles industriels
- L'aspect certification/qualification ANSSI

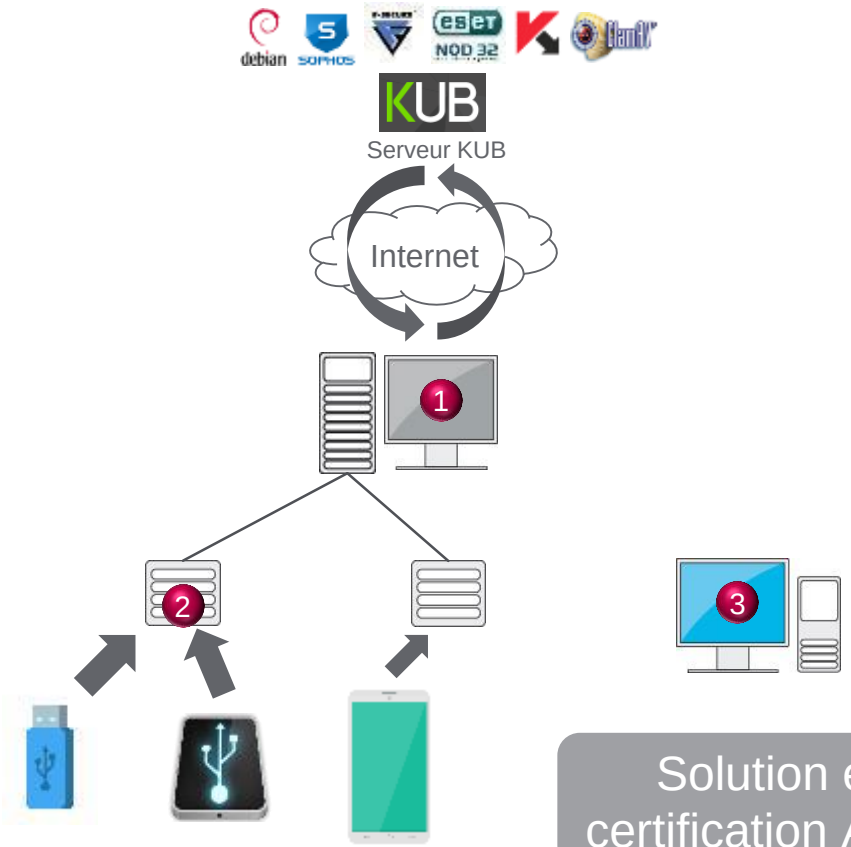
- Formation / Transfert de compétences (monitoring via un outil d'asset management qu'un des parefeux est HS et pas uniquement via les logs des parefeux)
- Filtrage des protocoles industriels sur le modèle IT => incompréhension
- Prix de la maintenance => impensable de prévoir 20% d'OPEX pour un industriel (un automate peut fonctionner pendant 20 ans sans s'arrêter et sans mise à jour)

Station de décontamination USB multi-antivirus

- Sophos
- F-Secure
- Eset
- Kaspersky
- ClamAV

KUB est livré avec 2 moteurs au choix
En option : 1 ou plusieurs moteurs supplémentaires

Station de décontamination USB multi-antivirus



1 Serveur d'administration :
- Virtual appliance
- Téléchargement et déploiement des mises à jour
- Paramétrage des stations (réseau, texte affiché…)
- Reporting

2 Station KUB :
- Communication sécurisée avec le serveur (SSL)
- Possibilité d'installation sans réseau
- Scan automatique ou sur action utilisateur
- Nettoyage

3 Agent Workstation Protect :
- Protection contre l'insertion de média non analysé
- Agent validé **à partir de Win XP SP2**
- Connecté ou non au serveur d'administration

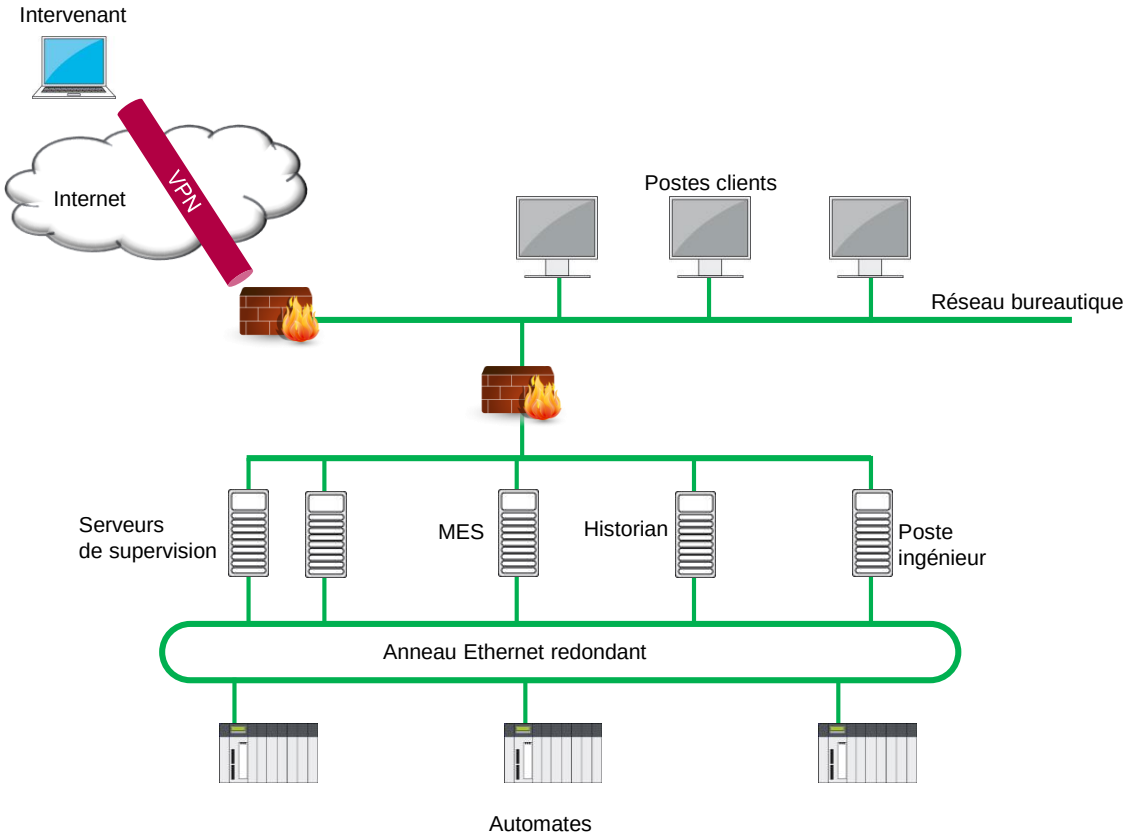
Solution en cours de certification ANSSI (CSPN)

REX station de décontamination USB

- Le côté concret, très utile pour faire de la pédagogie
- La réactivité du support lorsqu'on poste un ticket
- Le prix par poste dans la version avec l'agent (nombre d'agents illimité)
- L'aspect certification ANSSI en cours

- Le mode POC dans la version avec Agent car il existe une grande hétérogénéité de postes côté OT (tout le monde est admin de son poste, etc…)
- McAfee non disponible

L’accès à privilèges sécurisé iPAM Wallix / Schneider Electric



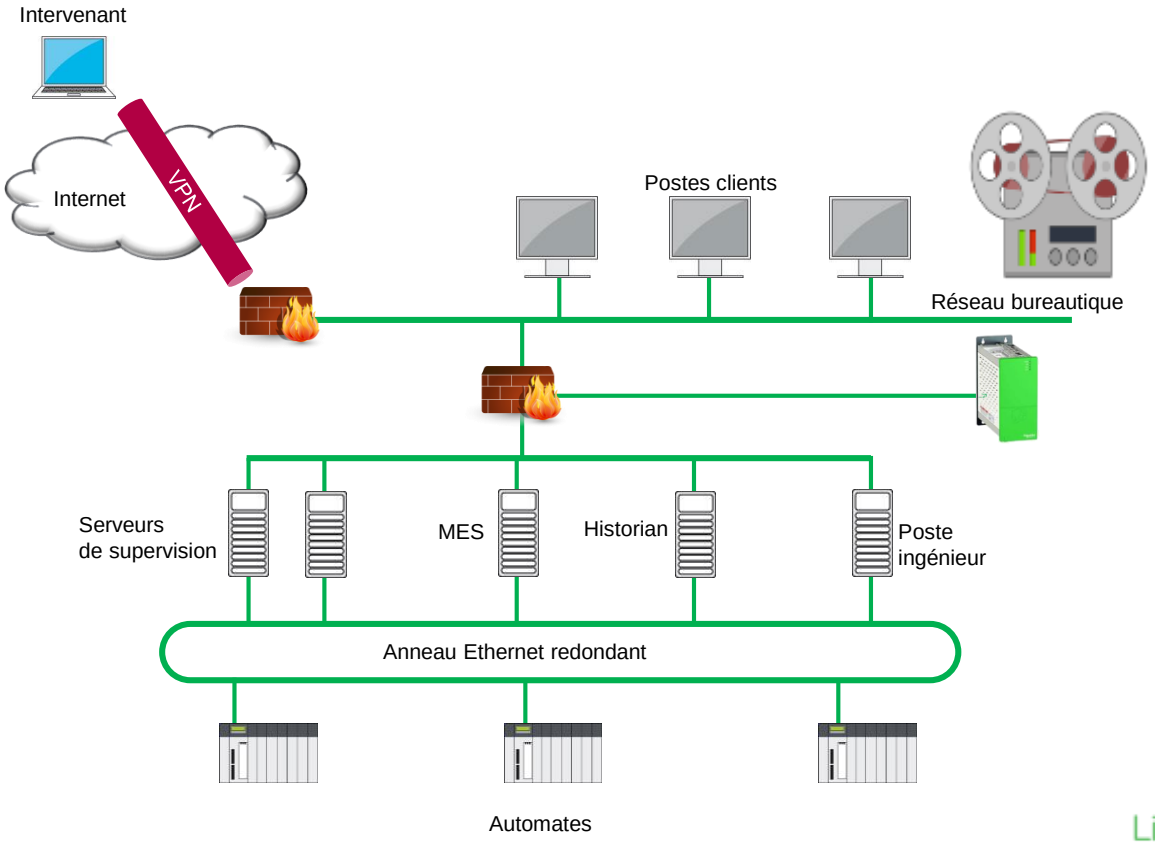
L’accès à privilèges sécurisé iPAM Wallix / Schneider Electric

Déroulement de l’attaque

- Un **ex-employé** de la société ayant installé le système SCADA de la centrale de traitement des eaux usées de la Maroochy Shire a postulé pour un poste au sein de cette dernière.
- Sa demande d’emploi ayant été refusée, il a décidé de **se venger** des 2 employeurs en prenant le contrôle de la station. Il a donc **volé un équipement radio de son employeur** et a envoyé des commandes au système de contrôle qu’il a aidé à installer.
- Les commandes envoyées lui ont permis de déverser des centaines de milliers de litres d’eaux usées.
- **Sa connaissance du processus industriel** lui a permis de faire croire que ses actions étaient dues à un dysfonctionnement du système.

Source : CLUSIF

L’accès à privilèges sécurisé iPAM Wallix / Schneider Electric



Traçabilité

Contrôle d’accès

Contrôle des actions

WALLIX
TRACE, AUDIT & TRUST

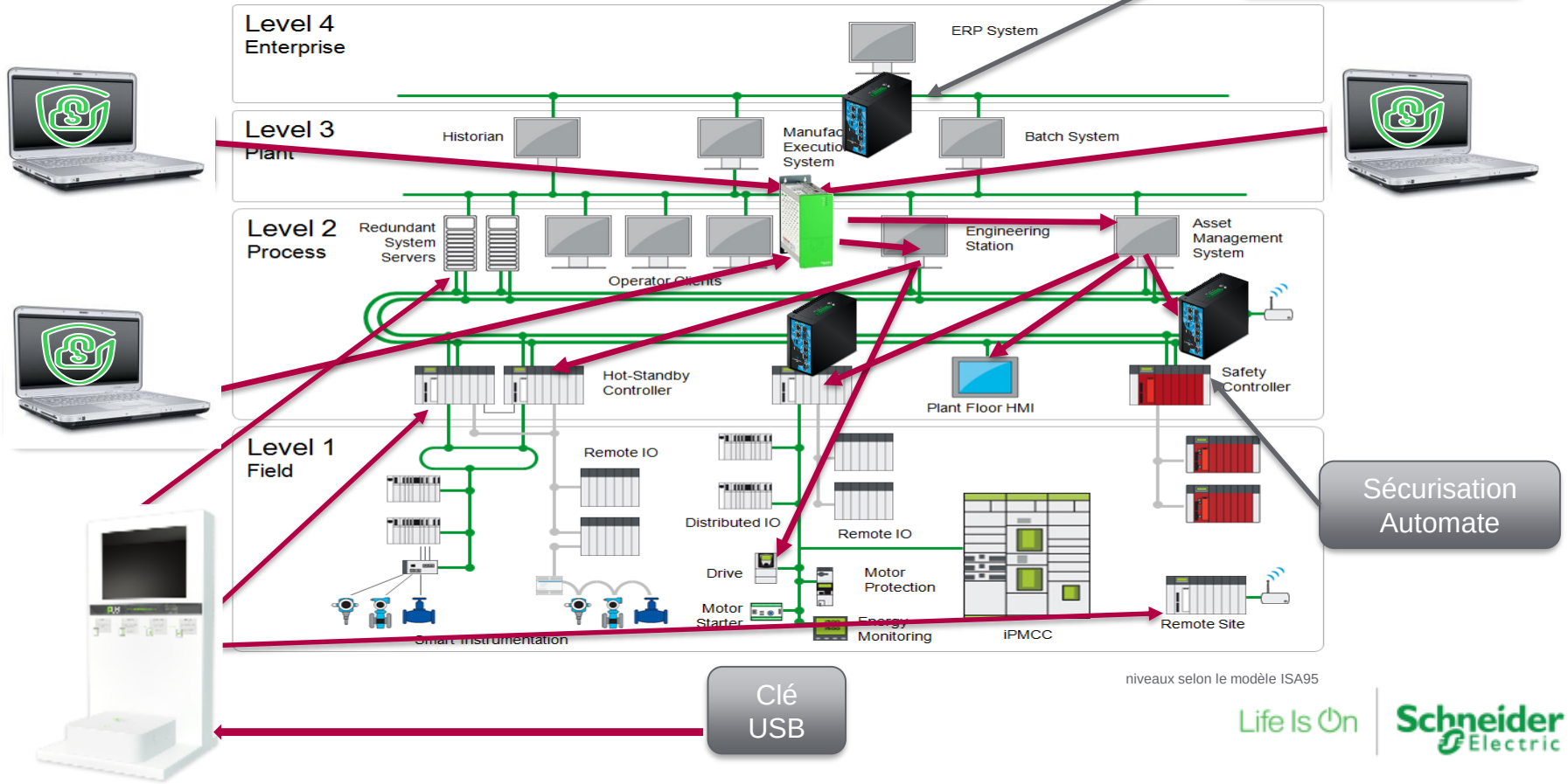
Life Is On Schneider Electric

REX implantation Bastion

- La solution « allégée » IPAM pour l'OT (licence de 5 postes seulement)
- Le mode intégré sur une seule machine et sans agent
- La réactivité du support lorsqu'on poste un ticket
- L'aspect certification/qualification ANSSI

- Le rebond sur une machine tiers qui ne peut pas avoir tous les outils de l'opérateur qui se connecte à distance (multiplicité des stations ingénieurs)
- L'implémentation d'un bastion implique souvent de repenser l'architecture ➔ crainte des décideurs de démarrer un tel projet

Principaux vecteurs d'intrusion : nos solutions



Life Is On Schneider Electric

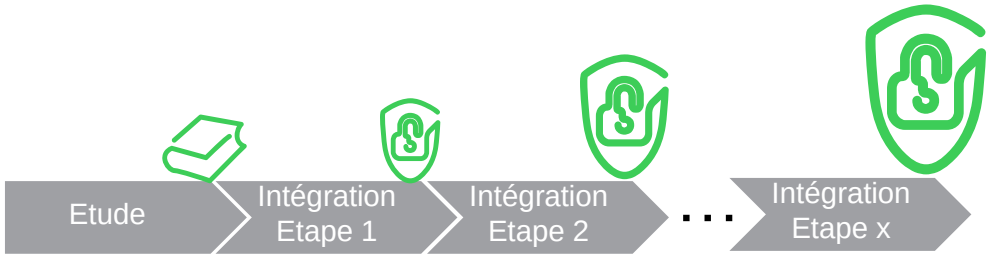
Une démarche échelonnée, un partenariat dans le temps

1 phase d'étude

- Evaluation du niveau de sécurité actuelle
- Identification des risques cyber
- Définition des objectifs de sécurité
- Définition de l'architecture sécurisée
- Définition d'étapes cohérentes

x phases d'intégration

- Fourniture de solutions de sécurité
- Intégration
- Configuration de la sécurité
- Formation
- **Maintien des performances du système**



Life Is On | Schneider Electric

FR-NEC@schneider-electric.com