UN SOC CONVERGÉ

LA RÉPONSE À UNE MENACE CYBER GLOBALE QUI IMPACTE LE PAYSAGE INFORMATIQUE ET INDUSTRIEL ?

INDUSTRIAL CYBERSEC FORUM

LYON 28 NOVEMBRE 2023

Sacha Hilic
General Manager
IMS Networks

Stéphane Rabette
Engineering Lead EU
Secureworks

Agenda

1. **L'état de la menace Cyber dans les environnements industriels**
2. **Quelles solutions pour endiguer le risque?**
3. **Les points clés pour une surveillance IT/OT convergée**

La Cybersécurité dans la perspective de l'industrie 4.0

Les évolutions

Edge Computing 	La continuité d'activité et le volume croissant de données à traiter font émerger des infras de Edge Computing (« OnSite »)
Analyse de données et intelligence artificielle 	Le besoin de stocker ces données volumeuses et de croiser ces données multi domaines métiers dans une logique de décisionnel étendu voire d'intelligence artificielle se font au travers de solutions embarquées au sein des infras cloud (« OnCloud »)

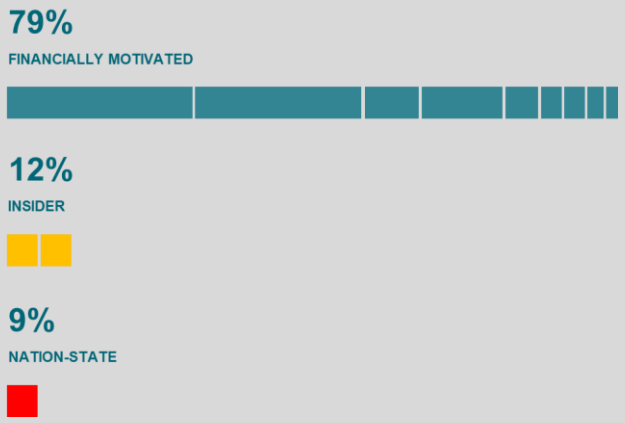
Les conséquences

Architecture intégrée IT & OT 	La nécessité de connectivité entre systèmes IT & OT redéfinissent le paysage et les architectures système et réseau avec des enjeux de convergence des protocoles, de standardisation de la donnée, d'alignement des identités et des accès, ...
Cybersécurité convergée IT & OT 	La cybersécurité IT & OT ne peut donc plus être vu d'une manière séparée. Il est nécessaire d'avoir une politique globale et d'embarquer les industriels dans cette démarche de résilience

L'Etat de la menace Cyber dans le monde OT

79%

of incidents we investigate are financially motivated



1. **1400 engagements IR mais < 1% concerne réellement l'OT**
2. **OT = acteurs étatiques / infrastructures critiques / géopolitique**
3. **… mais un shift vers des attaques OT plus opportunistes**
4. **Accès initial : sauf accès physique, le point d'entrée reste l'IT,**
5. **Sureté / Sécurité: les brides physiques des process industriels**

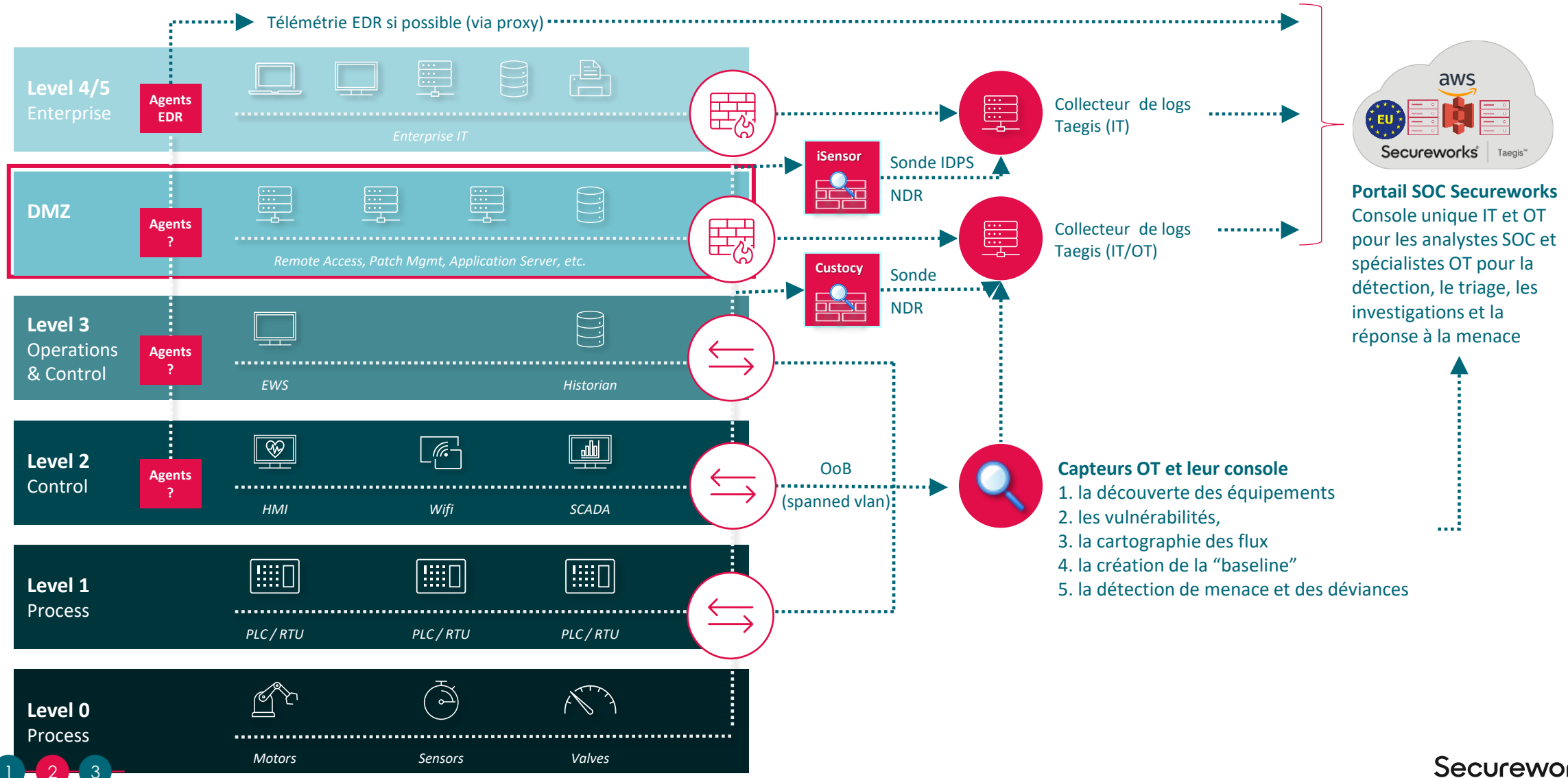
La réalité dépasse souvent la fiction

- ✓ Utilisation de KeyGenerator pour activer Windows
- ✓ Installation du Sopcast (P2P TV Streaming) couplé à un routeur Internet « sauvage » pour regarder du contenu inapproprié depuis une sous-station Electrique
- ✓ Des sous-traitants qui se connectent depuis des laptops compromis ou utilisant des clés USB infectés pour les maj OT
- ✓ L'isolation par un « non expert » du process industriel d'une machine Windows 2000 qui contrôle la ventilation d'un local abritant 100'000 poulets …

Retour d'expérience d'une crise dans le monde industriel

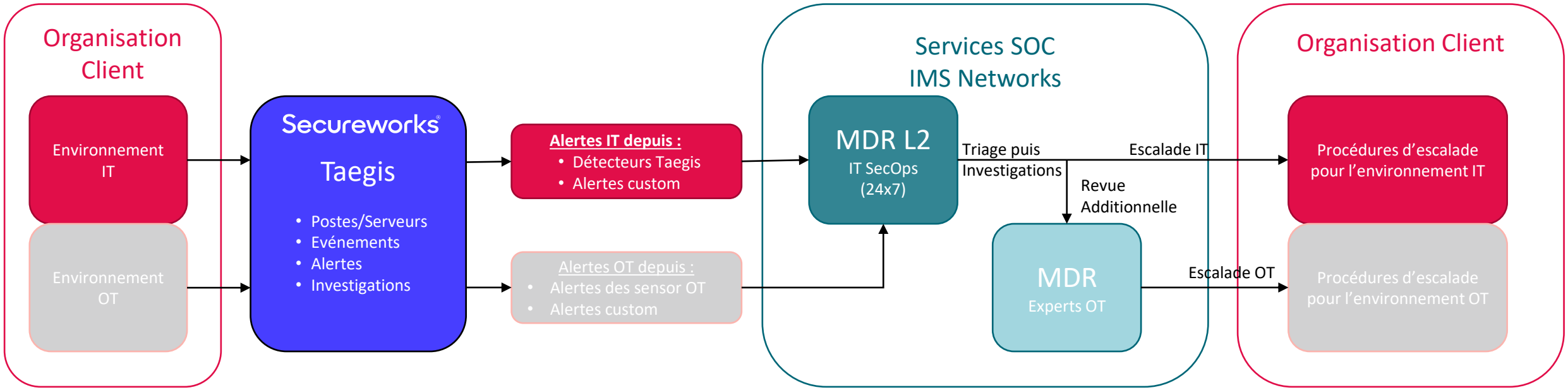
Grand Groupe Français Env. 2,5 M€ de CA 13000 collaborateurs 25 filiales	15 jours sans logistique	Reconstruction de toutes les briques d'infra Back-up & restore SI Nettoyage des réseaux
Attaque Revil un 31 mars à 04h du matin motivée par la rançon	1 mois sans production + 1 mois avec une prod. dégradée + perte quelques docs critiques	Difficultés sur le SI Industriel non maîtrisé par la DSI
Tous les env. windows infectés et cryptés par le ransomware Sodinokibi	1 mois ½ sans R&D	Roadmap Cyber tenant compte du SI Industriel avec implication du CoDir

Quelle architecture pour une surveillance convergée ?



1 2 3

Le volet OT du SOC – compétences et process spécialisés



Experts OT

- ✓ Expertise SOC L2+/L3
- ✓ Création des investigations depuis les alertes OT prétriées – ajout du contexte, voire accès aux console OT dans l'environnement du client
- ✓ Suggestion d'un plan de remédiation basé sur les bonnes pratiques du monde OT
- ✓ Escalade vers les interfaces OT nommée du client au besoin pour validation des actions

NIS2 : leviers, impacts ?

CNTL NO.	CONTROL NAME	INITIAL CONTROL BASELINES		
		LOW	MOD	HIGH
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
CA-7	Continuous Monitoring	CA-7 (4)	CA-7 (1) (4)	CA-7 (1) (4)
IR-4	Incident Handling			
IR-5	Incident Monitoring			
IR-6	Incident Reporting			
IR-7	Incident Response Assistance			
IR-8	Incident Response Plan			

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 6 – Timely response to events (TRE)				
SR 6.1 – Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
SR 6.2 – Continuous monitoring		✓	✓	✓

Etes-vous concerné par NIS2 ?

Les articles importants pour l'OT (assez vague pour une cible OT)

- ✓ Article 21 « Appropriate Level of Security »
  - S'appuie largement sur le référentiel ISO27001
  - Réduire la surface d'attaque; Utiliser du «x» DR
- ✓ Article 23 « Report Incident in 24h »
  - Définition du Plan de réponse sur Incident
  - Le pratiquer

Anticiper !

Utiliser NIS2 comme un levier de votre programme OT !!

Applications des standards

- ✓ **IEC62443** (complet …et très complexe)
  - Etablissement d'un programme (2-1)
  - Prérequis et exigences de sécurité des systèmes (3-3)
  - Contrôles de sécurité adaptés aux exigences (SL0 to SL3)

- ✓ **NIST CSF** (SP800-82r2, r3 en draft)
  - "Guide to Industrial Control Systems (ICS) Security"
  - Accessible gratuitement
  - Guide très riche sur les bonnes pratiques OT
  - Liste des contrôles de sécurité adaptés à l'OT

Points clés de l'approche d'un SOC convergé

1. **La menace Cyber sur les environnements industriels est bien réelle et concerne une organisation sur cinq**
   - ✓ Le principal vecteur de menace pour les environnements OT reste l'IT
   - ✓ Les attaques sont d'abord opportunistes (accès initial) pour ensuite devenir plus ciblées (adaptation aux process indus)

2. **La transformation digitale de l'industrie 4.0 impose une surveillance convergée et globale qui intègre IT et OT**
   - ✓ Le risque s'accroit avec la technologie IT « connectée » mise en œuvre pour satisfaire les besoins métiers et les process
   - ✓ Une surveillance 4.0 qui impose des moyens nouveaux (sensors OT, compétences OT, process triage/investigation SOC)
   - ✓ La convergence des cultures IT et OT impose une gouvernance unifiée

3. **Ajouter l'OT dans un SOC IT impose des technologies, des process et des compétences spécifiques**
   - ✓ Le dernier étage d'une fusée qui en a 6, c'est un programme complet qu'il faut construire en exploitant le leviers NIS2
   - ✓ L'analyse de risque est clé, le modèle opérationnel l'est tout autant, les deux étant spécifiquement adaptés
   - ✓ Quelques points importants :
     - Sécuriser l'accès distant à l'infrastructure OT
     - Gestion « pragmatique » des vulnérabilités et exploitation de sonde IPS/NDR pour limiter l'exposition
     - Segmentation/Isolation en fonction de la matrice assets/flux

La proposition de valeur IMS en environnement industriel

- Surveillance convergée 24x7 de la menace IT & OT
  Détection, investigation, et réponse collaborative
- Intégration des outils de détection spécialisés OT
- Construction collaborative des processus spécifiques
  de réponse, d'escalade de de reporting pour l'OT
- Visibilité de la menace IT et OT dans une console unique
- Réponse sur incident, gestion de crise
  Services de consulting permettant d'améliorer la cyber résilience

Secureworks

70%

des organisations auront fait converger leurs fonctions de sécurité dans les environnements IT et OT d’ici 2025.

Gartner Market Guide for OT, August 2022

ims NETWORKS

engagés pour un monde
numérique plus sûr

TOULOUSE – PARIS – CASTRES – BORDEAUX – SOPHIA ANTIPOLIS

contact@imsnetworks.com
+33 (0)5 63 73 50 13
www.imsnetworks.com