OT : MENACES CYBER ET RÉPONSES

CONFÉRENCE CLUSIF

23 JUIN 2022

CONSIDÉRER UNE INTERCONNEXION IT/OT

Théo GISSINGER-SCHUMANN (EIFFAGE ÉNERGIES SYSTÈMES)

INTERVENANT

Théo GISSINGER-SCHUMANN

Expert en cybersécurité des systèmes industriels

EIFFAGE ÉNERGIE SYSTÈMES

LE BESOIN D'INTERCONNEXION IT/OT

Partager	Optimiser	Exploiter	Maintenir
- Les ressources, processus, méthodes - Collaboration entre les équipes IT/OT - Opportunités technologiques (5G,IIoT)	- Amélioration de la performance - Statistiques - Analyses temps-réel - IA & ML - Facturation	- Valoriser les données métiers - Standardiser, collecter, analyser, croiser les données - Développer de nouveaux services	- Amélioration de la visibilité et de la surveillance - Maintenance prédictive - Service SOC/CSIRT

La question n'est plus « allons nous le faire ?» mais plutôt « quand et comment le sécuriser ? »

FOCUS CYBERSÉCURITÉ

Incidents IT plus fréquents et incidents OT plus destructeurs

(Interconnexion IT /OT)

Augmentation de l'exposition du réseau OT

Augmentation de la surface d'attaque

De nouveaux risques à prendre en compte

Incidents OT plus fréquents et toujours autant destructeurs

FOCUS CYBERSÉCURITÉ

Vecteur/Attaque en ligne (rebond depuis l'IT)

Exploit. vulnérabilité composant exposé → Vraisemblance élevée

Déni de service, chantage → Vraisemblance élevée

Introduction dans le réseau OT via rebond → Vraisemblance élevée

Espionnage, vol, C&C, APT → Vraisemblance élevée

Constat : attaque ciblée ou non, peu de prise de risques, budget et motivation minime

Vecteur/Attaque hors ligne

Accès physique → Vraisemblance faible

Piégeage matériel → Vraisemblance faible

Compromission du personnel → Vraisemblance faible

Naïveté et mauvaises habitudes → Vraisemblance faible

Constat : attaque majoritairement ciblée qui implique un budget et une motivation moyenne

Près de ¾ des vulnérabilités des systèmes industriels sont exploitables à distance

FOCUS CYBERSÉCURITÉ

Conclusion : l'interconnexion IT/OT implique une prise en compte supplémentaire dans l'approche cybersécurité des systèmes concernés

- Analyse de risque
- Exposition et criticité des composants, fonctions, données
- Mesure de protection
- Mesure de détection
- **Conformité réglementaire**

La cybersécurité est-elle toujours intégrée en amont des projets d'interconnexion entre IT et OT ?

LA BONNE APPROCHE

1

RASSEMBLER LES ACTEURS

Direction, métiers, DSI/RSSI

2

CONSOLIDER LE BESOIN

QQOQCCP

3

CONSTRUIRE UNE SOLUTION

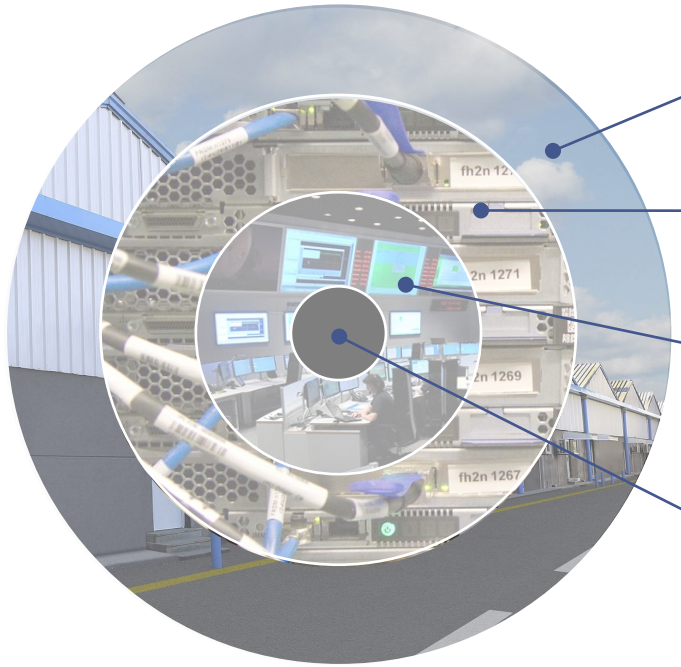
Exigences fonctionnelles et de sécurité

4

PILOTER & MAINTENIR

Surveillance, évolution

DÉMARCHE CYBERSÉCURITÉ



Défense en profondeur

Maintenir et surveiller

Mise à jour, HIPS/NIPS, SIEM, SOC
Gestion des équipements

Segmenter & filtrer

Cloisonnement des réseaux en zones
Filtrage des protocoles

Durcir et contrôler

Durcissement des équipements et configurations
Activation des fonctions de sécurité (AC, AV)
Authentification, chiffrement

Limiter l'exposition

Restreindre les composants et services exposés
Restreindre les données externalisées

SÉCURITÉ DES INTERCONNEXIONS

#1 PASSERELLE UNIDIRECTIONNELLE

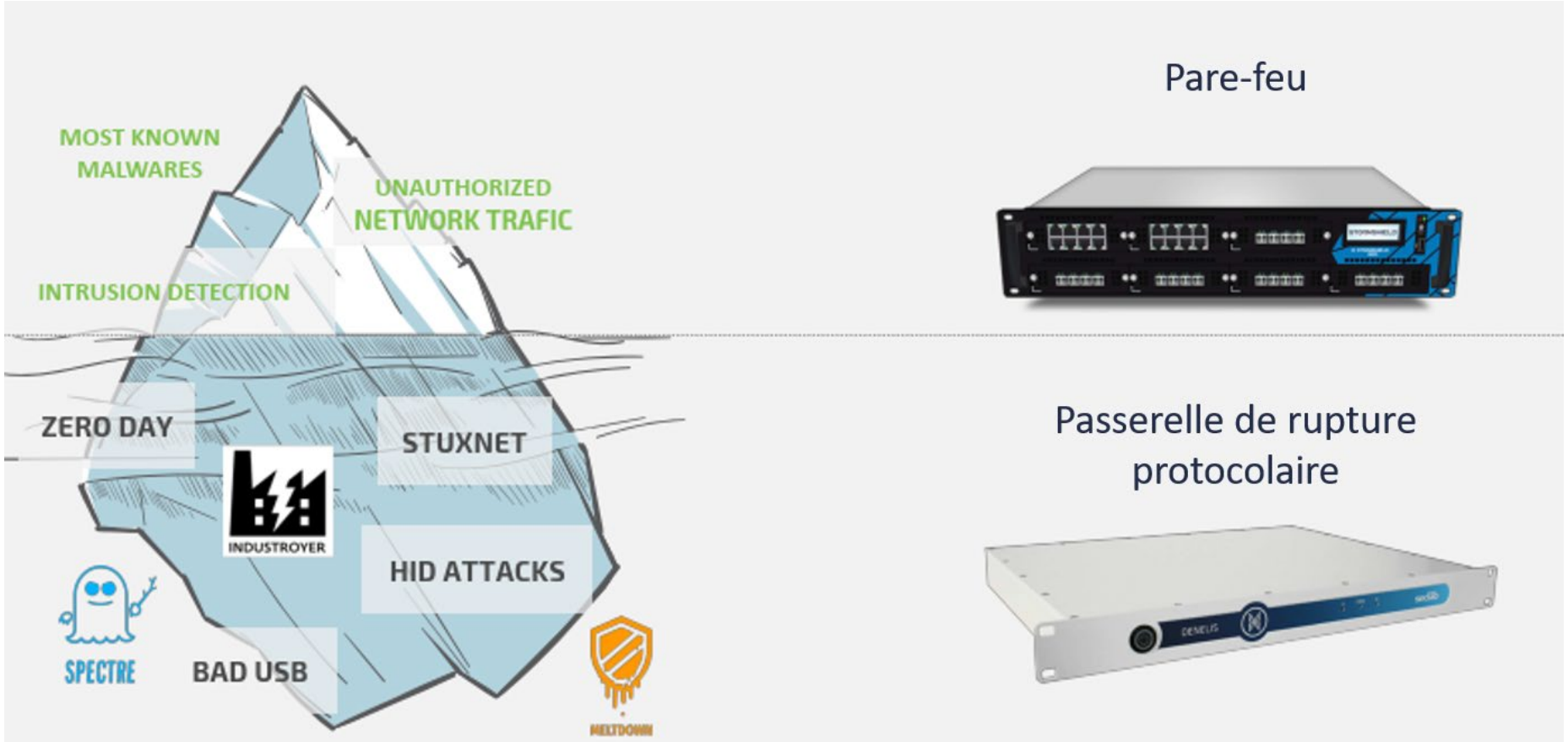
SÉCURITÉ DES INTERCONNEXIONS

#1 PASSERELLE UNIDIRECTIONNELLE 

#2 PASSERELLE DE RUPTURE PROTOCOLAIRE 

#3 PARE-FEU (NGFW, UTM) 

SÉCURITÉ DES INTERCONNEXIONS



SÉCURITÉ DES INTERCONNEXIONS

#1 PASSERELLE UNIDIRECTIONNELLE 

#2 PASSERELLE DE RUPTURE PROTOCOLAIRE 

#3 PARE-FEU (NGFW, UTM) 

Constat : Souvent des architectures « simples » impliquant une seule couche de protection type pare-feu ainsi que des échanges bidirectionnels

SÉCURITÉ DU SYSTÈME OT

01.
Sécurité du réseau
- Segmentation et filtrage
- Authentification sur le réseau
- Chiffrement des flux sensibles
- Interconnexion
- Télémaintenance

02.
Sécurité du système
- Administration sécurisée
- Gestion des comptes et droits
- Host-Based firewall
- HIPS / EDR / AC
- Durcissement OS et configs

03.
Sécurité du process
- Mécanisme de sécurité natif
- Cloisonnement
- Authentification préalable
- Limitation des commandes
- Authentification des flux

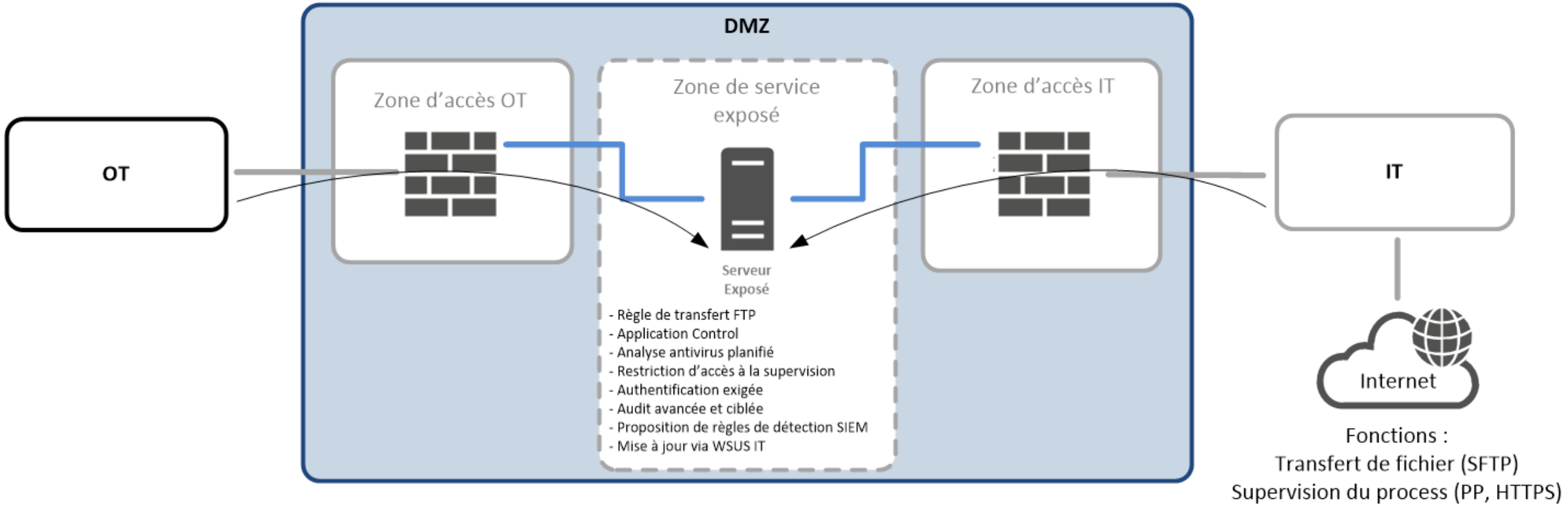
04.
Auditer & surveiller
- Stratégie d'audit de sécurité
- Export des évènements
- Monitoring système & réseau
- Sonde de détection OT
- Audit de sécurité, Pentest

05.
Exploiter & maintenir
- Règles de détection (SIEM)
- Surveillance et réaction (SOC)
- Gestion des vulnérabilités
- MCO & MCS
- Sensibilisation / simulation d'attaque

Gouvernance cybersécurité

Constat : Brique souvent manquante causant une faille dans la sécurité globale et augmentant le risque de rebond sur le réseau OT

CAS PRATIQUE



MERCI POUR VOTRE ECOUTE