Par webinaire Zoom

Lundi 10 mars

18h00 - 20h00

Cybersécurité industrielle

Garder une longueur d'avance sur les risques OT

Pierre-Marie LORE
Directeur cybersécurité
Framatome*u*

Organisateurs

Pr Ahmed Mehaoua
Université Paris Cité

Béatrice Laurent

Gérard Peliks

Pierre-Marie Lore

Depuis 2022
Directeur des services Framatome Cybersecurity

2019-2022
. Directeur cybersécurité Groupe RATP
#OT #CRISE #GOUVERNANCE #COMPLIANCE #ASSURANCE

2016-2019
. Chargé de mission sécurité des sources radioactives à l'ASN
#AIEA #INSPECTIONS #PROTECTION_PHYSIQUE

1999-2016
. Officier de marine
#NATO #COMMANDEMENT #SIC #GUERRE_ELECTRONIQUE

. MBA Management de la Cybersécurité
. Mastère Réseaux Telecom Sécurisés ETRS-CentraleSupélec
. Ecole Navale
. ANSSI

Membre de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information

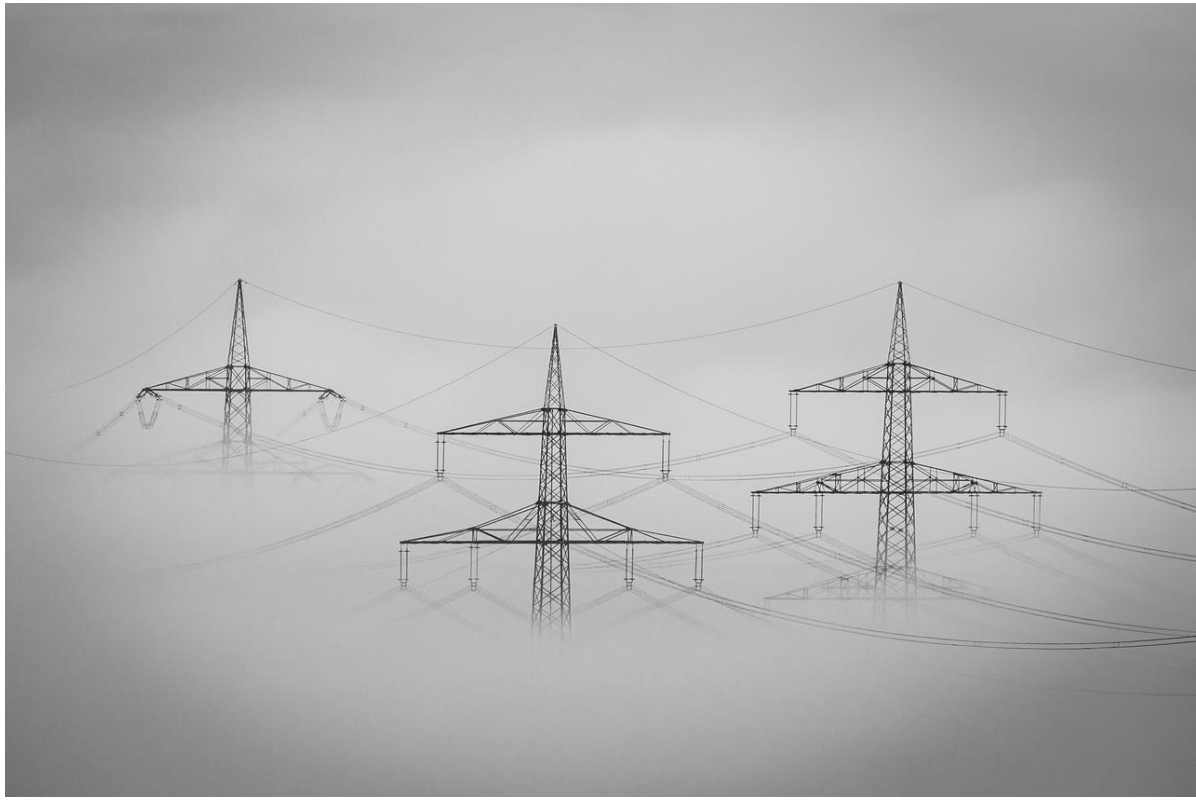
Cybersécurité des systèmes industriels: garder une longueur d'avance sur les risques OT

Systèmes industriels
. Non connectés?
. Ultra-spécifiques?
. Sûreté ou la sécurité?

Cybersécurité
. Centre de coûts?
. Que des spécialistes?

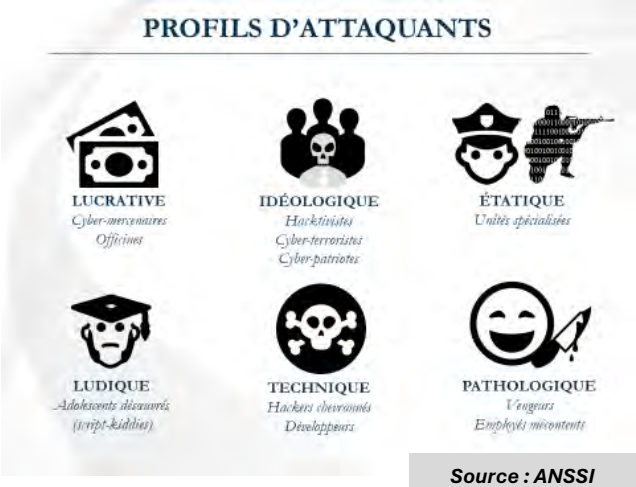
Une longueur d'avance
. L'innovation encore possible?
. Comment être sûr d'avoir anticipé?

De quoi doit-on se défendre?	01
Que doit-on protéger?	02
Des solutions pour prévenir et réagir	03
Orchestrer pour garder une longueur d’avance	04



De quoi doit-on se défendre?

01



Source : ANSSI

Menaces logicielles

- Malwares spécialisés ICS : Stuxnet, Triton, Industroyer
- Ransomwares ciblant l'OT : LockerGoga (Norsk Hydro), DarkSide (Colonial Pipeline)
- Exploits de vulnérabilités : Failles non corrigées sur SCADA, PLC, RTU, IHM

Menaces réseaux

- Man-in-the-Middle (MITM) : Interception des trames Modbus, DNP3, OPC UA
- Relecture/rejeu de trames : Modification des commandes envoyées aux automates
- Attaque sur protocoles industriels : Injection de fausses commandes sur Profibus, CAN
- Déni de service

Menaces physiques

- Intrusions physiques : Accès aux baies réseau, automates, salles de contrôle
- Attaques électromagnétiques : Espionnage ou perturbation des signaux (ex: TEMPEST)
- Sabotage matériel : Déconnexion physique, destruction d'infrastructures

Ingénierie sociale

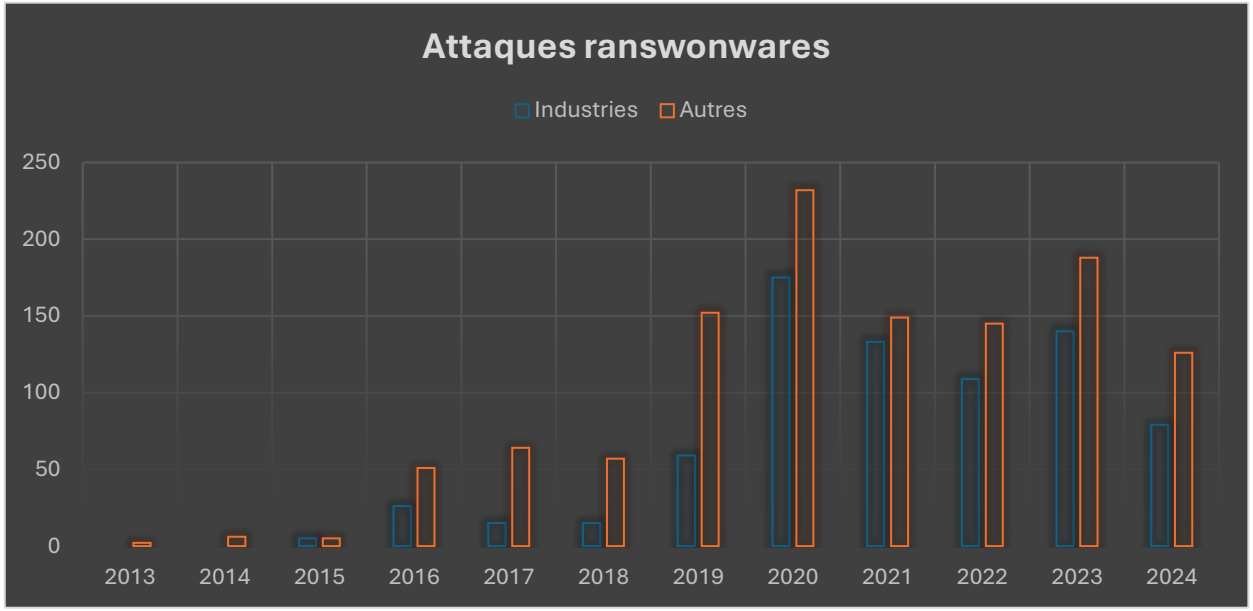
- Elicitation
- Phishing/Vishing

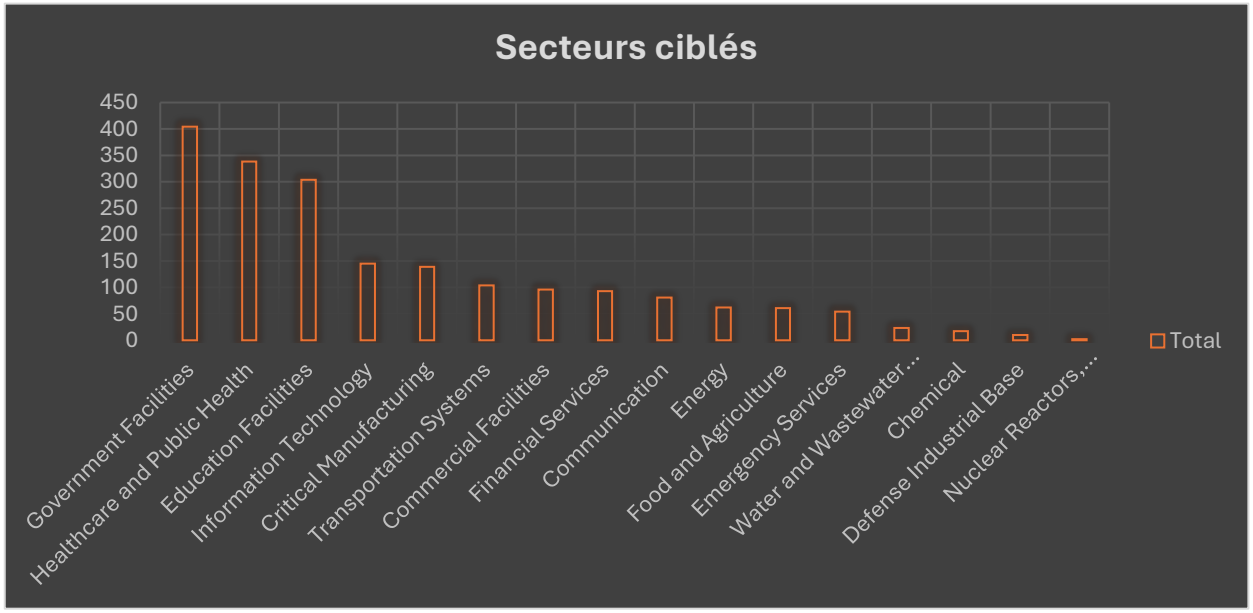
Bien souvent… des menaces hybrides

De quoi doit-on se défendre? 01

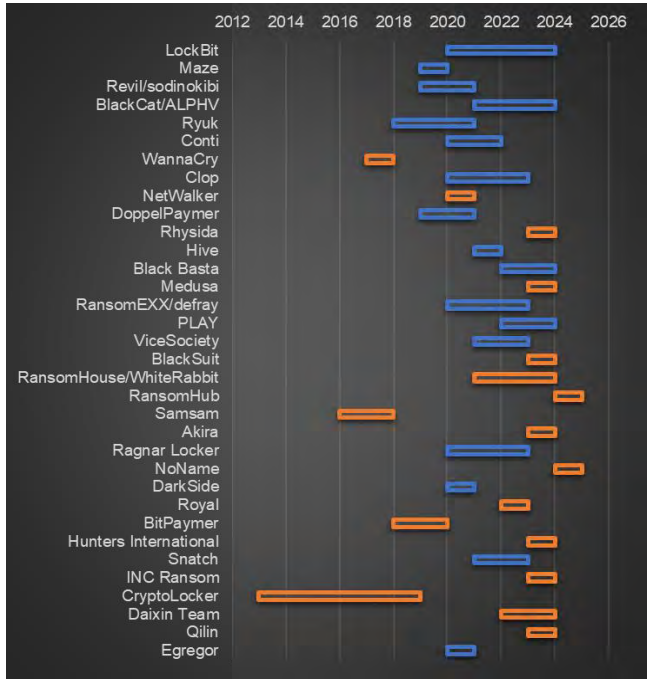
On observe un tassement des attaques visant les systèmes industriels

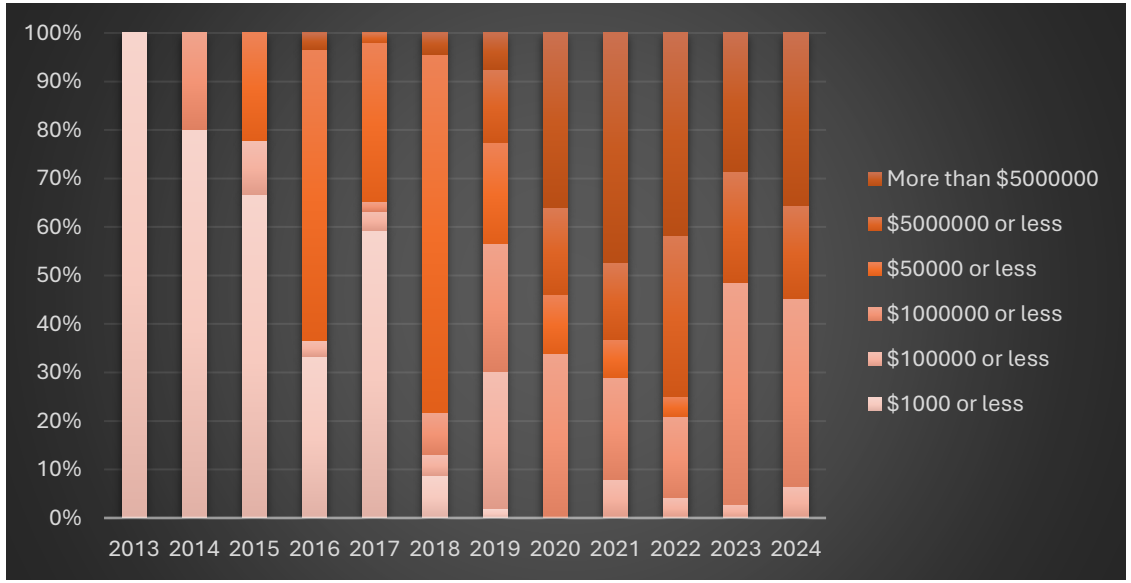
Toutefois:
. Une augmentation des attaques avancées (APT: advanced persistent threats), parfois en appui d'opérations plus vastes
. Le ciblage accru de petites installation (énergies renouvelables, assainissement)





Données: Temple University | Department of Criminal Justice | NOV 2024
"Critical Infrastructure Ransomware Attacks (CIRA) Dataset". Version 12.11


2012 2014 2016 2018 2020 2022 2024 2026
LockBit
Maze
Revil/sodinokibi
BlackCat/ALPHV
Ryuk
Conti
WannaCry
Clop
NetWalker
DoppelPaymer
Rhysida
Hive
Black Basta
Medusa
RansomEXX/defray
PLAY
ViceSociety
BlackSuit
RansomHouse/WhiteRabbit
RansomHub
Samsam
Akira
Ragnar Locker
NoName
DarkSide
Royal
BitPaymer
Hunters International
Snatch
INC Ransom
CryptoLocker
Daixin Team
Qilin
Egregor


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024
More than $5000000
$5000000 or less
$50000 or less
$1000000 or less
$100000 or less
$1000 or less

Que doit-on protéger?

02

Niveau 4 - Entreprise
Actifs: IT Corporate (messagerie, applicatif, web, etc)

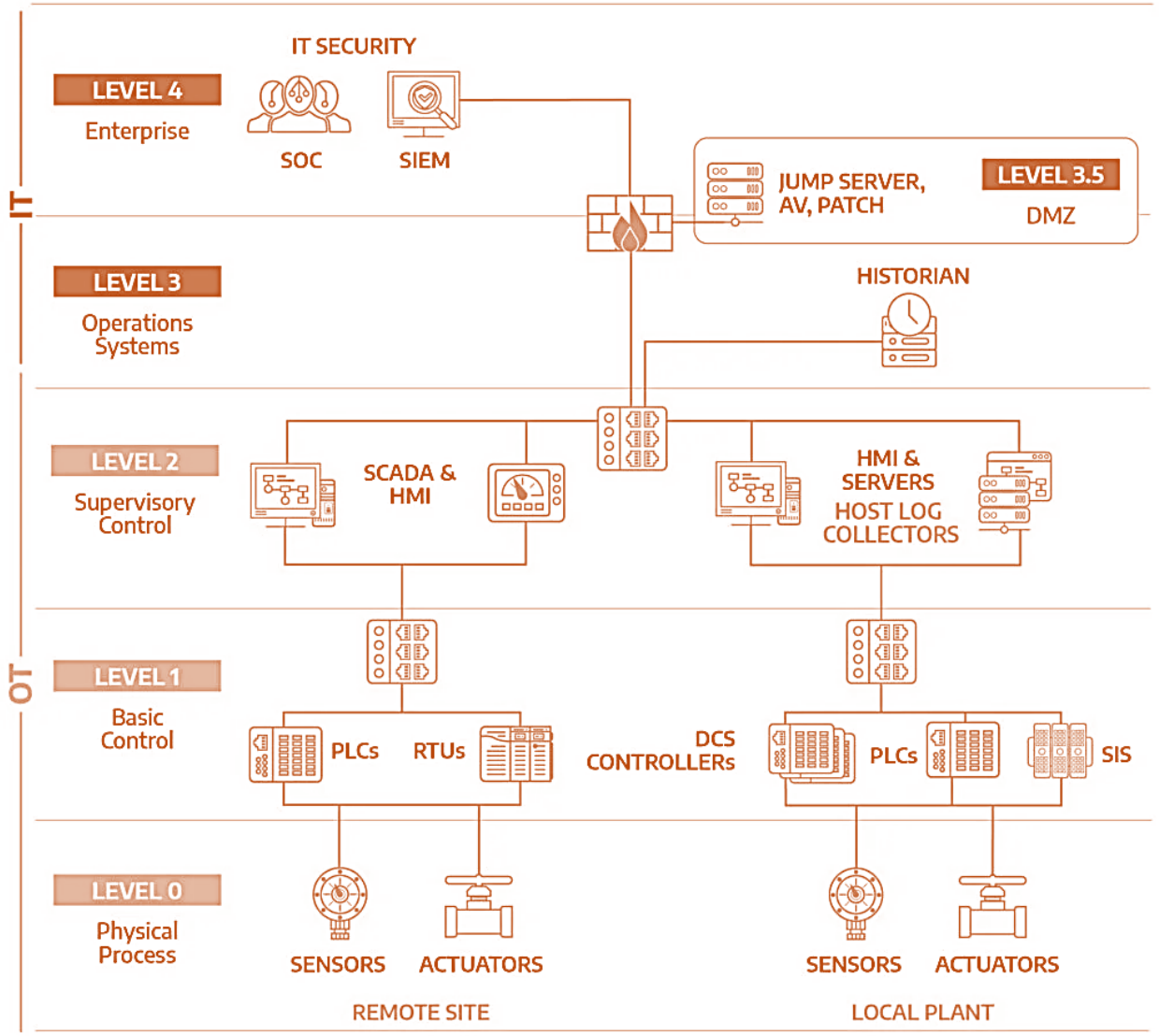
Niveau 3.5 – Zone Tampon (DMZ)
Actifs: proxies, pare-feu, antivirus pour les accès à distance

Niveau 3 – Gestion des opérations
Actifs: MES, historians, serveurs de logs, serveurs d'authentification, SIEM

Niveau 2 – Supervision
Actifs: SCADA, IHM, serveurs OPC, passerelles de communication

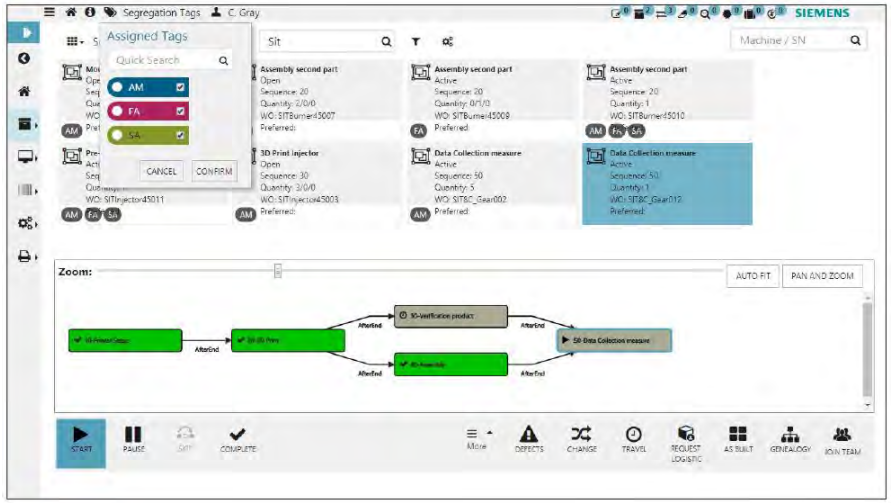
Niveau 1 – Contrôle de base
Actifs: DCS (Distributed Control Systèmes), PLC (Programmable Logic Controllers), RTU (Remote Terminal Units), I/O Modules.

Niveau 0 – Processus
Actifs: capteurs et actionneurs

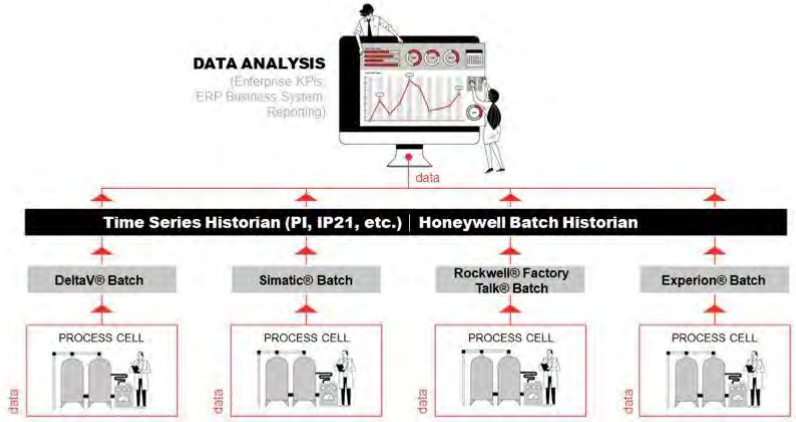


Que doit-on protéger?

02



MES Siemens SIMATIC
Source: Siemens



Historian Honeywell
Source: Honeywell

SCADA iFIX GE
Source: GE

DCS PCS 7 Siemens
Source: Siemens

RTU ROC800
Source: Emerson

PLC Modicon M241
Source: Schneider Electric

Thermocouples Omega
Source: Omega

Capteur capacitif VEGA
Source: Vega

Thomson - BSA Actuators
Source: Thomsonlinear

PArker
Source: Thomsonlinear

Des solutions pour prévenir et réagir 03

DESIGN SECURISE

▽

GESTION DES ACTIFS

▽

GESTION DES VULNERABILITES

▽

SURVEILLANCE ET DETECTION

Avant de parler des solutions, rappel de quelques bonnes pratiques

. Protection des accès
. Gestion des interventions
. Sauvegardes
. Mots de passe (renforcés, renouvelés)
. Inventaires
. Sensibilisations
. Périphériques amovibles
. Protection de l'information (et chiffrement)
. Communications sans-fil
. ...

DESIGN SECURISE

▽

GESTION DES ACTIFS

▽

GESTION DES VULNERABILITES

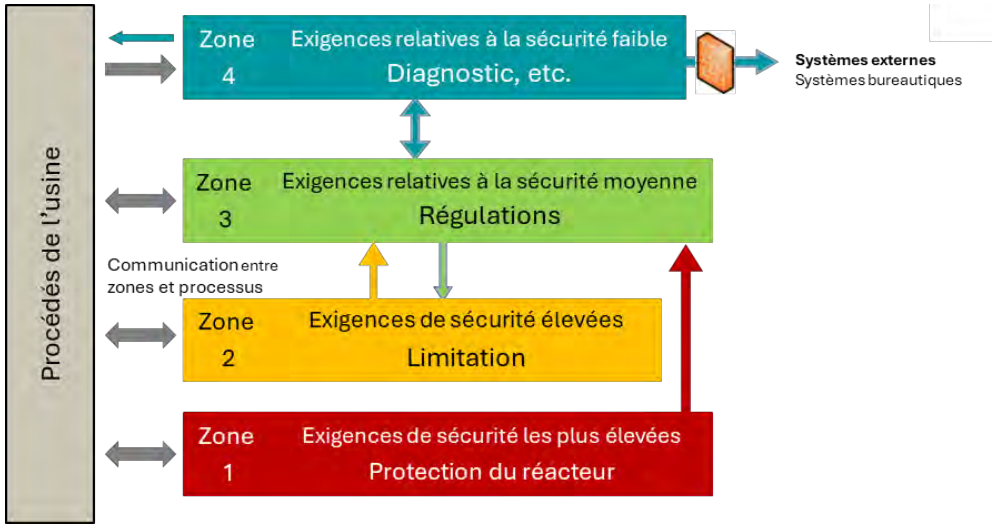
▽

SURVEILLANCE ET DETECTION

« By Design »

. Analogique ou numérique?
. CPU, GPU, ASIC, FPGA?
. Durcissement, whitelisting
. ...

Architectures



Solutions de sécurité

. Pare-feu industriels
. Bastions
. Sondes
. Antivirus/antimalware
. PKI, VPN
. ...

DESIGN SECURISE

▽

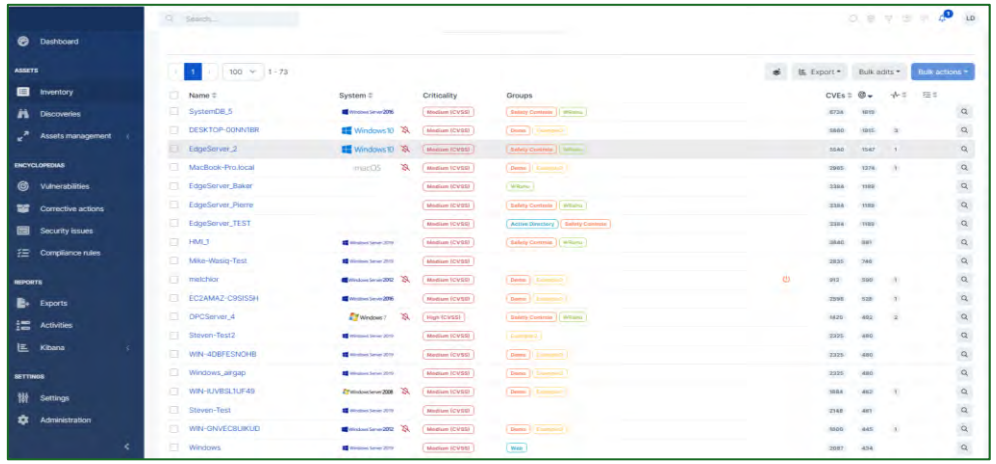
GESTION DES ACTIFS

▽

GESTION DES VULNERABILITES

▽

SURVEILLANCE ET DETECTION



DESIGN SECURISE

▽

GESTION DES ACTIFS

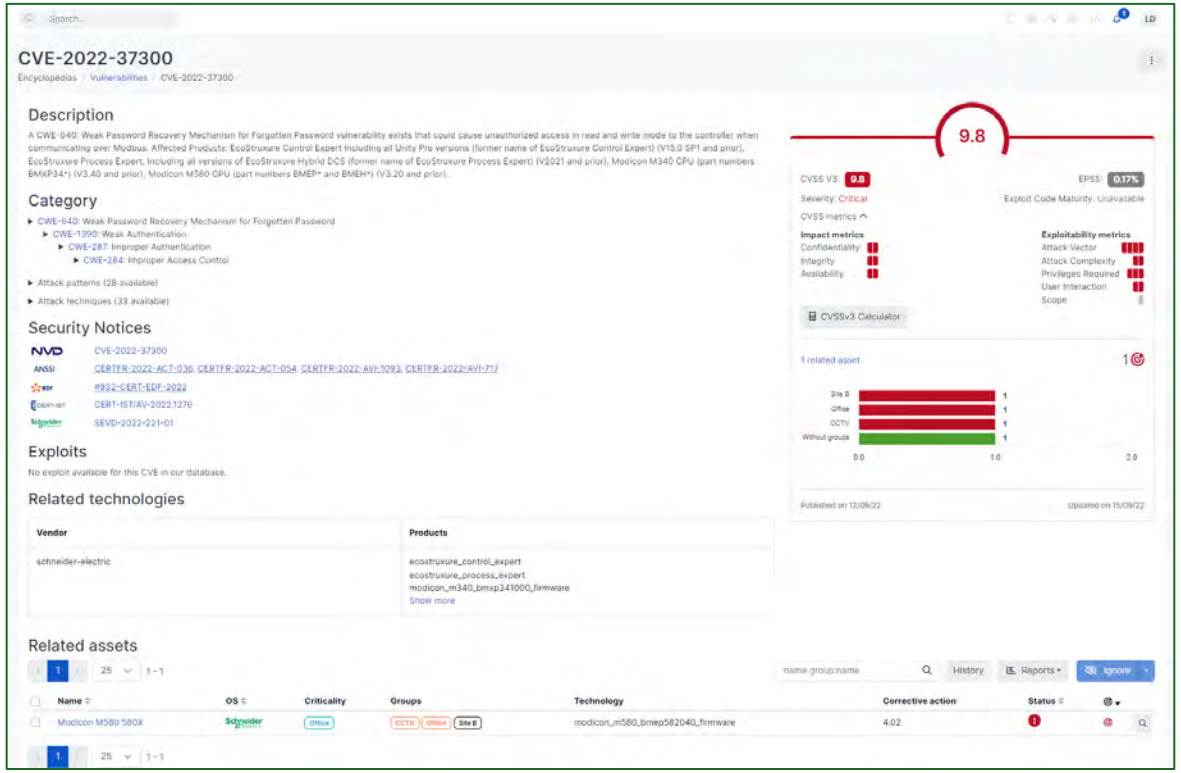
▽

GESTION DES VULNERABILITES

▽

SURVEILLANCE ET DETECTION

▷



CVSS Score	EPPS Score	SSVC Reco	KEV Catalog
Asset Context	Running SW/FW Service	Patch Available	EoS Info
CIS Benchmark	ICS Best Practices	Security Best Practices	OWASP
AD Checks	Exploit Maturity	Open Ports	Custom Checks

DESIGN SECURISE

▽

GESTION DES ACTIFS

▽

GESTION DES VULNERABILITES

▽

SURVEILLANCE ET DETECTION

▷

Surveillance physique
. Scellés
. Vidéoprotection
. Détection d'ouverture
. Boîtes à clés

Surveillance réseau

. Surveillance des réseaux industriels
. Détection sur base de signatures
. Détection comportementale
. Détection opérationnelle

Surveillance applicative
. HIDS
. HIPS
. EDR

Orchestrer pour garder une longueur d’avance

04

GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE

▽

AUDIT

▽

MAINTIEN EN CONDITION DE SECURITE

▽

SECURISATION DES FINS DE CYCLE

GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE

▽

AUDIT

▽

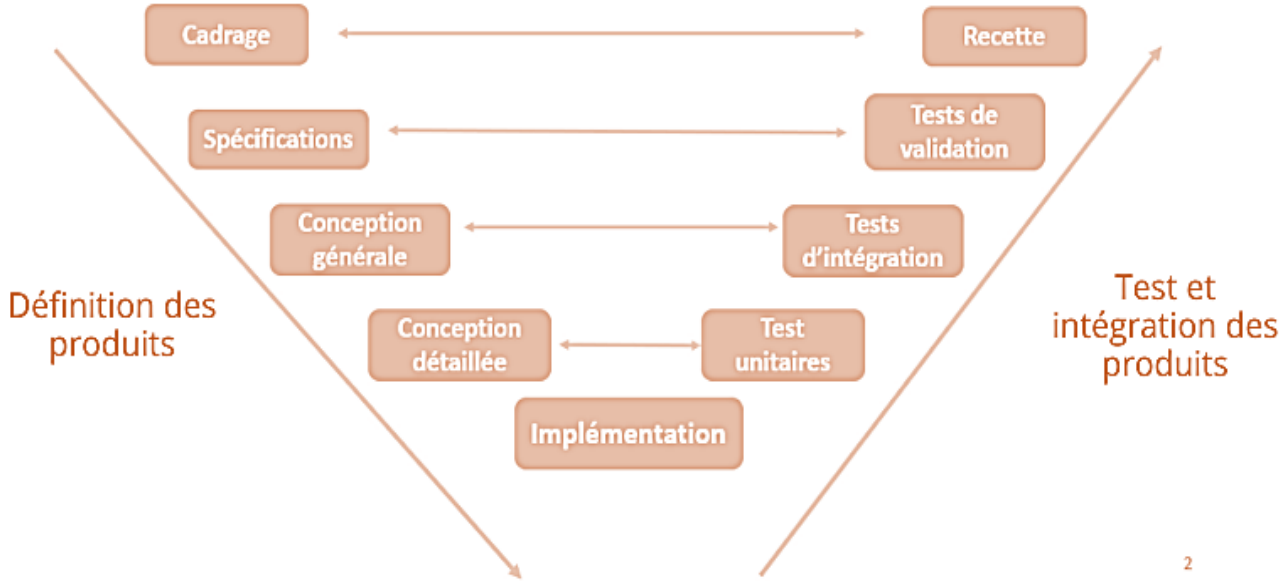
MAINTIEN EN CONDITION DE SECURITE

▽

SECURISATION DES FINS DE CYCLE

Un important travail de planification et de documentation

. Spécifications (fonctionnelles, techniques)
. Stratégie d'homologation
. Procédures de sécurité
. Guides de configuration
. Bill of materials
. Matrices de durcissement
. Plans de tests
. Plan d'audit



GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE

▽

AUDIT

▽

MAINTIEN EN CONDITION DE SECURITE

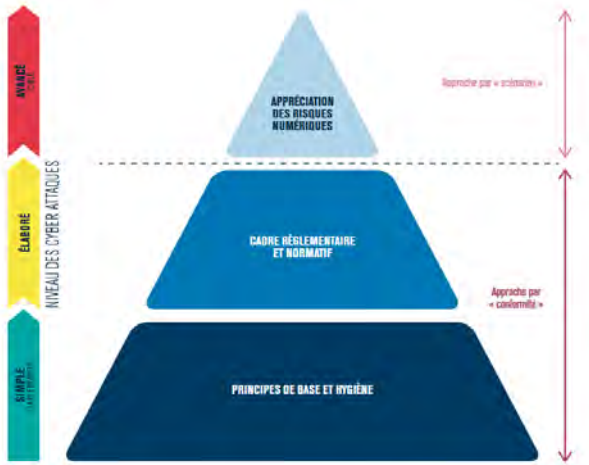
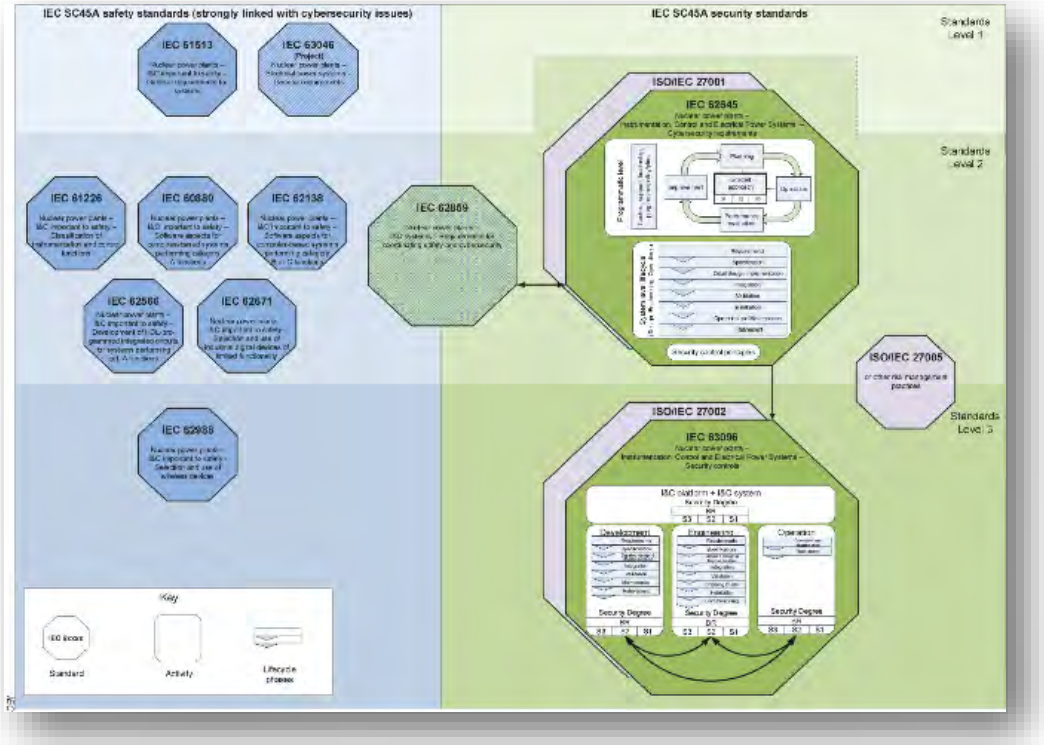


Figure 1 — Pyramide du management du risque numérique

Source : ANSSI



GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE ▷

▽

AUDIT

▽

MAINTIEN EN CONDITION DE SECURITE

▽

SECURISATION DES FINS DE CYCLE

Les essentiels:

. S'entraîner

. Définir des échelles de gravité

. Associer tous les niveaux de l'entreprise

. Identifier TOUS les acteurs (y compris externes)

. Conduire des ateliers d'approfondissement

GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE

▽

AUDIT ▷

▽

MAINTIEN EN CONDITION DE SECURITE

▽

SECURISATION DES FINS DE CYCLE

Audit de gouvernance et de conformité

Audit d'architecture et de segmentation

Audit de configuration

Tests d'intrusion

Audit de sécurité physique

Audits ciblés (réponse à incident, vulnérabilités, maintenance, sauvegardes)

GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE

▽

AUDIT

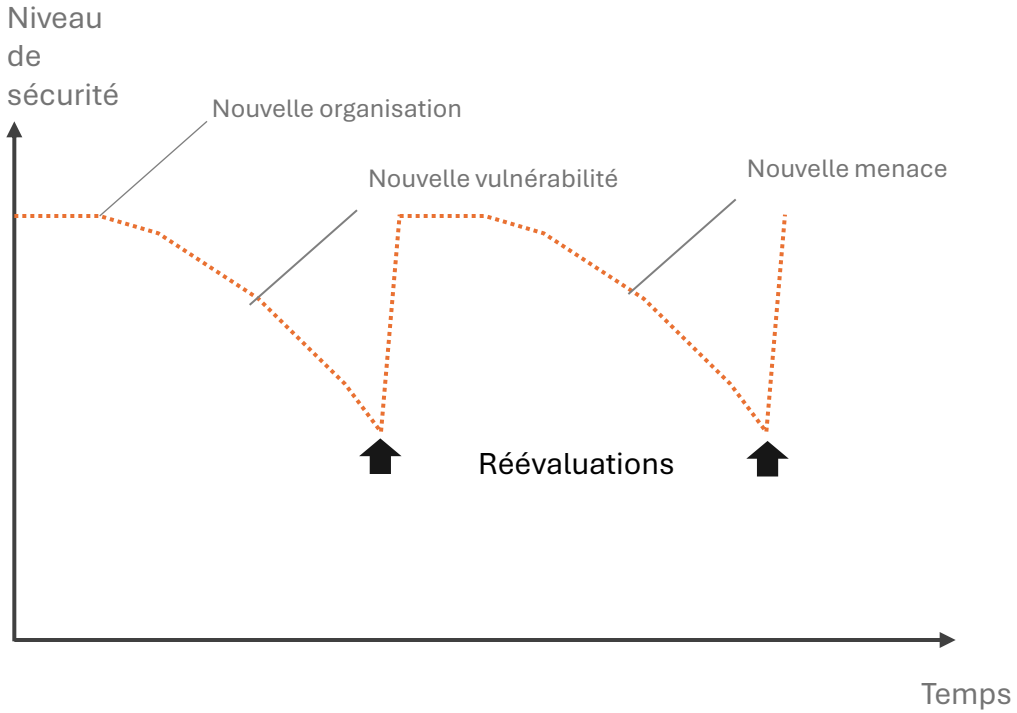
▽

MAINTIEN EN CONDITION DE SECURITE ▷

▽

SECURISATION DES FINS DE CYCLE

On cherche au minimum le maintien mais aussi l'amélioration continue de la posture de sécurité!



Action continue
. Surveillance systèmes
. Gestion des vulnérabilités

Actions récurrentes:
. Homologation
. Analyse de risque
. Audits
. Formation
. Contrôle de la supply chain

GESTION DE PROJET

▽

ANALYSE DE RISQUES

▽

PREPARATION CRISE

▽

AUDIT

▽

MAINTIEN EN CONDITION DE SECURITE

▽

SECURISATION DES FINS DE CYCLE ▷

Ne pas oublier...

. Dispositions contractuelles
. Neutralisation matérielle (suppression de composants critiques)
. Désactivation des firmwares spécifiques
. Effacement sécurisé
. Destruction sécurisée (ex: DIN 66399)
. Gestion des supports (EEPROM, Flash, SSD)
. Traçabilité post-décommissionnement
. Surveillances des marchés latéraux

Recyclage et Valorisation Sécurisée

MERCI

Cybersécurité industrielle: garder une longueur d’avance sur les risques OT

Lundi de l’IE 17.03.2025

Pierre-Marie LORE