Protection de l'Internet Industriel
une approche basée sur la connaissance et la surveillance

SENTRYO

Cybersecurity for Industrial Control Systems

Thierry Rouquet
thierry.rouquet@sentryo.net
@thierryrouquet

Cyber@hack
Edition #2

sentryo

- **Start up technologique** - crée en 2014
- Conçoit, développe et vend des solutions de **Cyber Securité** dédiées aux Systèmes de contrôle industriel (ICS, SCADA)
- Fondée par des “vétérans” de la Cyber Sécurité
  - **Thierry Rouquet**, Serial Entrepreneur, CEO Arkoon Network Security / AFDEL / Cluster EDIT / RCC.
  - **Laurent Hausermann**, 15 years cybersecurity R&D, CTO Arkoon Network Security, Hacking, Innovation, Blogger.

TREMPLIN ENTREPRISES 2015 SÉNAT

FINALIST
EIT ICT Labs IDEA CHALLENGE
8 topics. 8 cities. One challenge.

European Institute of Technology Idea Challenge

230 Cybersecurity startups
3rd prize winner

Sentryo protège les systèmes Industriels et les réseaux “*machine to machine*” contre les cyber-risques

Les systèmes industriels pilotent les installations nationales critiques. Ils sont vulnérables

Défense

Gaz

Énergie

Pétrole

Transport

Infrastructures Urbaines

Un monde différent

Des menaces réelles

HOME SEARCH

The New York Times

Service Banned oss Germany by nkfurt Court

Brainy, Yes, but Far From Handy

Drone Developers Consider Obstacles That Cannot Be Flown Around

DEALBOOK

Compuware Agrees to $2.5 Billion Buyout

MIU MIU WOMEN'S TALES PRESENTS SOMEBODY BY MIRANDA JULY

TECHNOLOGY

Russian Hackers Targeting Oil and Gas Companies

By NICOLE PERLROTH JUNE 30, 2014

EMAIL FACEBOOK TWITTER

SAN FRANCISCO — Russian hackers have been systematically targeting hundreds of Western oil and gas companies, as well as energy investment firms, according to private cybersecurity researchers.

Guillaume Poupard : « Ma crainte, c'est la panne d'électricité qui plonge la France dans le noir »

LESECHOS.FR | LE 06/05/14 À 18H09

Guillaume Poupard a pris les rênes de l'ANSSI le 26 mars dernier. Il fait le point sur la réalité des cyber-menaces qui pèsent sur les entreprises et les mesures de protection à prendre.

NEWS

US researchers find 25 security vulnerabilities in SCADA systems

Warwick Ashford

Friday 18 October 2013 15:24

Share 63 +1 6 Tweet 51

US researchers have identified 25 zero-day vulnerabilities in industrial control SCADA software from 20 suppliers that are used to control critical infrastructure systems.

Attackers could exploit some of these vulnerabilities to gain control of electrical power and water systems, according to Wired.com.

Nine of these potential exploits have so far been reported to the suppliers concerned and the US Department of Homeland Security.

The vulnerabilities were found in devices that are used for serial and network communications between servers and substations.

Electrical engineer Chris Sistrunk and consultant Adam Crain said these products have been overlooked as hacking risks

"41 % of cyberattacks are targeting Energy companies"

N.S.A - General Keith Alexander

Exemple
Compromission du système de contrôle commande d'un haut fourneau

WIRED – Jan 8th 2015

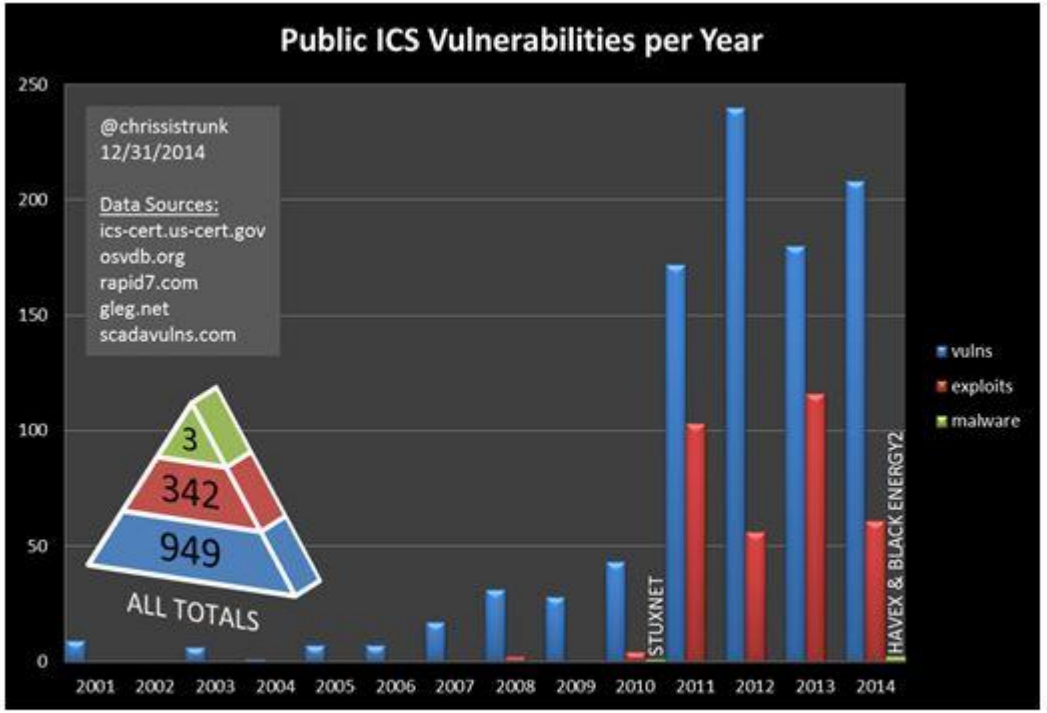
A Cyberattack Has Caused Confirmed Physical Damage According to the German BSI, hackers had struck an unnamed steel mill in Germany. They did so by manipulating and disrupting control systems to such a degree that a blast furnace could not be properly shut down, **resulting in "massive"** — though unspecified — **damage.**

Durée de vie de l'installation = 20 years

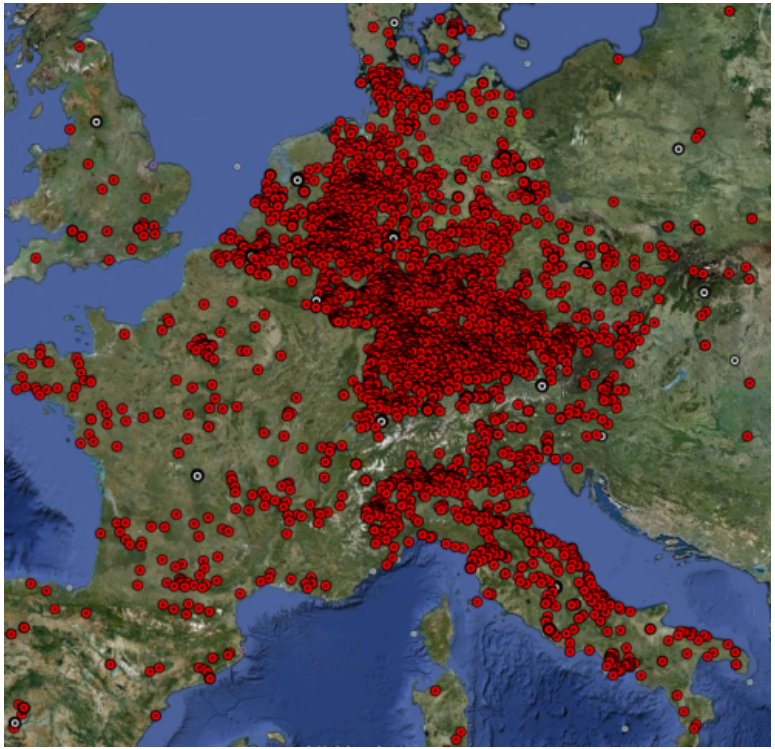
Revamping ≈ M€ 100

De nombreuses vulnérabilités

Stuxnet a été le point de départ à une activité forte de recherche de vulnérabilités des systèmes industriels



Trop facilement disponible



1 point rouge = 1 automate accessible directement depuis Internet.....

Souvent avec un mot de passe par défaut !!!!

On estime leur nombre à 500 000 dans le monde !

Source : Scada Security Group- Freie Universität Berlin

L’Internet Industriel est vulnérable

Open Web Application Security Project (*OWASP*)

...

OWASP Top 10 IoT Weakness

#1 Insecure Web Interface

#2 Insufficient Authentication/Authorization

#3 Insecure Network Services

#4 Lack of Transport Encryption

#5 Privacy Concerns

#6 Insecure Cloud Interface

#7 Insecure Mobile Interface

#8 Insufficient Security Configurability

#9 Insecure Software/Firmware

#10 Poor Physical Security

Le challenge

Maîtriser le risque cyber dans un environnement business de plus en plus volatile et ouvert

SMARTGRID

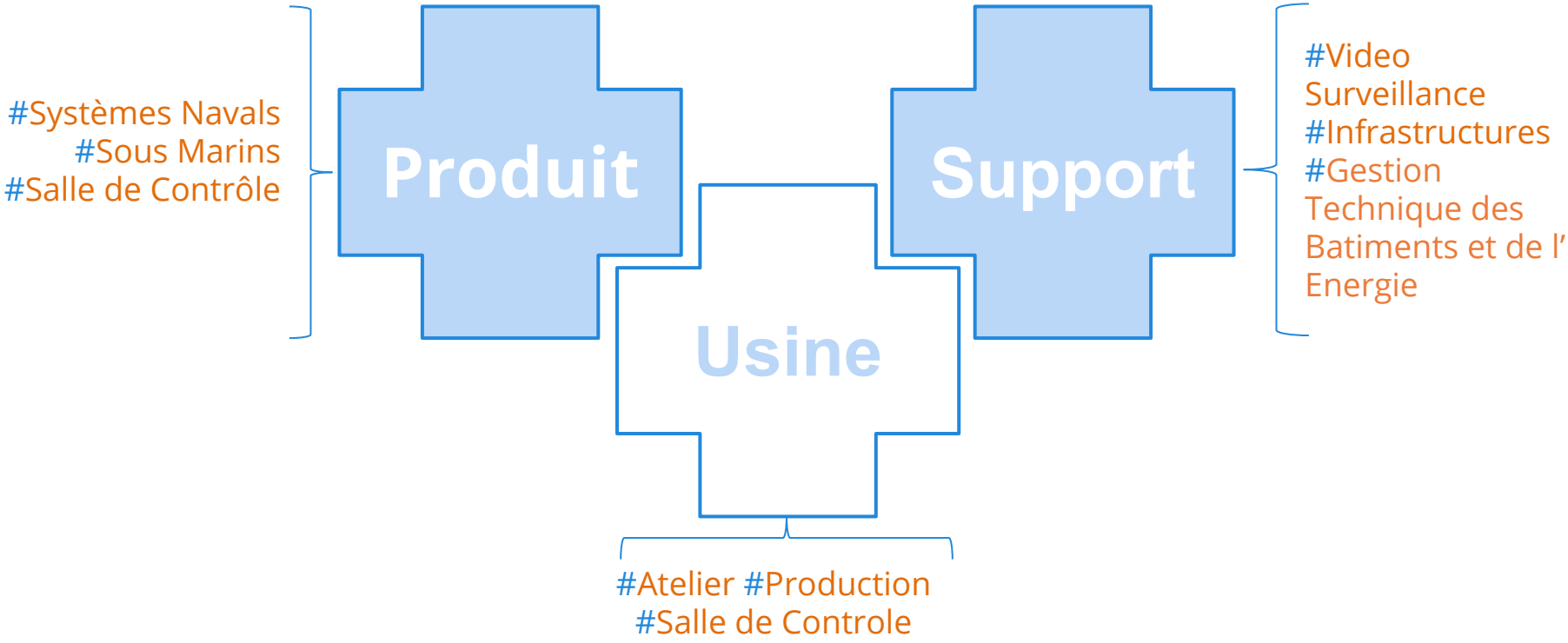
industrial Internet of Things

INDUSTRIE 4.0

OPPORTUNITES vs RISQUES

REGLEMENTATION

Penser à tous les systèmes industriels !



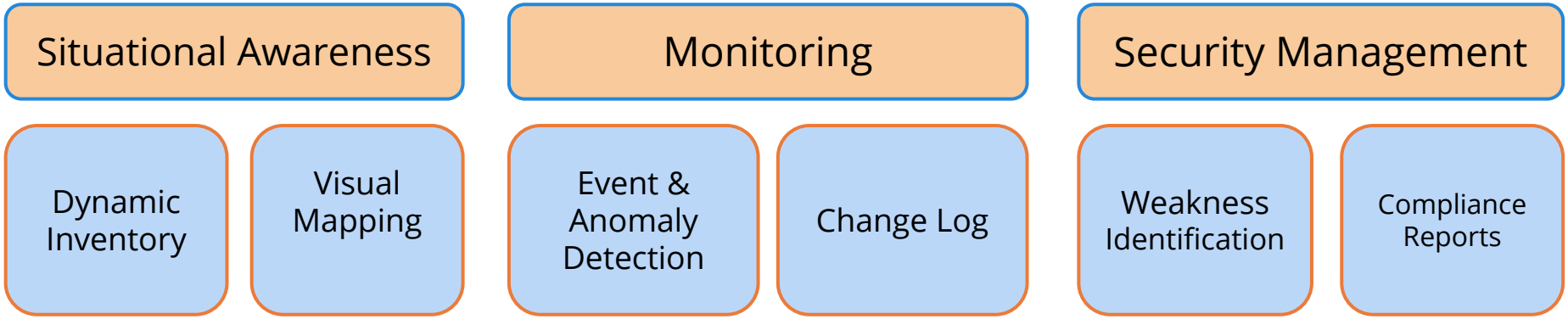
4 mesures urgentes

1. Nommer un Responsable Sécurité des Systèmes Industriels.
2. Lancer un projet de cybersécurité en constituant un groupe de travail multimétier
3. Réaliser un inventaire détaillé et une cartographie logique.
4. Se mettre dans une posture de Cyberdéfense (prime au défenseur)

Une posture de maîtrise du risque cyber par la connaissance de son environnement et la surveillance

Sentryo ICS CyberVision

Sentryo ICS Cybervision



Architecture typique d’un réseau industriel

Supervision network

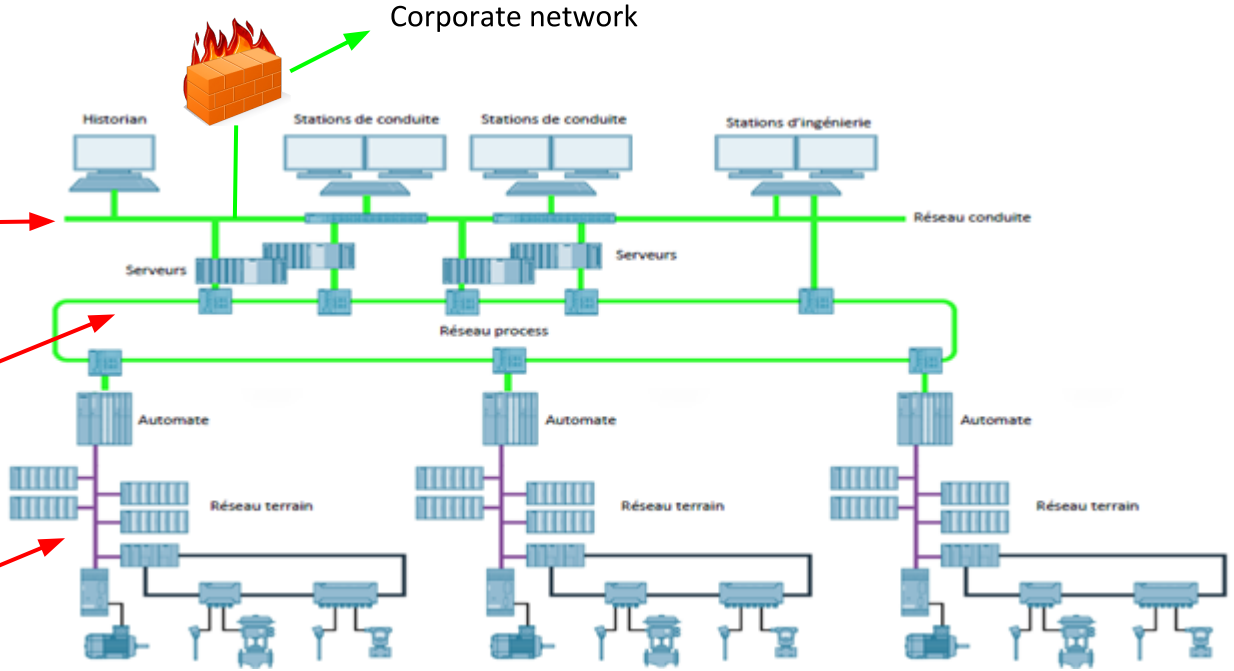
- Standard IT Network
- Protocols : TCP-IP, OPC-UA, SNMP, NTP

Process network:

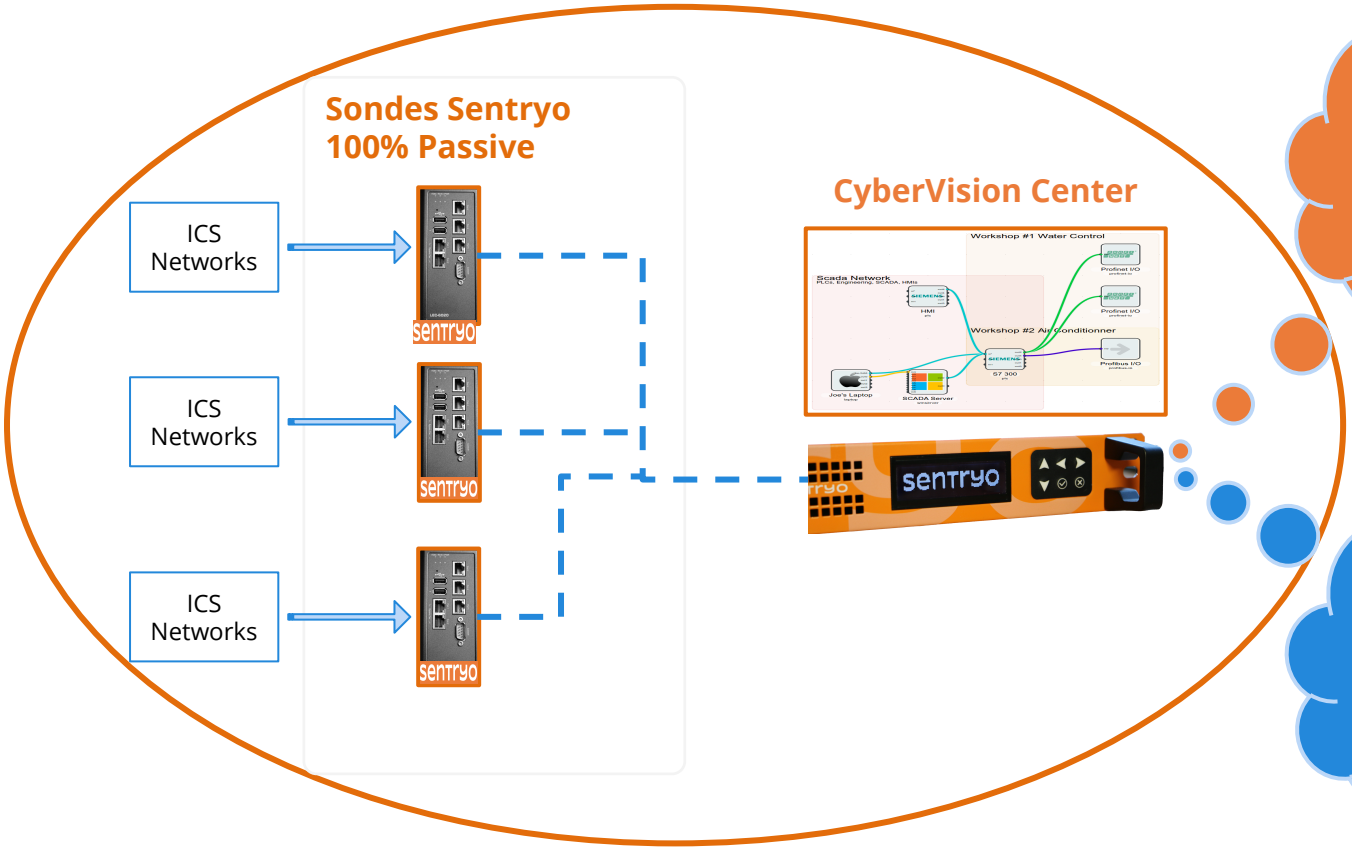
- Cycle : 500 ms << 1 s.
- Protocols : S7, Modbus TCP, Ethernet/IP, XWAY/UNI-TE….

Field network :

- Cycle : 1ms << 100ms.
- Protocols : PROFINET, PROFIBUS, Modbus TCP, Ethernet/IP



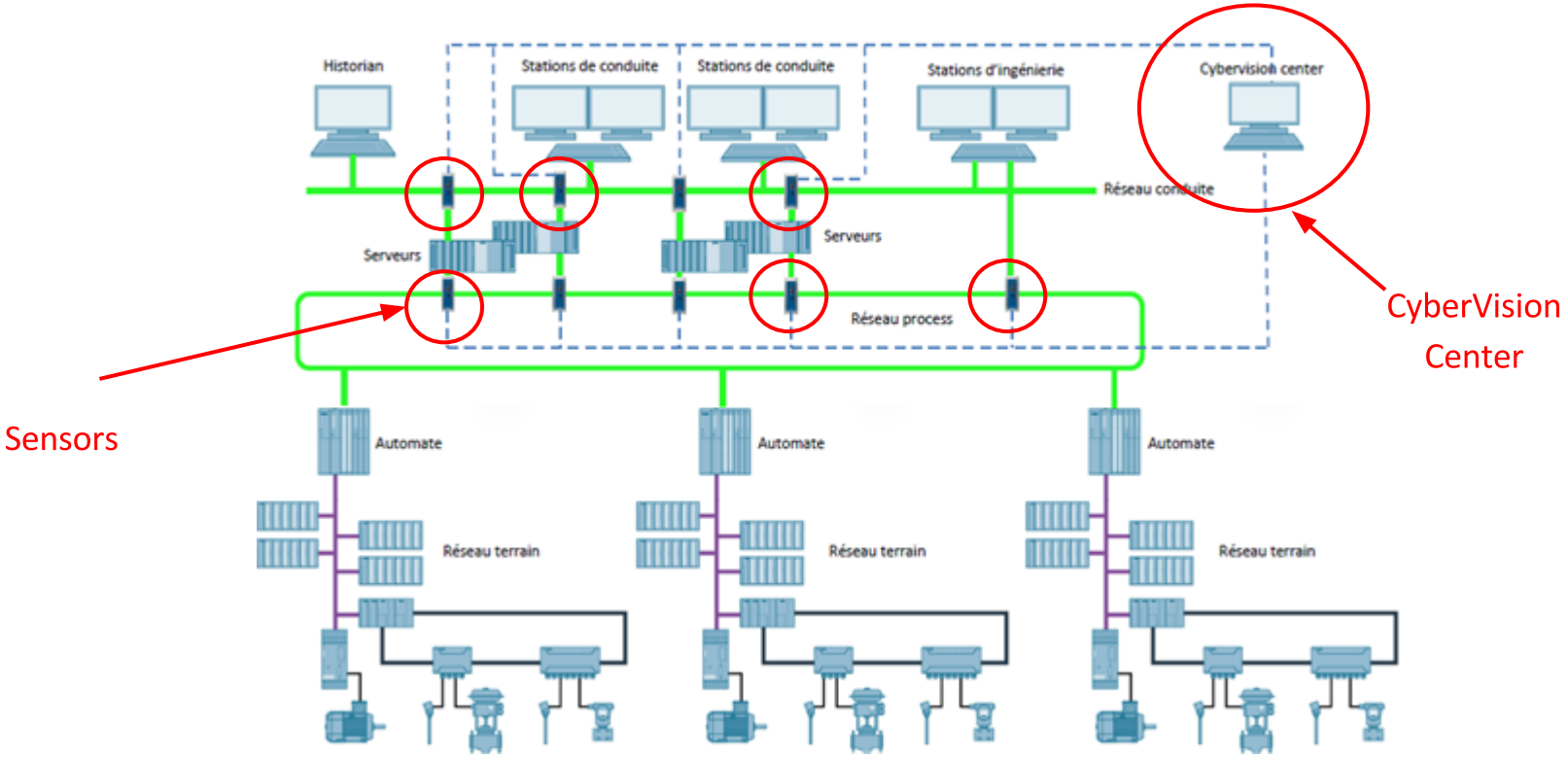
Sentryo ICS CyberVision



Threat Intelligence

Security Operation Center

ICS CyberVision implementation

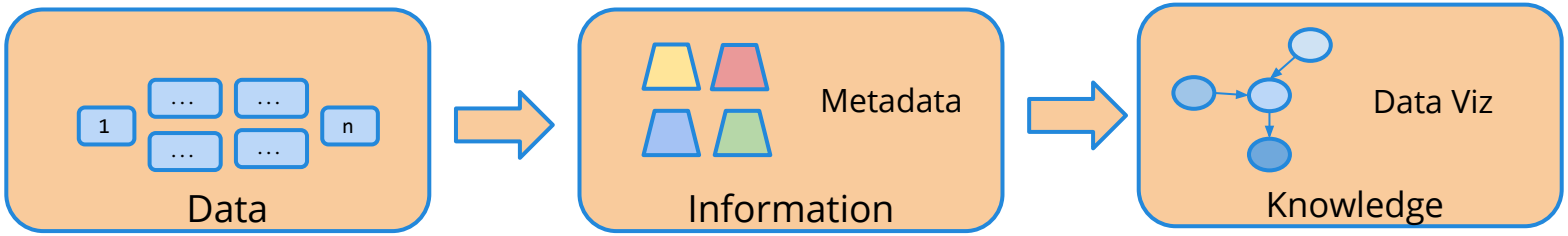


ICS CyberVision - Situational Awareness

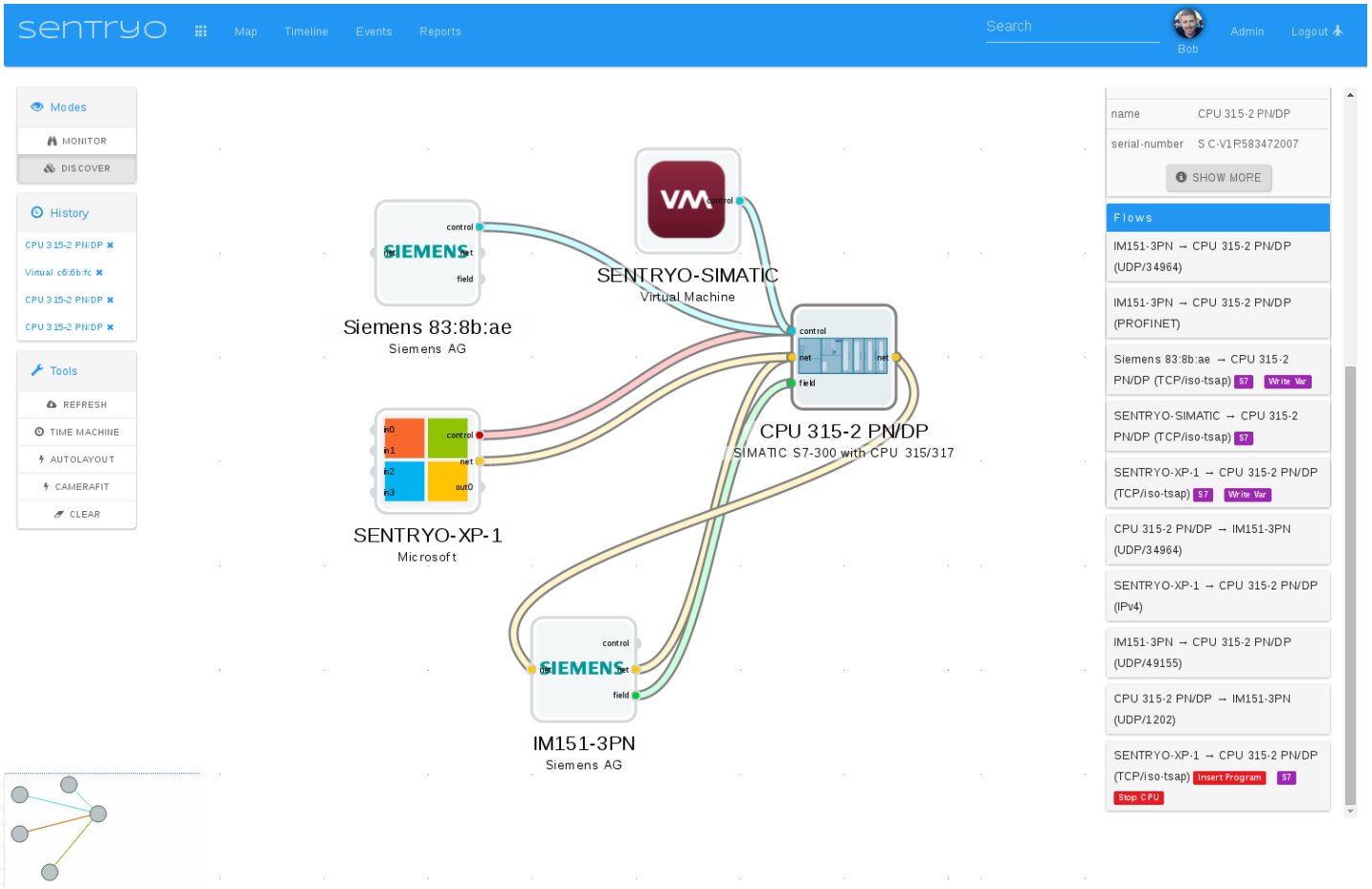
Analyse Temps Réel des Protocoles Industriels

Extraction des Meta Données

Visualisation

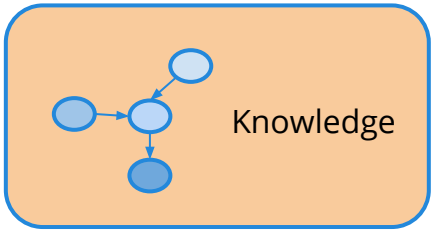


Situational awareness = inventaire & carographie logique

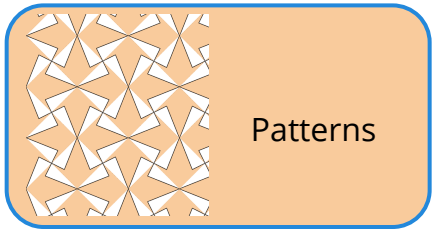


ICS CyberVision - Détection

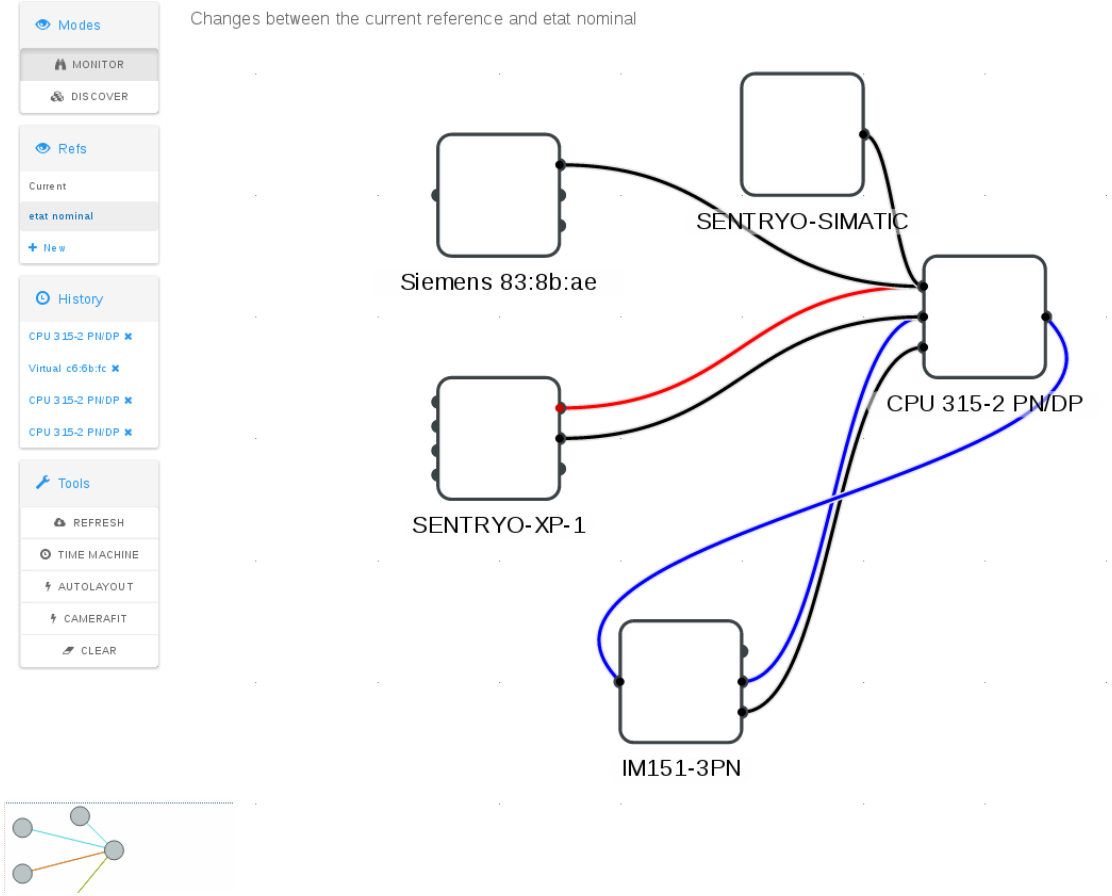
Connaissance fine du système basé sur l'historique des opérations



Apprentissage des modèles de *comportements normaux*



Détection des évènements anormaux



Détection d'Anomalies et d'Intrusions

Sentryo ICS CyberVision

- Solution 100% **passive** - pas d'impact sur le réseau-
- Near **zéro configuration** (Machine Learning).
- Approche de détection de type **white listing** (modèle comportemental).
- Conçu pour une adoption par les hommes de l'OT (**data visualization**).
- Support **multi** vendeurs : Siemens, Schneider, Rockwell .....

sentryo

Cybersecurity for Industrial Control Systems