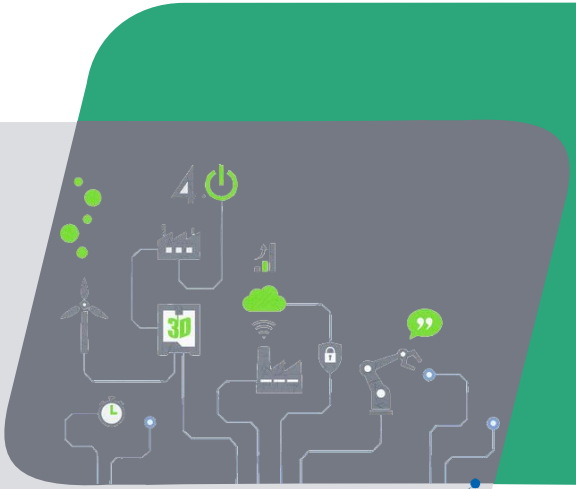
PROFIBUS • PROFINET



Comment créer et gérer une “Cyber Control Room” avec Sentryo ?

PROFINET® PROFIBUS® PROFIsafe PROFIenergy PROFIdrive IO-Link FDI

Créer et gérer une “Cyber Control Room” avec Sentryo

1. **Introduction**
2. **OT Cybersecurity in 2017**
3. **What is a Cyber Control Room**
4. **ICS CyberVision**
5. **Conclusion & Q&A**

1. INTRODUCTION

SENTRYO

Incorporated: June 2014

Headquarters: Lyon, France

Venture capital backed by UK/FR funds

Target **Industrial corporations:** Energy, Process Industries, Manufacturing, Transportation

Offices: **France/Germany/USA**

Partners: **USA, LATAM, South Asia, Middle East**

AWARDS

BMW TechDate **Winner** - June 2016

CISCO Acceleration **Prize** - June 2016

Lauréat Concours Mondial de l'Innovation CMI - June 2016

Winner Innovation Prize Monaco Cybersecurity Show October 2015

IIOT Cybersecurity startup of the year McRock Capital Symposium - May 2017

2. OT CYBER SECURITY IN 2017

OT security is not IT security but ...

IT risks are sources of **fraud**, **privacy & data** leaks, **financial** losses.

OT & IIoT risks are sources of **health, safety and environmental** casualties.

2. OT CYBER SECURITY IN 2017

OT security is 2017 OT/IT Security officers pains

- **Limited Visibility** over their assets/devices
- **Limited Conversation** with OT and IT staff members
- **Limited Resources** to setup a global scale project
- **Limited Time** to act due to many different OT systems and production constraints.

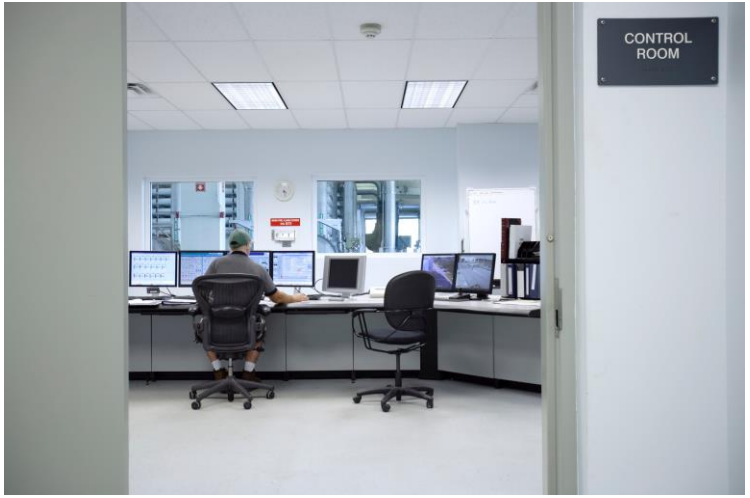
- **Digitization** and Industrie 4.0 programs are growing
- **OT Cyberattacks now** seen in the mainstream (Ukraine, Germany, etc.)
- **Compliance and regulation** pressure
- **Board level** awareness

But Now

3. WHAT IS A CYBER CONTROL ROOM?

What is a Cyber Control Room ?

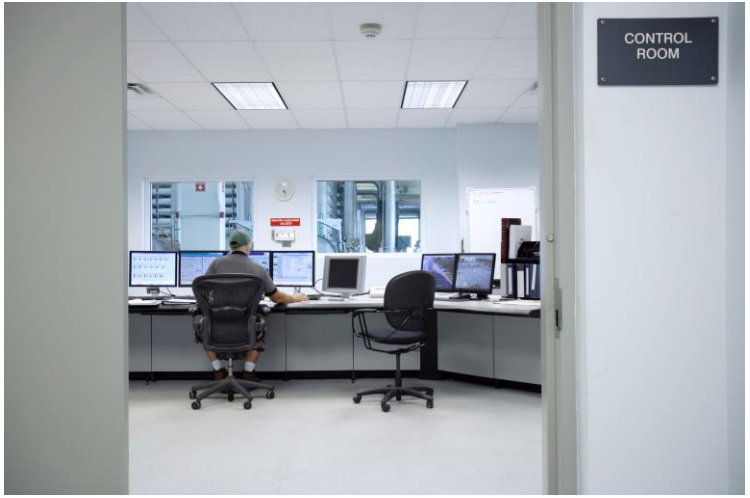
- **A Security operations Center** (SOC) dedicated to **OT environments.** It's a virtual facility for monitoring cyber security of OT networks and assets;
- A mix of people, processes and technology, **composed of activities;**
- Leveraging **years of IT Cybersecurity experience;**
- Incorporated into **OT control and maintenance processes.**



3. WHAT IS A CYBER CONTROL ROOM?

What is a Cyber Control Room ?

- **A Security operations Center** (SOC) dedicated to **OT environments.** It's a virtual facility for monitoring cyber security of OT networks and assets;
- A mix of people, processes and technology, **composed of activities;**
- Leveraging **years of IT Cybersecurity experience;**
- Incorporated into **OT control and maintenance processes.**



3. WHAT IS A CYBER CONTROL ROOM?

Suggested Actions Build a Cyber Control Room

- Increase visibility, integrity and security by installing monitoring and detection systems and employing formal controls;
- Engage a passive monitoring approach by using lightweight sensors near the different processes;
- Start as soon as possible and grow process and the scope step by step by setting up a comprehensive project plan;
- Leverage existing IT Infrastructure (SIEM) and processes (SOC) by embedding SOC people as well as OT people.

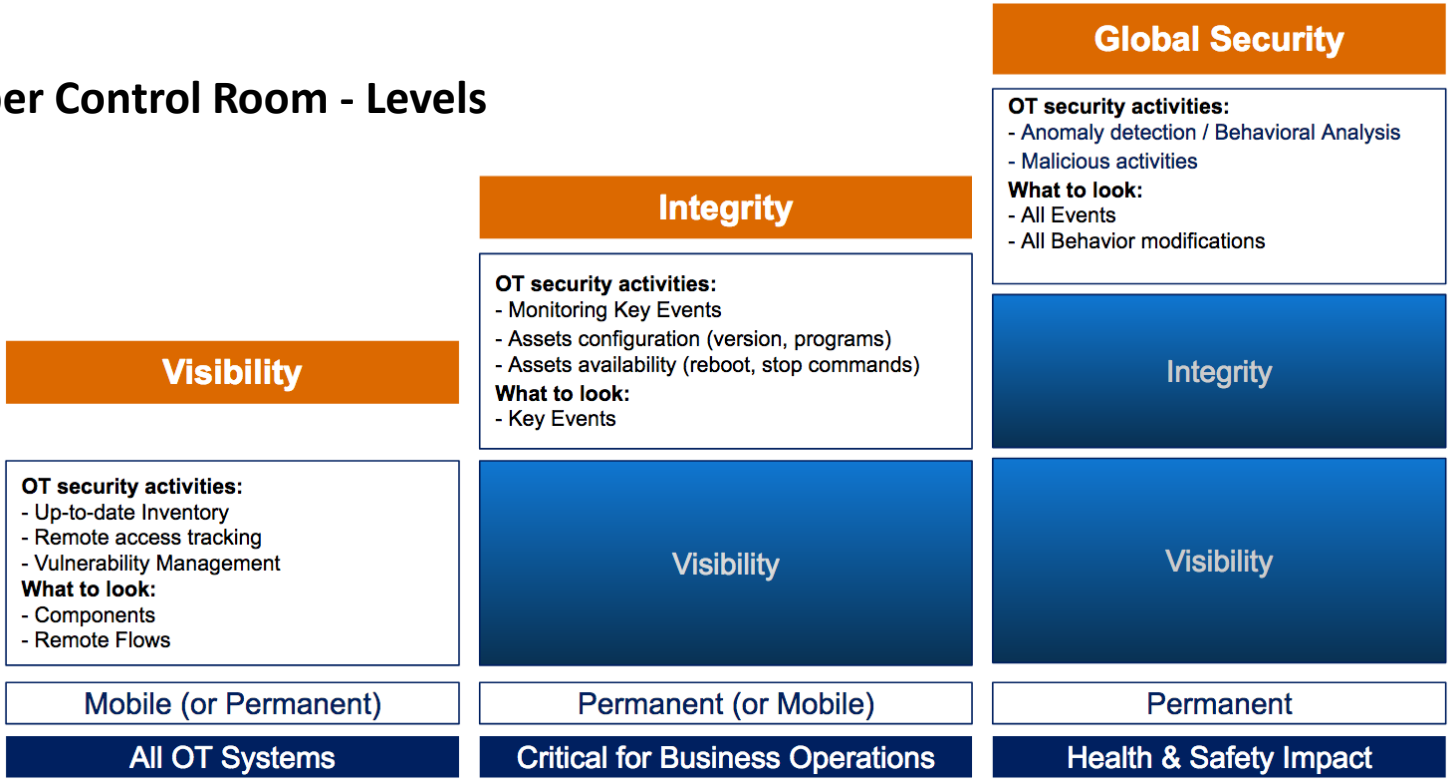
3. WHAT IS A CYBER CONTROL ROOM?

Key success factors for a Cyber Control Room

- **Understand first that all sites, or OT process are not “critical”.** The OT security strategy shall be prioritized by risk;
- **OT teams must be at the core of the OT Security project**. OT&IT Collaboration is key. OT Teams should be in decision making roles for OT systems;
- **OT Security is a multi department project** : General Management (CDO, CSO), IT Dep (CISO, Network Admin), OT Dep (Control Engineers, Maintenance, Engineering).

3. WHAT IS A CYBER CONTROL ROOM?

Cyber Control Room - Levels



3. WHAT IS A CYBER CONTROL ROOM?

Cyber Control Room - Organisation

Cyber Control Room Levels	Visibility	Integrity	Security
Industrial Installation Class	Not critical	Important for business operations	Critical for business + HSE impacts
Investment	$	$$	$$$$
Monitoring Period	Once in a year	On a regular basis (weekly)	24/7
Cyber Control Room Localisation	On site + Reports exchange	On site or centralised	Centralised and co-localized with the IT SOC + SIEM integration
OT Staff Workload	Punctual (some days per year) to link OT maps with business logic	Punctual (few days per month)	Regular (20% FTE minimum per site)
OT&IT Collaboration	Links with IT pentester	Virtual SOC Operation (see Gartner definition)	OT native people working with cyberdefense expert (SOC or CSIRT)

4. ICS CYBERVISION

Sentryo ICS CyberVision increases visibility, integrity and security

OT Integrity:
Full OT asset inventory and flow mapping
OT configuration tracking
Weaknesses & Vulnerabilities identification

OT Security Monitoring:
Track all changes
Anomaly Detection
Malicious Behaviors Identification

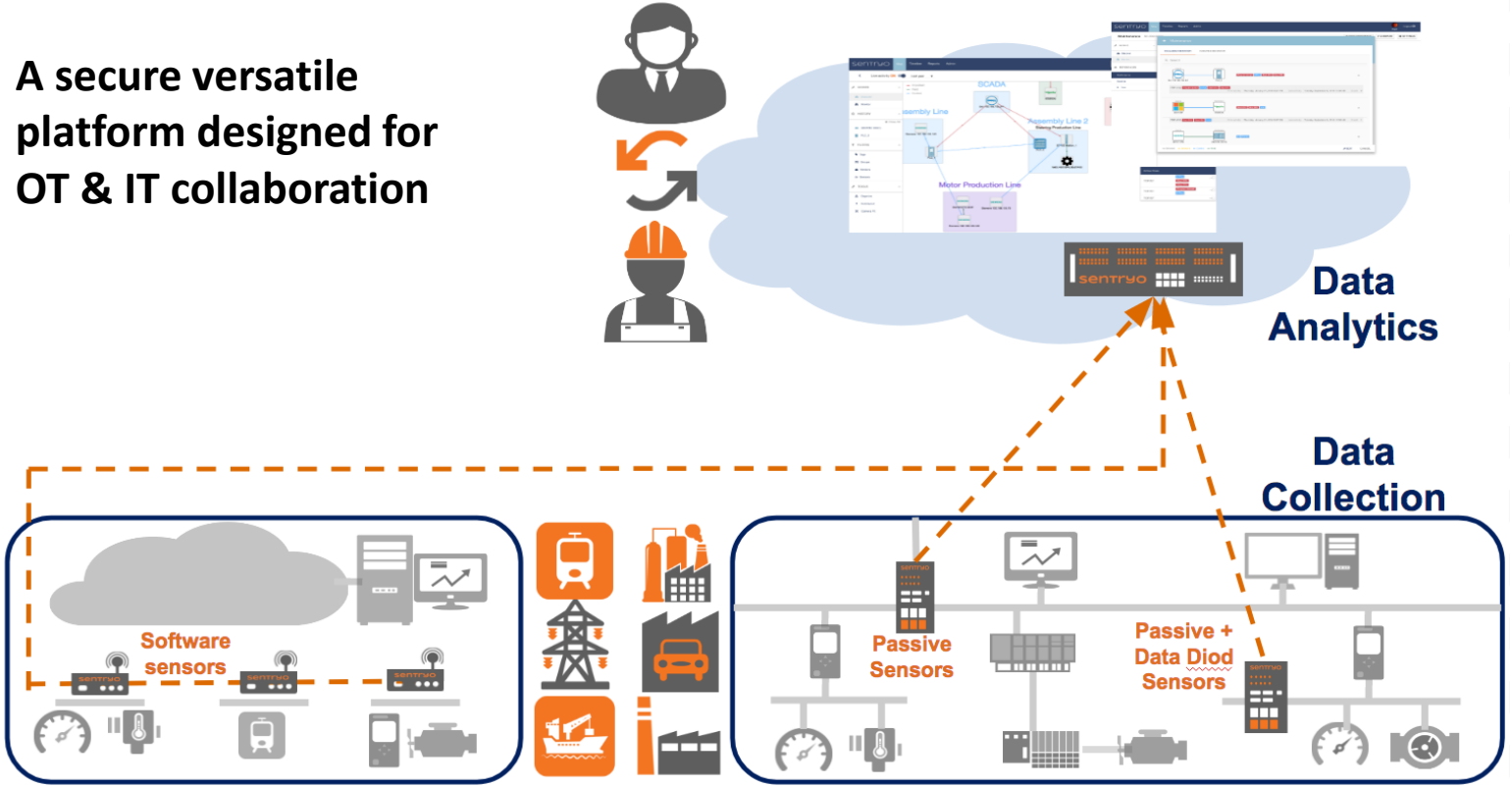
Cyber Control Room:
Intuitive OT User Experience
OT “Flight Recorder”
Advanced Data Visualisation Algorithms

Benefits:

- **100% Passive**
- **Fosters OT & IT collaboration**
- **Increased availability & resilience**
- **Alert on malicious behaviors or untracked changes**

4. ICS CYBERVISION

A secure versatile platform designed for OT & IT collaboration



4. ICS CYBERVISION

A versatile, two tier architecture

Fits with all kinds of Industrial architectures: centralised, multi-sites, massively distributed

CyberVision Center

Hardware appliance/Software appliance/Cloud deployment

Sentryo Sensors

Critical Infrastructure ← → **Industrial IoT**

SENSOR7
Hardware Diod included

SENSOR3
Industrial DIN Form Factor

Software Appliance Virtual Machine

Cisco IoX Container Embedded inside IE4K Switch

CISCO Cisco live! February 20 - 24, 2017 · Berlin

Potential Cisco SolutionX Program

4. ICS CYBERVISION

Démonstration