USE CASE 1 STEEL MILL IN GERMANY

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’ damage.
ICS CERT – Dec 10th 2015

Experts have identified a sophisticated malware campaign that had compromised numerous industrial control systems (ICSs) environments. They have found multiple variants of the Black Energy malware.

Analysis indicates that this campaign has been ongoing since at least 2011.

Multiple companies have identified the malware on SCADA stations from various vendors including GE Cimplicity, and Siemens WinCC.
sentryo

Protects
the Industrial Internet against cyber risks

- **Incorporated** in June 2014
- **Headquarter:** Lyon
- Design, develop & sell cybersecurity solutions
- Funded and managed by serial entrepreneurs & cybersecurity veterans

**Award winner**
Prix de l’innovation des Assises de la sécurité July 2015

**Prize winner**
European Institute of Technology Idea Challenge Nov 2014

**Award winner**
Tremplin Entreprise Sénat / Essec Feb 2015

**Member:** Hexatrust
Cybersecurity & Digital Trust

**Member:** AFDEL
Les éditeurs de logiciels et solutions internet
WHAT IS THE INDUSTRIAL INTERNET

Today
Industrial Automation

Industrial Control System (ICS)

Tomorrow
The Industrial Internet Of things

Industrie 4.0, Smart cities, Smart grids, eHealth..

PRODUCT
#Connected Objects
#CloudOriented
#As A Service™

FACTORY
#Manufacturing
#Exploitation Teams

SUPPORT
#CCTV
#HVAC
#SmartBuilding
#SupplyChain
#SubContractors
The Industrial Internet is cluttered and vulnerable

- Attack surface of existing and upcoming systems is increasing
- No cyber security culture in industrial (OT) teams
- Upcoming Industrial Internet requirements
THE PROBLEM (2)

IT Cybersecurity solutions do not fit OT environment requirements

IT SYSTEMS
- Real Time
- Reliability
- Performance
- Integrity
- Confidentiality

OT SYSTEMS
- Safety
- Availability
- Real Time
- Integrity
- Performance
Sentryo

THE PROBLEM (3)

Industrial Protocols are complex

- Proprietary and Standard at the same time.
- Focusing on high level of abstraction and indirection
- Multiplexed, mixing physical, serial bus and network data
- Used in flat, unsegmented networks
**Sentryo ICS CyberVision** delivers an operational security capacity to prevent, detect and respond to cyber attacks targeting the Industrial Internet.

- **Prevent**: Enable *Control Engineers* reduce the attack surface
- **Detect**: Detect malicious behaviors and *weak signal* of cyber attacks.
- **Respond**: Facilitate incident response by gathering all the informations required by *Cybersecurity Expert*
- **Report & Comply**: Provide reports to the *Security Officer*
- **Streamline OT and IT collaboration**: Offer a common language and *collaboration tool* centered on risk management
The Sentryo ICS CyberVision workbench

**Key Features**

- **Extract metadata from the network flow using passive sensors**
- **Dynamically build an inventory of all components and a map of all connections**
- **'Learn' the system and deliver statistical and behavioral patterns. Detect abnormal events**
- **Take preventive decision based on the situational awareness**
- **Trigger incident response upon advanced compromise evidence to avoid damage**
- **Implement preventive action to enhance network protection**
- **Execute remediation plan**

**Industrial Control Systems (ICS)**

**Sentryo Sensors**
- Hardware or software agents

**Sentryo CyberVision Center**
- Appliance (HW/Virtual) or cloud

**Collaboration**

**Reporting**

**Control Engineer**

**CSO**

**Cybersecurity Expert**