

Cyber system industrial

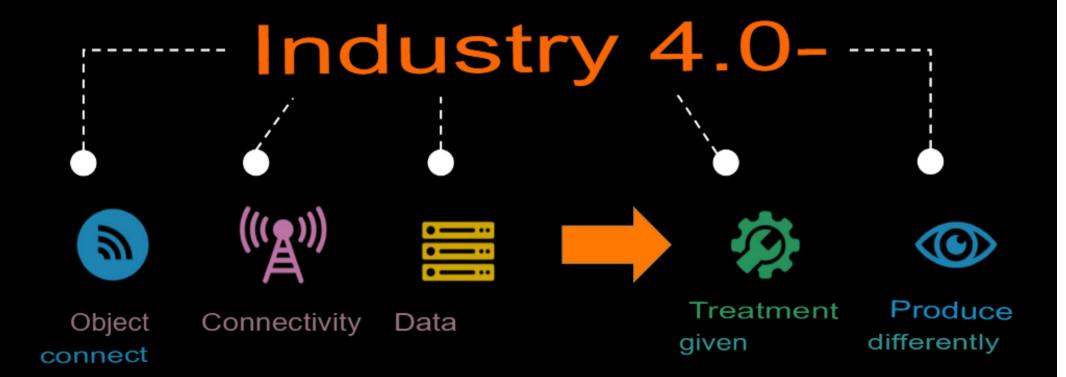


Summary

- Intensification of attacks
- The repositories and regulation
- Our value proposition



Industry 4.0



The industry is digitizing



An ever more connected industry based on IT standards

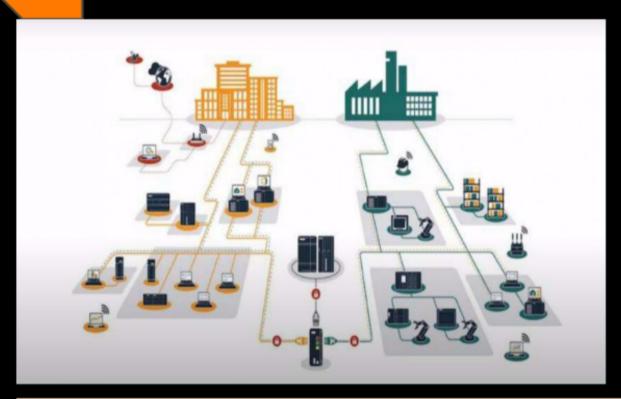




Thus exposing more and more the systems industrial cyberattacks



IT/OT Convergence



An IT/OT convergence pushed by :

- * A simplification of the production processes control :
- A need for real-time visibility
- A need for optimization of the tool industrial

Increase in the attack surface involving new controls to be put in place

Industrial(in)safety

99

Air Gap is no longer just a myth

"Safety measure consisting of isolating physically a system to be secured from any computer network."



- · Long service life
- · Integrated and proprietary IT
- *Rare on-site IT skills
- *Historically, lack of security by design



- *Evolution from factory 3.0 to factory 4.0
- * Connected objects
- •Machine-to-Machine Communication
- Cloud Computing
- Big Data, etc.



Key figures

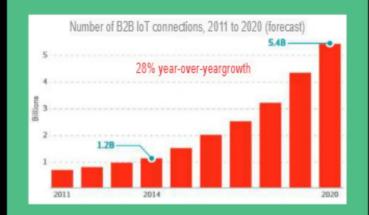
201 days for discover for one cyberattack
And another 70 days to overcome the damage caused

Source: Ponemon Institute

The most important industrial fields affect:

- Oil & Gas
- · Building automation
- Engineering

Increase attacks for the Industrial SI of 33.4% between S1 and S2 2020



"Only 50% of industrial companies will have switched over towards the use of all the potentialities of industry 4.0" --- Roland Berger

5 365 families of malware stuck in S1 2020 +51% of ICS in Africa have been attacked in 2020





TOP 3 sources of threats
Internet
Removable media
Email

Protections to improve

57%

industrial sites do not have no protection of their position of supervision (SCADA) 40%

industrial installations
have a direct connection to
the Internet

53%

industrial installations own systems outdated operating systems

Industrial cybersecurity, an essential element to ensure

Safety of operation

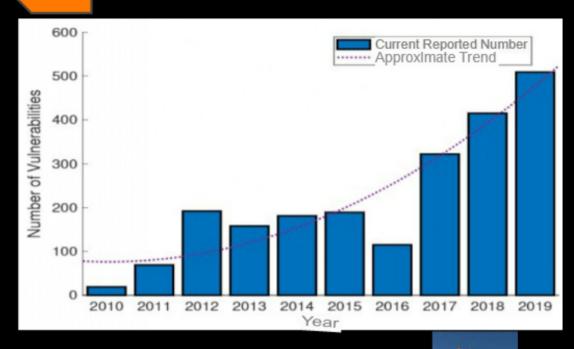
Availability of installation Security functional

Productivity

Maintainability



Intensification of threats



2021- US Oil Pipeline System paralyzed





2017- Not Petya causing €250M of damage to a French industrialist



2015 - Industroyer made breaking the networks electric

2010 - Discovery from the Stuxnet worm



2014-Cyberattack on a steel mill German

ICS Threat Timeline

STUXNET US & Israeli developed malware leveraged to KOSOVO delay the Iranian Nuclear Program's ability to enrich Uranium. The malware targeted Slow ICS and physically destroy Uranium centrifuges US military used cyberattacks along with bombing campaigns to weaken Serbian Air Defense Systems leveraging 4 zero-days

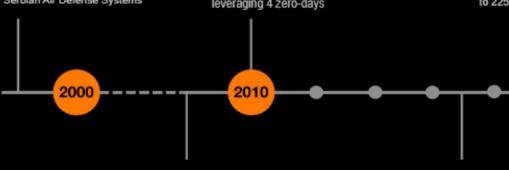
BLACK ENERGY

Russian attack three Ukrainian Energy Distribution Companies. Cutting power to 225,000 civilians

2015

TOYOTA

Toyota subcontractor was attacked by a ransomware. They have to shut down 28 production lines at 14 plants in Japan



OPERATION BUCKSHOT YANKEE GERMAN STEEL MILL

USB flash drive infected by a foreign intelligence agency was connected to a laptop attached to USA Central Command

Attack on ICS controlling blas furnace, resulting in significant physical damage

TRITON

Intrusion into the IT network then rebound to the industrial network to corrupt the program of a safety PLC

NOTPETYA

Russia targeted large Ukraine companies. Estimated to have cost over S10 trillion in damages.

SEEHOTEL JAGERWIRT

CTM-BMS attacked in an Austrian hotel Electronic key system to open & close the doors, the editing of new car and reservation & payment system was blocked.

HOSPITALS

2020

France in 2021, more than 750 cybersecurity incidents have been identified. Hospitals IT system are blocked, from a simple scanner to medical prescription

Summary

- Intensification of menances
- The repositories and regulation
- Our value proposition



International standards

more than 50 international standards*

2 seem to win the membership

IEC 62443

ISO/IEC 27000

Cyber System industrial Generic repository of the safety of information



*Clusif

Summary

- Intensification of threats
- The repositories and regulation
- Our value proposition



Orange Cyberdefense

As a leader
european of
provision of services
of security, we will
let's accompany in the
whole world.

977 €million
CA
in 2022



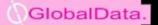
more than 3,000 dedicated multidisciplinary experts to cyber security



8 500 customers in the world, on all sector of activity



Recognized " Very Strong Performer » MSS;



50 billion of events managed all the days by our CyberSOC Note:
" Strong
Perform "
MSS

Forrester

24/7/365

Capacity of services in Follow the

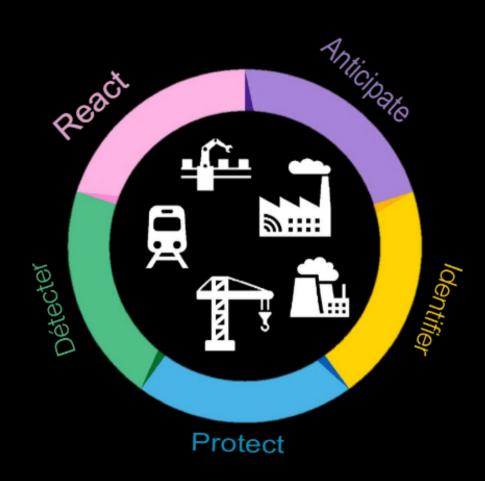
Included In the market gulde Gartner of the best actors in threat detection and management

Gartner



Orange Restricted

360 support to secure industrial systems



Step 1

Diagnose, raise awareness, train, map

Step 2

Backup, restore, segment, access

Step 3

Deploy, monitor, alert

Step 4

Intervene, analyze, rebuild

Step 5

Watch, test, model

Orange Restricted

Our offers



100% OCD Africa





Identify

Protect



Detect



React



Anticipate

Identification of industrial systems

Governance of the security

Classification

Risk analysis

Mapping

ICS Assetinventory

Assessment of maturity

Training

Compliance regulatory

Awareness

IT/OT Segmentation IT/OT Segmentation

Hardening of the equipment

Protection of the workplace

Identity Access management ICS Lock box password

Remote access

OT Segmentation

Decontamination USB flash drives ICS Malware Cleaner

Deployment of probes

Anomaly detection

Cyber SOC

MicroSOC:

Training

Incident response

Cyber resillence

Training

Post-mortem analysis

Threat analysis

Vulnerability watch

Technical monitoring

Intrusion test ICS Ethical Hacking

Training

Layout CS Mock-up)