



# Cyber system industrial



# Summary

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



# Industry 4.0

## Industry 4.0-



# The industry is digitizing



An ever more connected industry  
based on IT standards



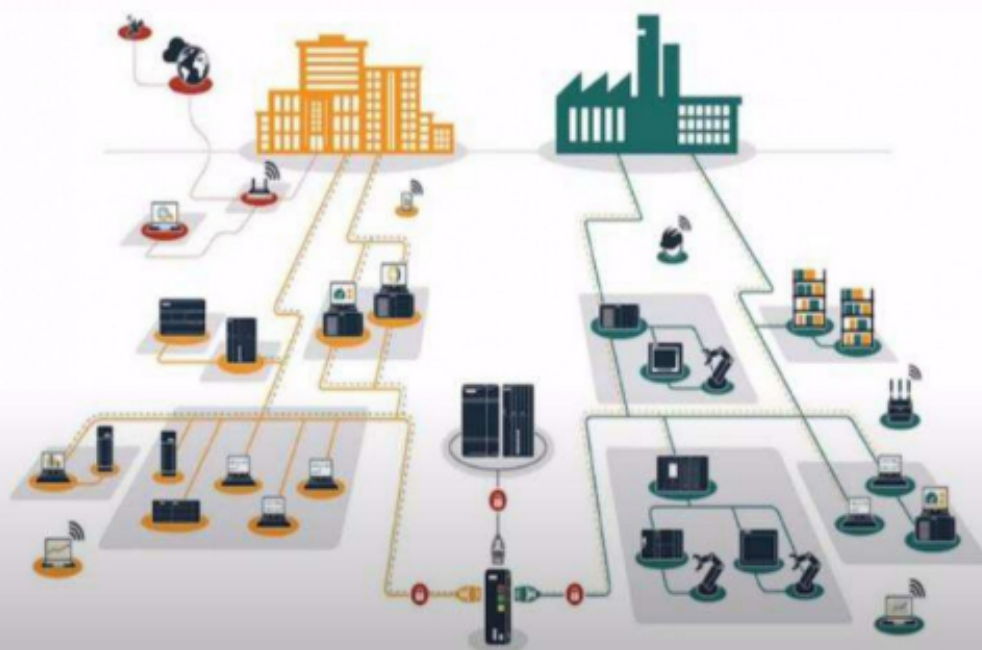
Increases the  
IT/OT convergence



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

”

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.

How to reconcile transformation  
industrial digitalization and cybersecurity

?



# Key figures

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



Source: Ponemon Institute

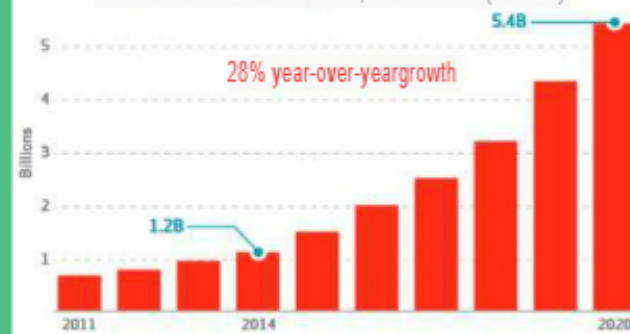
**The most Important Industrial fields affect :**

- Oil & Gas
- Building automation
- Engineering

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



Number of B2B IoT connections, 2011 to 2020 (forecast)



"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

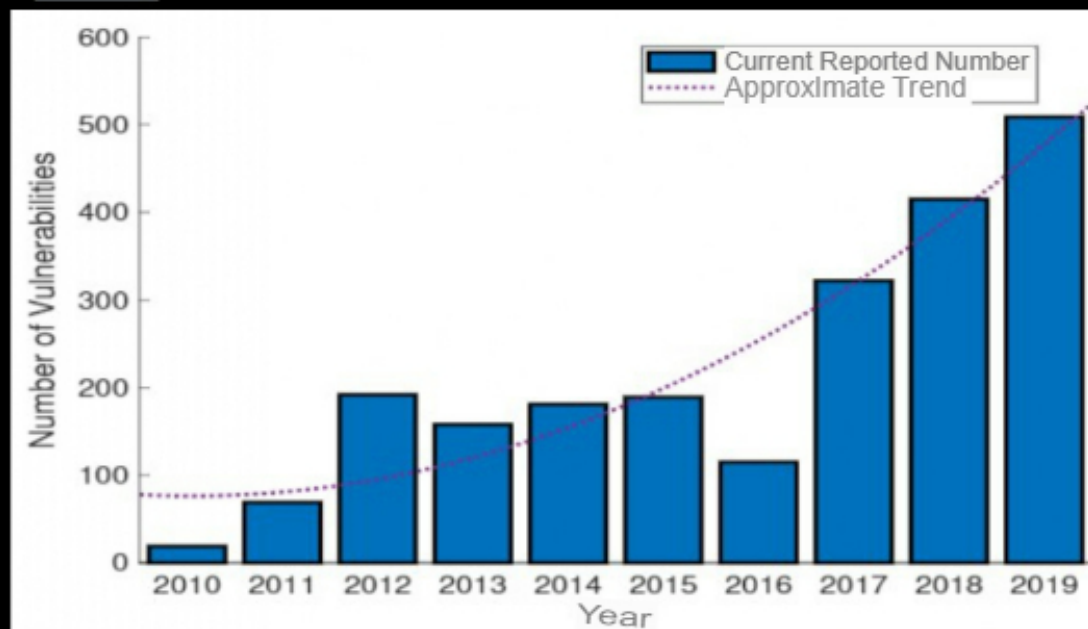
Productivity

Maintainability





# Intensification of threats



2010 - Discovery from the Stuxnet worm



2014-Cyberattack on a steel mill German



2015 - Industroyer made breaking the networks electric



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

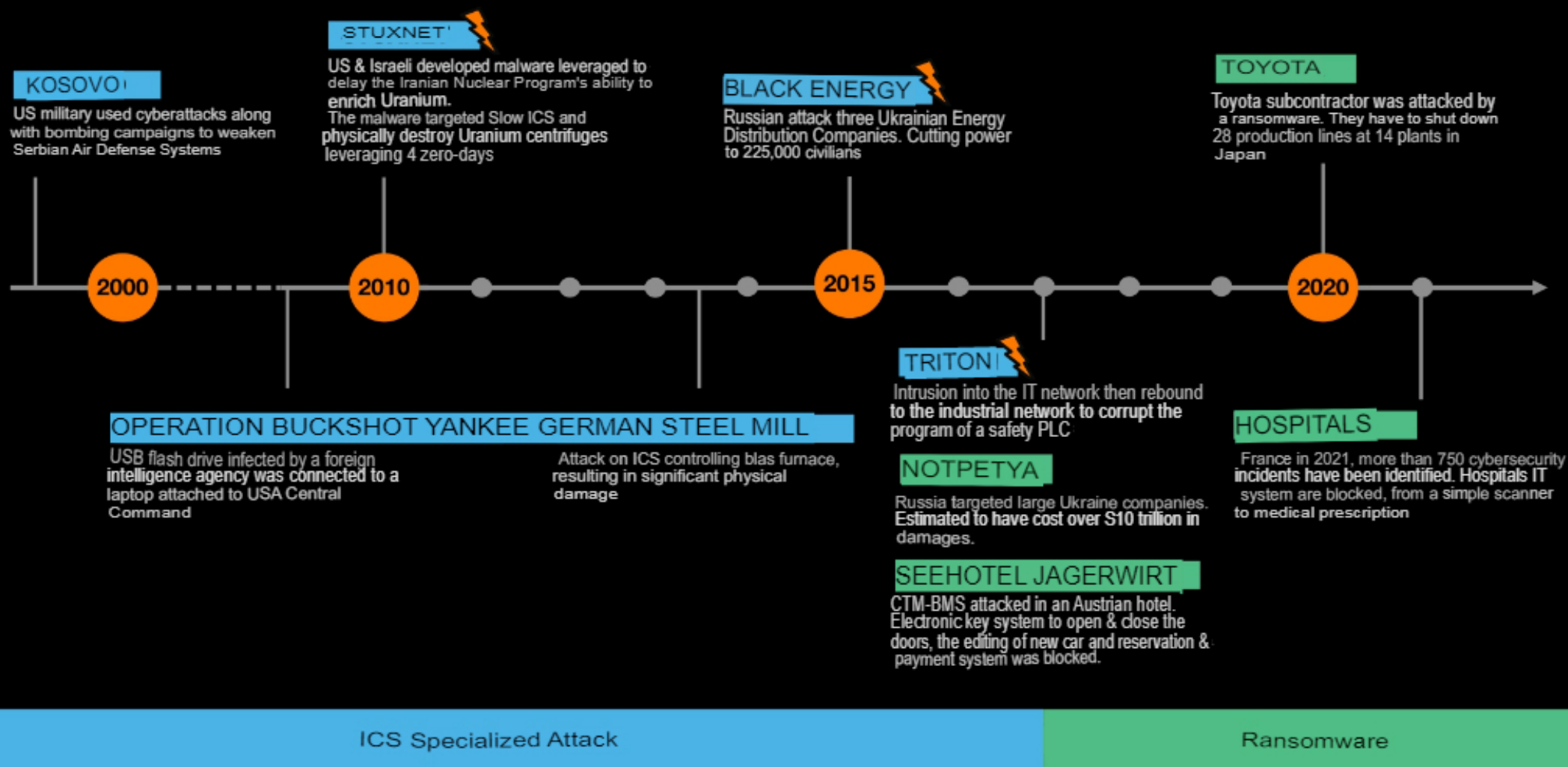


2021- US Oil Pipeline System paralyzed



Increasing impact of attacks

# ICS Threat Timeline



# 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

Cyber  
System  
industrial

ISO/IEC  
27000

Generic repository  
of the safety of  
information

\*Clusif

Orange Restricted





# 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;

 **GlobalData.**

**50 billion**  
of events  
managed all the  
days by our  
CyberSOC

Note:  
" Strong  
Perform " MSS

**Forrester**

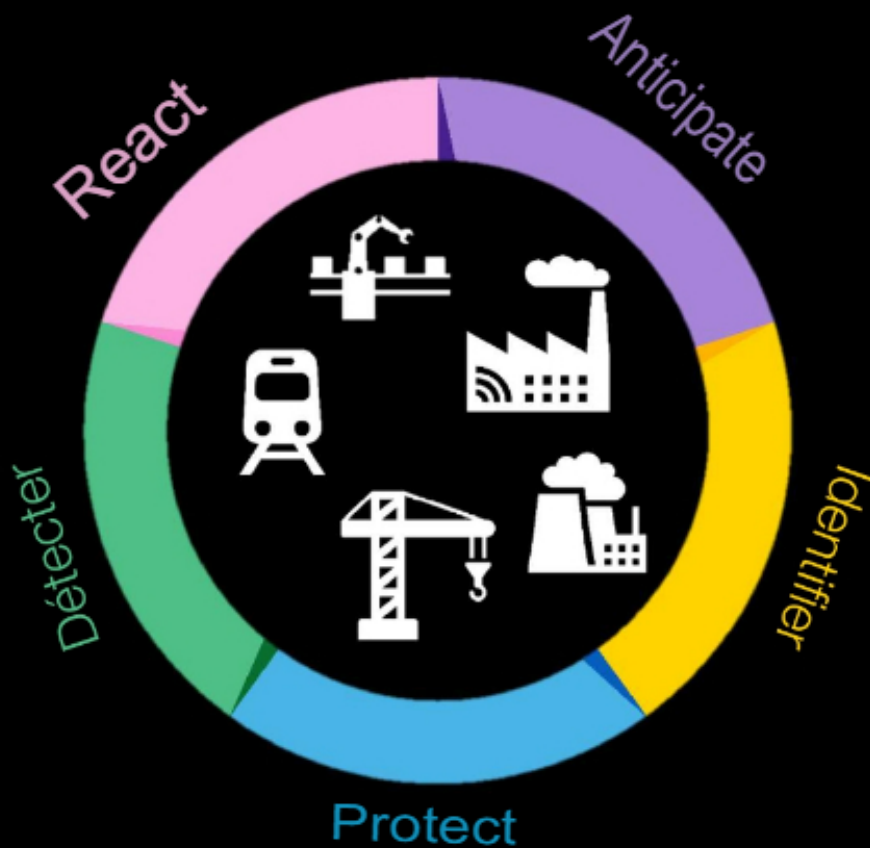
**24/7/365**  
Capacity of  
services in  
" Follow the  
Sun »

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

**Gartner**



## 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

# Our offers



## Identify

Identification of Industrial systems

Governance of the security

Classification

Risk analysis

Mapping  
ICS Asset inventory

Assessment of maturity

Training

Compliance regulatory



## Protect

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



## Detect

Deployment of probes

Anomaly detection

Cyber SOC:

MicroSOC:

Training



## React

Incident response

Cyber resilience

Training

Post-mortem analysis



## Anticipate

Threat analysis

Vulnerability watch

Technical monitoring

Intrusion test  
ICS Ethical Hacking

Training

Layout  
ICS Mock-up

Hybrid OCD France /  
OCD Africa

100% OCD Africa