Convergenza IT/OT e Cyber Resilienza Operazionale nel Settore Trasporti

NOVEMBER 2022

ENGINEERING
CYBERTECH
ENGINEERING GROUP

Agenda

- **Engineering Cybertech at a glance**
- OT Cybersecurity Trends & Challenges
- Cybertech Approach and Solution

At a Glance: a Global Company

1.24 B€
REVENUE FY2020

+20
M&A LAST 4 YEARS

+11.600
ASSOCIATES

+1.000
NEW HIRES PER YEAR

+16.000
PROJECTS IN 2020

+40
OFFICES AROUND THE WORLD

GLOBAL HQ
ROME, ITALIY

OFFICES IN EUROPE, NORTH AMERICA, LATIN AMERICA

RESEARCH & INNOVATION

+40m€ Investments / YR
+100 Active Research Projects
+450 Data Scientists and Researchers

IT & MANAGEMENT ACADEMY
"ENRICO DELLA VALLE"

15.000 Man Days of Training / YR
+1.000 Professional Certifications
+5.400 Courses & E-learning Courses

Cybertech / Engineering's Cybersecurity Company

6
International Branches

Enabling a Secure Digital Transformation for your organization.

We protect your data, networks and infrastructures and ensure a safe digital space for your employees, clients and partners.

Members of **Organization for Security (EOS)** and **European Cyber Security Organization (ECSO)**

300+
Cybersecurity Specialists

550+
Individual Certifications

450
Clients

20+
Client Countries

20 petabyte
Of Data Protected

22K
Servers

1
Certified SOC ISO27001/2017

3
SOC Control Rooms: Rome / Zurich / Belgrade

3
Certified datacenters Tier IV, AGID, ISO27001/2013, TIA-942

1
Vulnerability Assessment Lab ISO17025/2018

ADVISORY

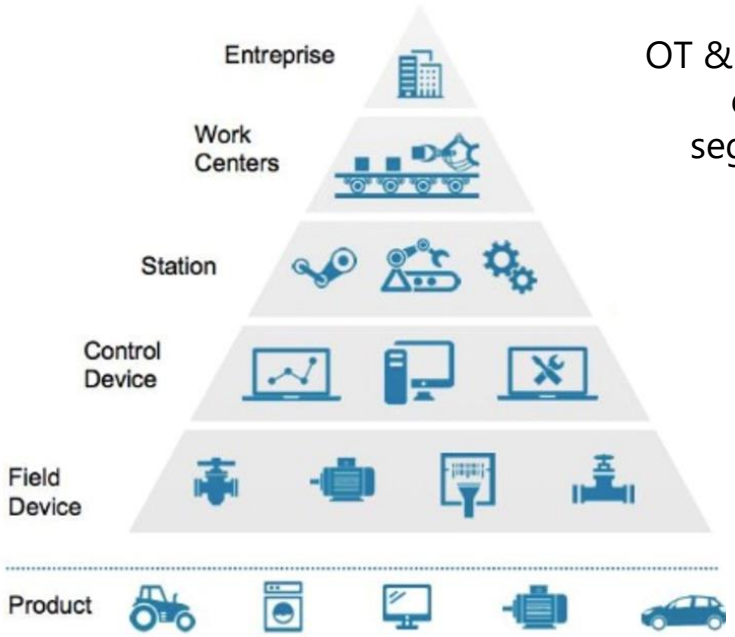
TECHNOLOGY & IMPLEMENTATION

MANAGED SECURITY SERVICES

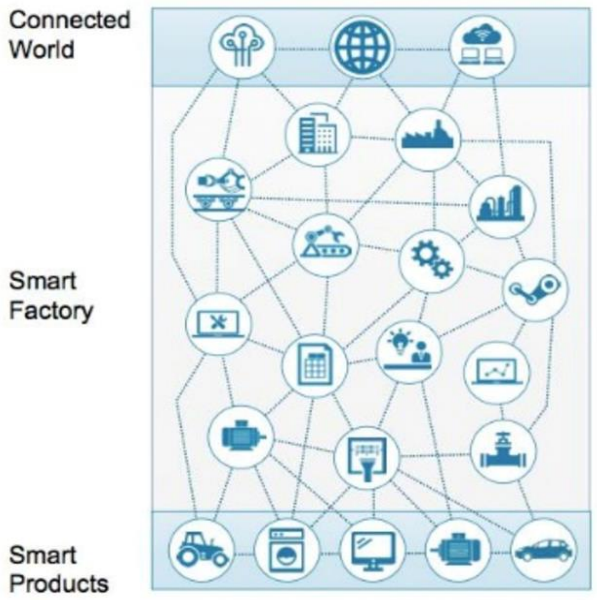
Agenda

- Engineering Cybertech at a glance
- **OT Cybersecurity Trends & Challenges**
- Cybertech Approach and Solution

A Connected World



OT & IT convergence: networks are now connected distributed and most of the time without segregation and segmentation between them



Traditional Isolated Silos

Connected World

The Reality of Cyber Attacks to IACS Infrastructures

Incidents range from what I call commodity-type malware, which could be a Trojan design dealing with banking information that is proliferating around the Internet accidentally getting into an industrial control system and infecting the machines, or it could range all the way out to a significant, advanced and persistent threat from a nation-state-level actor who is very surgically and specifically targeting that control system for whatever the reason is.

Marty Edwards
Director of Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
U.S. Department of Homeland Security

2020-21

- US Natural Gas Operator
- Ekans Ransomware on Honda
- Water Treatment Facility FL
- Colonial Pipeline

2019

- ASCO Belgium
- PILZ manufacturing Germany
- Deutsche Bahn

2018

- Automotive Giants
- Cathay Pacific

2015

- Ukrainian Power Grid
- Company's water treatment plant

2014

- German Steel Mill

Outdated IACS and IoT smart devices further expand the attack surface

Cyber-attacks on smart buildings, along with related attacks on smart cities and infrastructure, can have wide-ranging impacts and can pose risks to human safety. An attack in a large public building or structure (particularly in a densely populated area), could potentially cause chaos.

> **ARC Advisory Group**
> Cybersecurity for Smart Buildings

Less-than-perfect software patching, outdated operating systems, and above all insufficient network segmentation. That last vulnerability in particular … could allow malware with access to one part of the network to spread wildly beyond its initial foothold, exactly as NotPetya would the next year.

> **WIRED**
> The Untold Story of NotPetya
> the Most Devastating Cyberattack in History

CPO MAGAZINE

Hackers Use Smart Building Technology Access Control Systems to Launch DDoS Attacks
February 2020
Access control systems are typically installed in corporate headquarters, industrial facilities, and factories. They are designed to control the doors through which employees and visitors can pass by using a system of access cards.

The MARITIME EXECUTIVE

Cyberattack Penetrated Cargo Facility's Operating Controls
November 2020
A cyberattack on a U.S. maritime facility targeted cameras and physical access control systems with the Ryuk ransomware, disrupting the network.

CBS NEWS

Ransomware Attack Shut Down Some Michigan Schools
January 2020
District officials said that attackers gained access to the IT network via heating and cooling systems, causing three schools to close for a week.

THE WALL STREET JOURNAL

Atlanta International Airport Hit With Cyberattack
March 2018
The Hartsfield-Jackson Atlanta International Airport's Wi-Fi service was down Friday amid a cyberattack on the city.

Timeline of notable Ransomware Attacks to OT/IACS infrastructure in recent past

Samples of ransomware attacks from around the world that either disrupted operations or involved large ransom demands

FEBRUARY 2021
Kia Motors[31]
Automobile Manufacturer
Ransomware Group: DoppelPaymer
Ransom Demand: $20 Million
Ransom Paid: Unknown

MARCH 2021
Acer[32]
Computer Manufacturer
Ransomware Group: REvil
Ransom Demand: $50 Million
Ransom Paid: Unknown

MARCH 2021
CNA Financial[33]
Cybersecurity Insurance Provider
Ransomware Group: Phoenix
Ransom Paid: $40 Million

APRIL 2021
RaceTrac Petroleum[34]
Retail Gasoline Company
Ransomware Group: Clop
Ransom Paid: Unknown

APRIL 2021
Quanta[35]
Technology Supplier
Ransomware Group: REvil
Ransom Demand: $50 Million
Ransom Paid: Not Paid

MAY 2021
Colonial Pipeline[36]
Fuel Pipeline
Ransomware Group: DarkSide
Ransom Paid: $4.4 Million

MAY 2021
Brenntag[37]
Chemical Distribution Company
Ransomware Group: DarkSide
Ransom Demand: $7.5 Million
Ransom Paid: $4.4 Million

MAY 2021
AXA Group[38]
Cybersecurity Insurance Provider
Ransomware Group: Avaddon
Ransom Paid: Unknown

MAY 2021
Irish Department of Health[39]
Healthcare Services
Ransomware Group: Conti
Ransom Demand: $20 Million
Ransom Paid: Not Paid

MAY 2021
JBS Foods[40]
Global Meat/Protein Producer
Ransomware Group: REvil
Ransom Paid: $11 Million

Reference Standards for OT Security

International Electrotechnical Commission
IEC 62443 (series) Industrial communication networks -Network and System Security

International Society for Automation
ISA 99 (series) is a framework for Industrial Automation and Control System (IACS) Security

SP 800-82 Guide to Industrial Control System (ICS) Security, NISTIR 7628 Guidelines for Smart Grid Cyber Security

Critical Infrastructure Protection (CIP) -002 through -011

Guidance for Addressing Cyber Security in the Chemical Industry

Protecting Industrial Control Systems - Recommendations for Europe and Member States

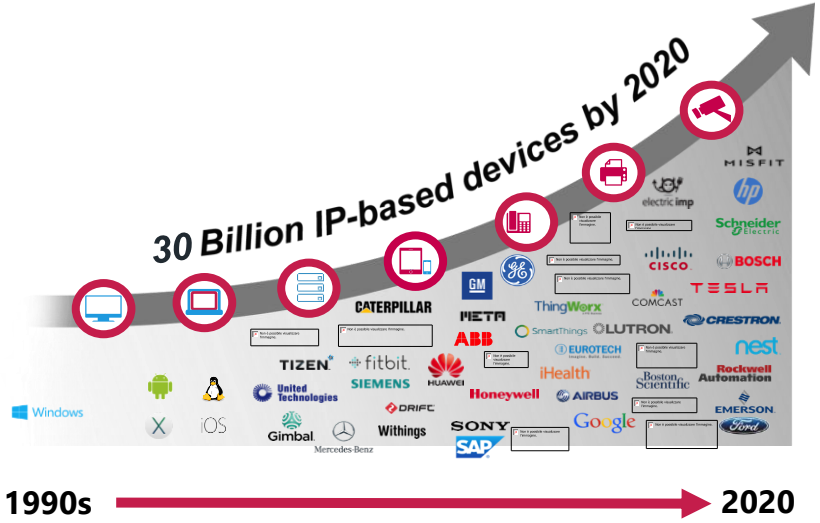
Guidance of Security for Industrial Control Systems

Consequences of a Cyber Attack to OT and Transportation Infrastructures

- Business Continuity and Availability of Critical Components of the Transportation chain
- Data Confidentiality and Integrity, including Data Breach, Data Manipulation, Config Exfiltration
- Delay on Scheduling
- **Safety compromised**
- **Environment compromised**
- Regulatory breaches / financial penalties
- Financial Loss or Impacts
- Damage to Company Image
- Loss of customers

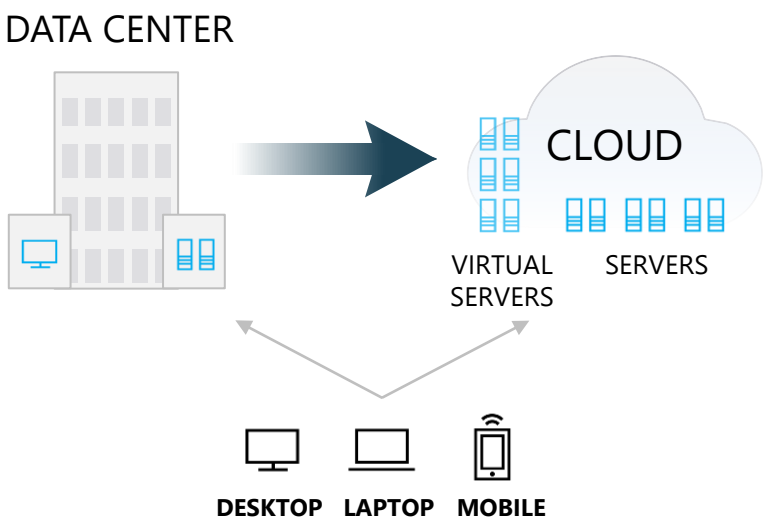
3 Trends specifically amplify the Cybersecurity risk for OT and Trasportation Infrastrucuture

Growth of Devices & Platform Diversity with associated Vulnerabilities



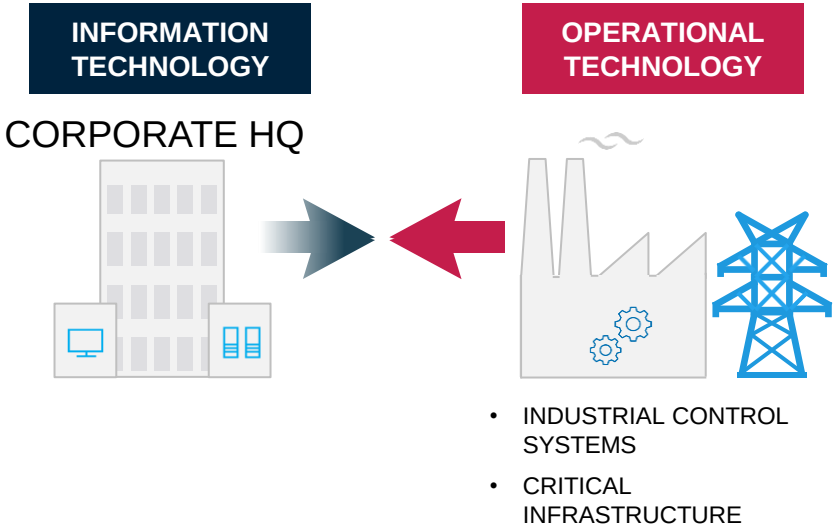
- Innumerable device-specific operating systems (OS)
- Cannot get agents onto new devices
- Cannot write agent-based software for every OS

Cloud Adoption, Mobility and Remote Working Create New Challenges



- Multiple Device Locations and Access Points
- Heterogeneous Environment with Multiple Vendors
- De-centralized Management

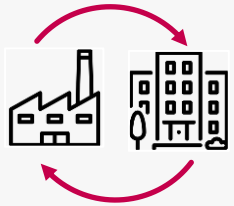
OT Convergence With IT amplifies Risk



- OT networks are no longer physically separated
- Threats moving between cyber & physical dimensions
- Assets are highly vulnerable & rarely can be patched

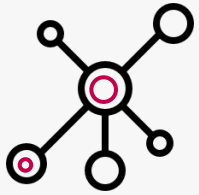
Cybersecurity Challenges in the OT/ICS environment / combined with Network & day-to-day operation issues

Cybersecurity
(Visibility, Vulnerability, Threat Detection)



- No (to limited) visibility in OT networks
- Inability to discern if systems are vulnerable
- Complex and clunky integration into SIEM and other enterprise tools
- Slow and expensive threat detection and response time

Networking



- No network maps
- No segmentation
- Inability to monitor and understand packet/traffic flows
- Lack of device compliance (Is my switch configured correctly?)

Operations

- No real-time asset inventory
- Inaccurate tracking device firmware and model information
- Incomplete vendor and contractor activities
- Cost and often inability of site visits to field

OT Security for Critical Transportation Infrastructures

Core Functions and Technology Areas

- Asset discovery, visibility, profiling, classify and tracking, also used for OT asset & network hygiene and inventory.
- Core Operational Network Security, Segmentation, Network IPDS.
- Advanced Network traffic analysis and threat detection.
- Core Endpoint and Server protection (hardening, antimalware, and core host EPP).
- Advanced Host Anomaly Detection and Vulnerability Management (including asset configuration integrity and firmware protection).
- Access Control and Secure Remote Access from external parties.
- Security Governance & Risk Management according to ISA99-IEC62443.

Agenda

- Engineering Cybertech at a glance
- OT Cybersecurity Trends & Challenges
- **Cybertech Approach and Solution**

Operational Cyber Resilience / The overall and primary objective of OT Cybersecurity

Device Visibility, Identification and Protection

See in real-time what your OT network devices are doing, their vulnerabilities, and protect against along with defending the integrity of crucial operational processes and system health, to mitigate the risk of unexpected downtime while lowering operational costs

Threat and Anomaly Detection

Catch known and unknown threats at their earliest stages to stay ahead of targeted or common attacks and prevent breaches

Control, Respond and Recover

Know what's going on at all times and easily share that data with the organization for a fast and effective reaction to breaches and auditable recover





Multi-layered Defense for IT & OT Security

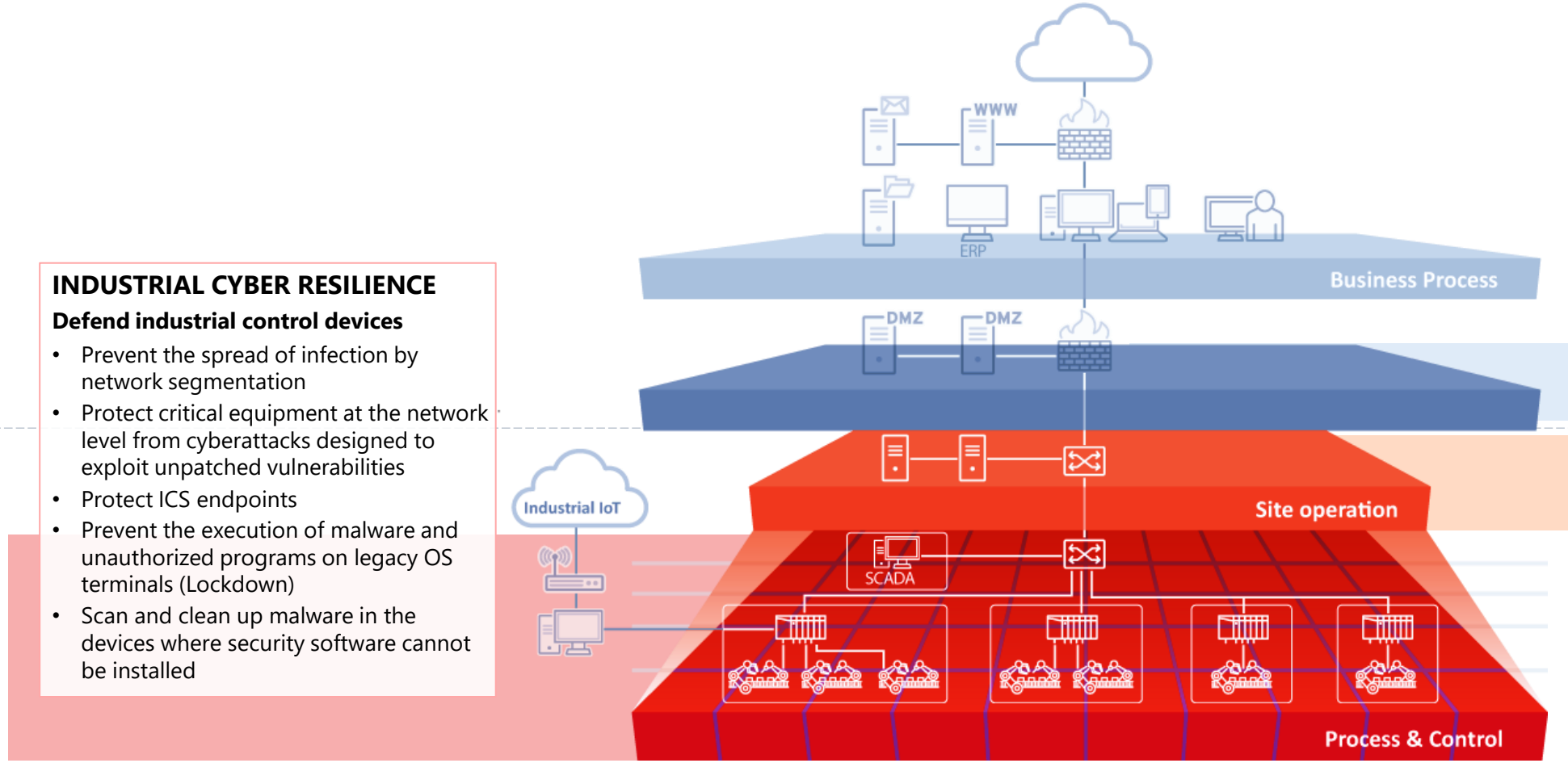
Core capabilities applied to **IT & OT layers**

IT

Enterprise Zone

OT

Manufacturing Zone



INDUSTRIAL CYBER RESILIENCE

Defend industrial control devices

- Prevent the spread of infection by network segmentation
- Protect critical equipment at the network level from cyberattacks designed to exploit unpatched vulnerabilities
- Protect ICS endpoints
- Prevent the execution of malware and unauthorized programs on legacy OS terminals (Lockdown)
- Scan and clean up malware in the devices where security software cannot be installed

PROTECT BY SEGREGATION IT vs OT

Stop cyberattacks moving from the IT environment to the OT infrastructure

- Perimeter defense to prevent cyberattacks designed to exploit vulnerabilities
- Protection of various IoT devices such as IoT gateways used in industrial services

IDENTIFY OT ASSETS and DETECT TRAFFIC ANOMALIES

Identify internal activities and monitor the insurgence of cyberattack over the OT environment

- Gain visibility into the asset configuration and connections of production devices
- Monitor network traffic from multiple perspectives. Receive early detection of suspicious movements

Cybertech Portfolio and major Use Cases for Defending Operational Technologies

OT Assessment

- High- and low-level risk assessment
- Business impact analysis and reporting
- Risk priority driven remediation plan

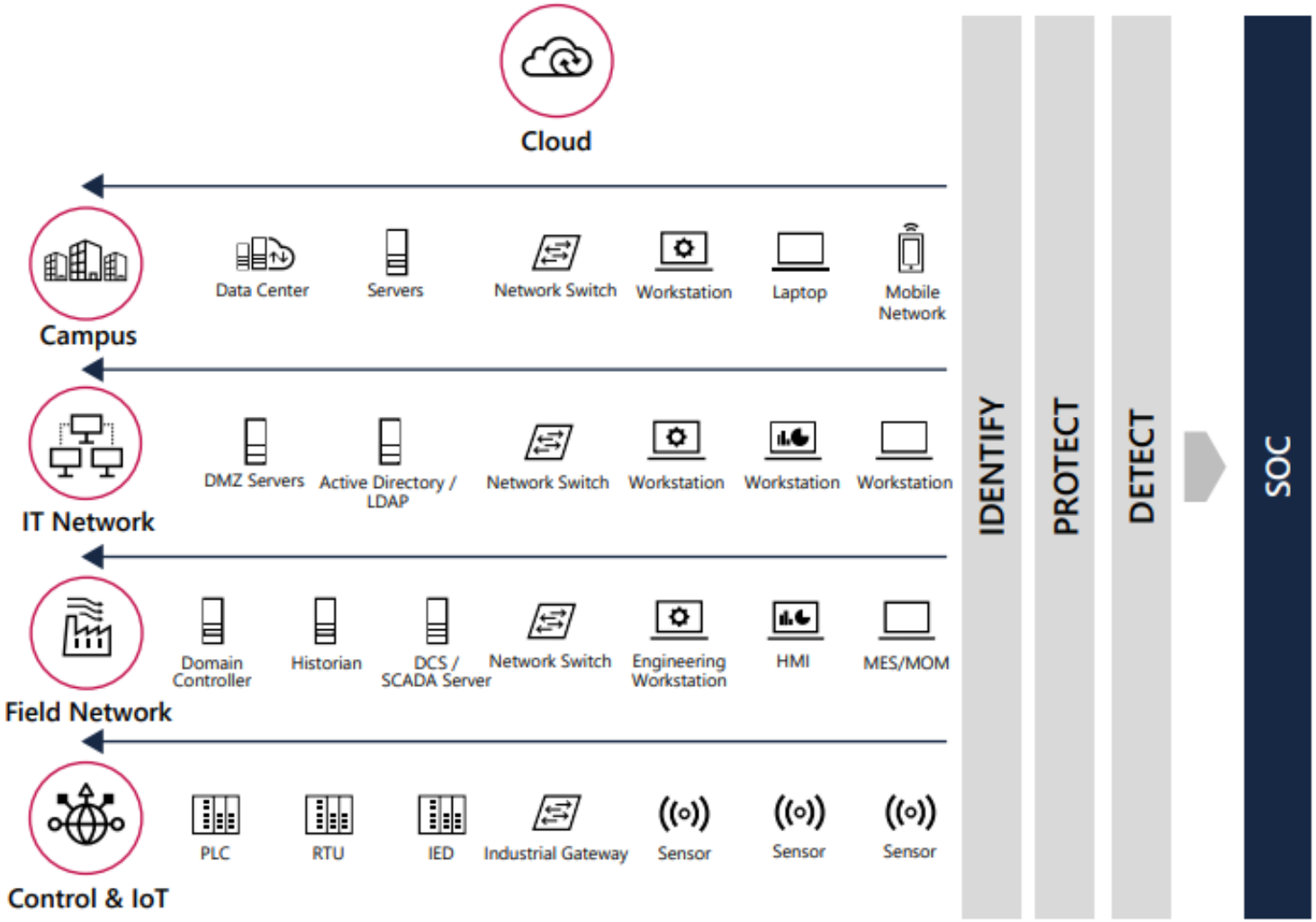
OT Visibility, Protection and Anomaly Detection

- OT Network segmentation and protection (IPDS)
- Asset discovery and inventory
- Network scanning & traffic capture for threat detection
- Vulnerability management, anti-malware and host hardening
- Integrity monitoring

OT Secure Remote Access

- Centralized access requests
- Outbound Connection on encrypted tunnels w granular access rules
- Password Management and MFA
- Session Management for Auditing

OT Ready Service Model



A consolidated "**OT Ready" service model** able to integrate vertical and multilayered IT-OT defense with horizontal identify-protect-detect-respond capabilities.

Our **implementation capability and MSS/SOC** align to industry processes and standards to offer best of breed risk mitigation strategies and prove conformity.

Thanks

Aldo Lentini
Principal Security Architect - R&D Manager

www.eng.it

Engineering Ingegneria Informatica SpA

@EngineeringSpa

gruppo.engineering

LifeAtEngineering