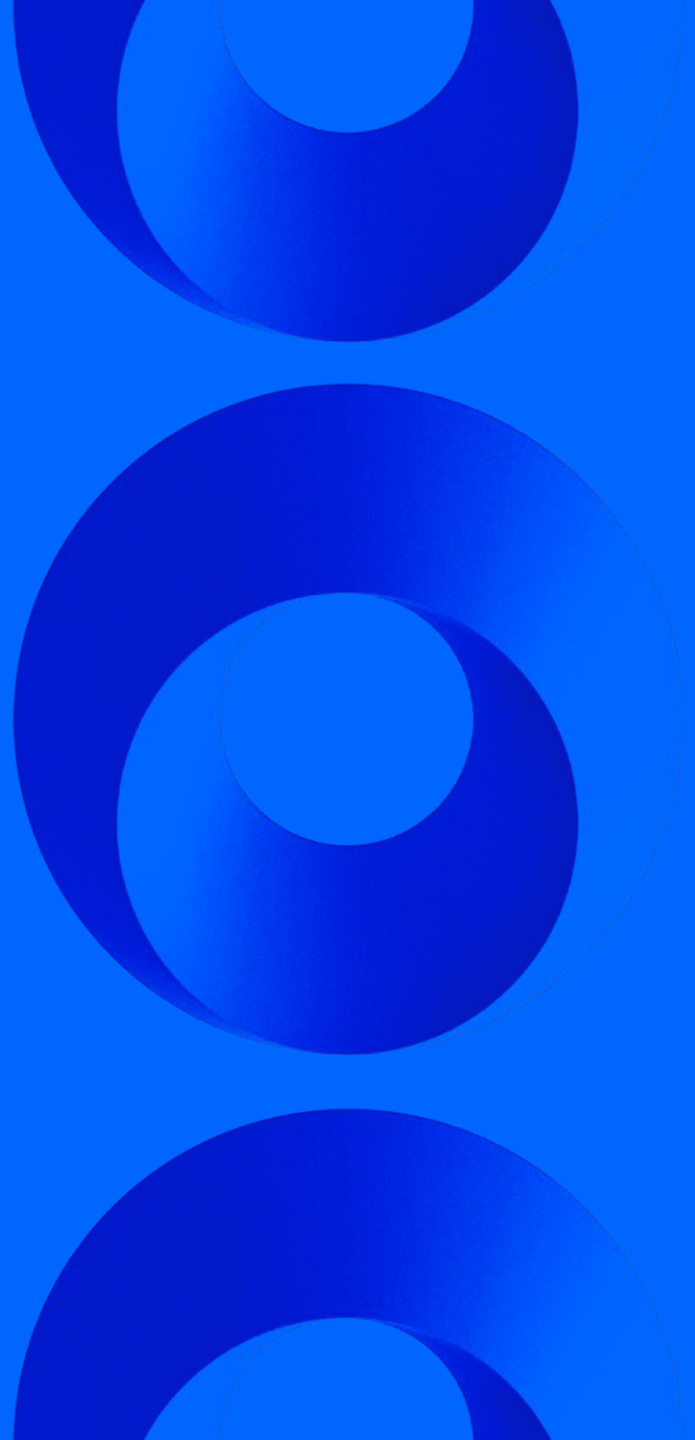


# Industrial Cybersecurity Challenges and Solutions

Helping our customers to securely  
embrace the next digital wave

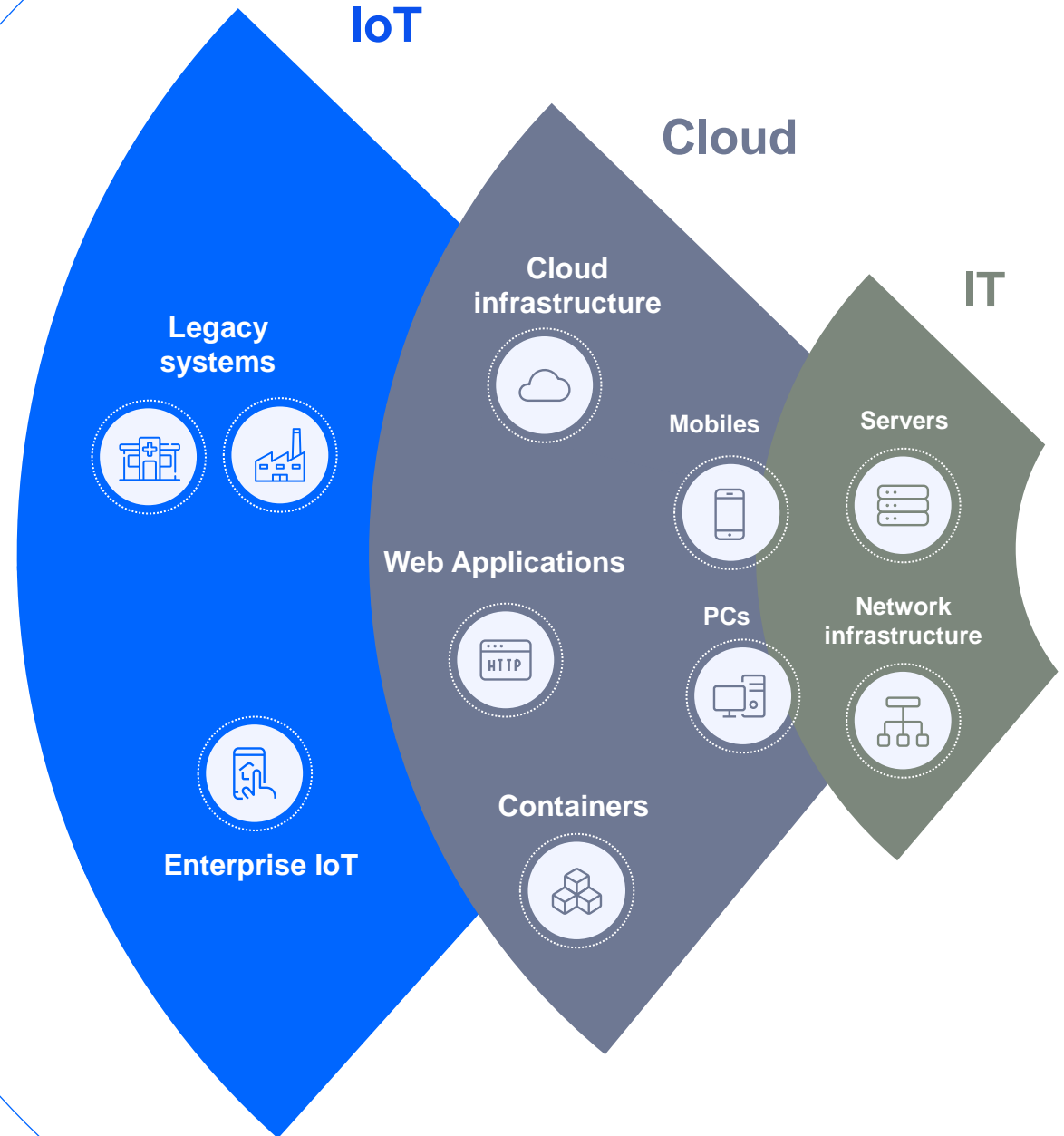
# Challenges



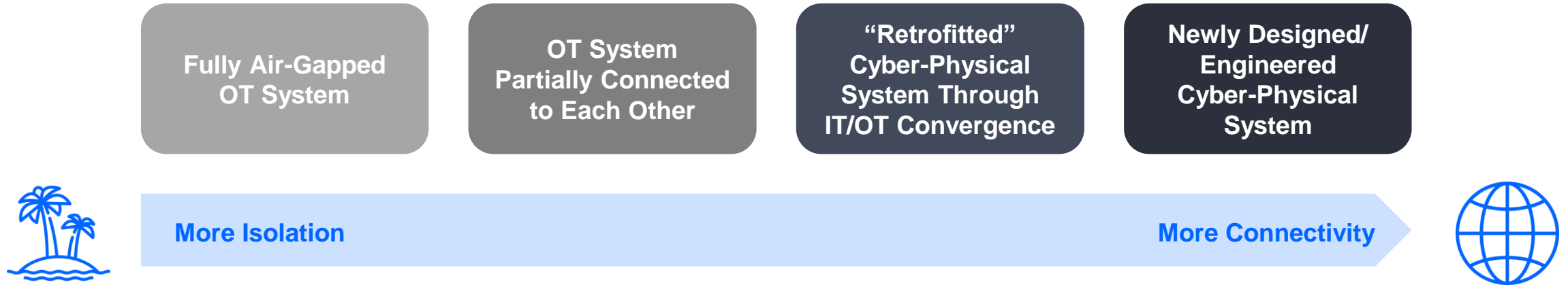
CYBERSECURITY CHALLENGES

# Internet of Things

New wave in digital evolution...  
Increases your attack surface



# OT Systems Evolution



## Examples of Traditional OT Systems

- Supervisory Control and Data Acquisition (SCADA)
- Industrial Control Systems (ICS)
- Programmable Logic Control (PLC)
- Process Control Networks (PCN) – Including Safety Instrumented Systems (SIS), Engineer Workstation and Human Machine Interface (HMI)
- Distributed Control Systems (DCS)
- Computer Numerical Control (CNC)

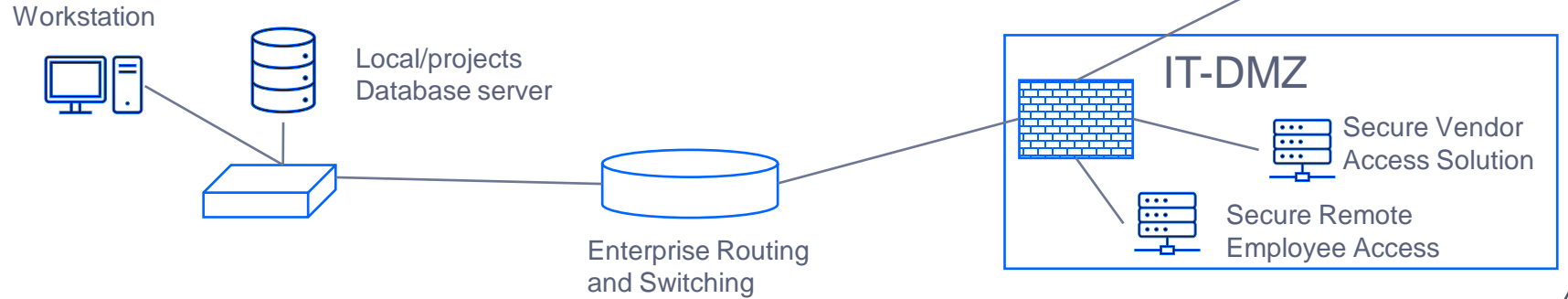
## Examples of OT-Related Cyber-Physical Systems

- Industrial Robots
- Virtual Reality Manufacturing Simulation Systems
- Self-Optimizing Press-Bending and Roll-Forming Machine
- Adaptable Production Systems
- Energy-Efficient Intralogistics Systems
- Connected 3D Printers
- Smart Grids

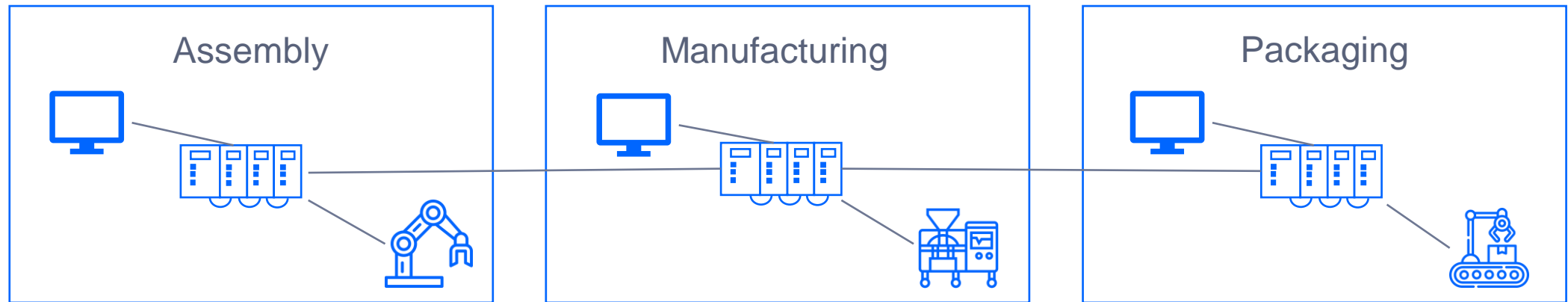
# Fully Air-gapped OT system (at the end of 1990s)



## Office Network



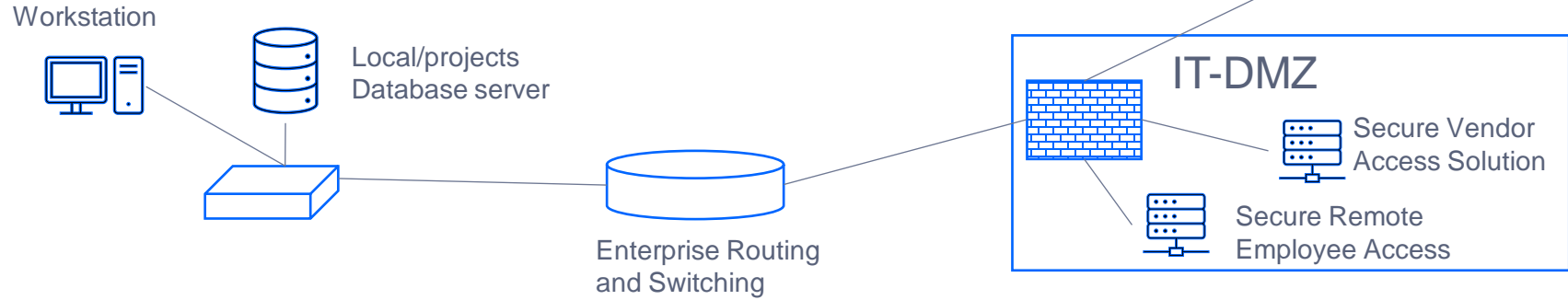
## Production Network



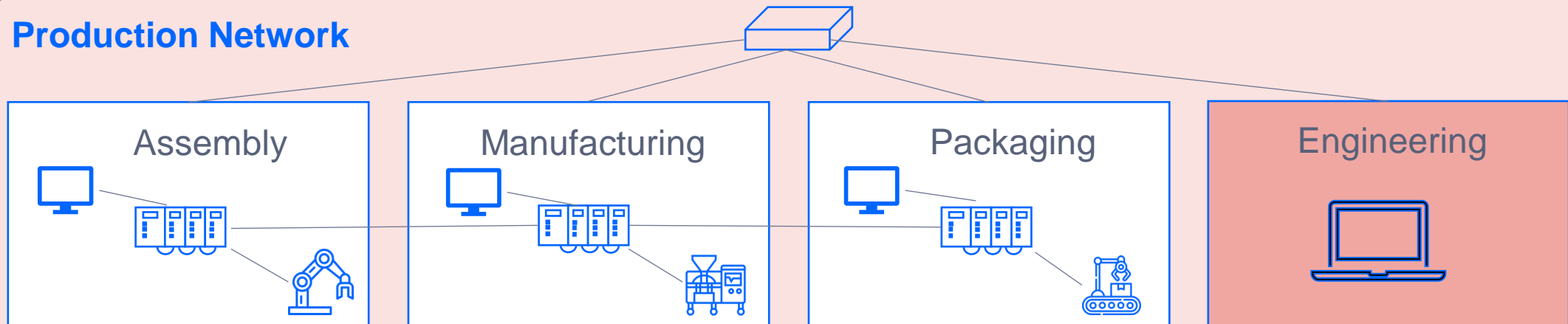
# OT Systems starts connecting to each other (2005-2010)



## Office Network

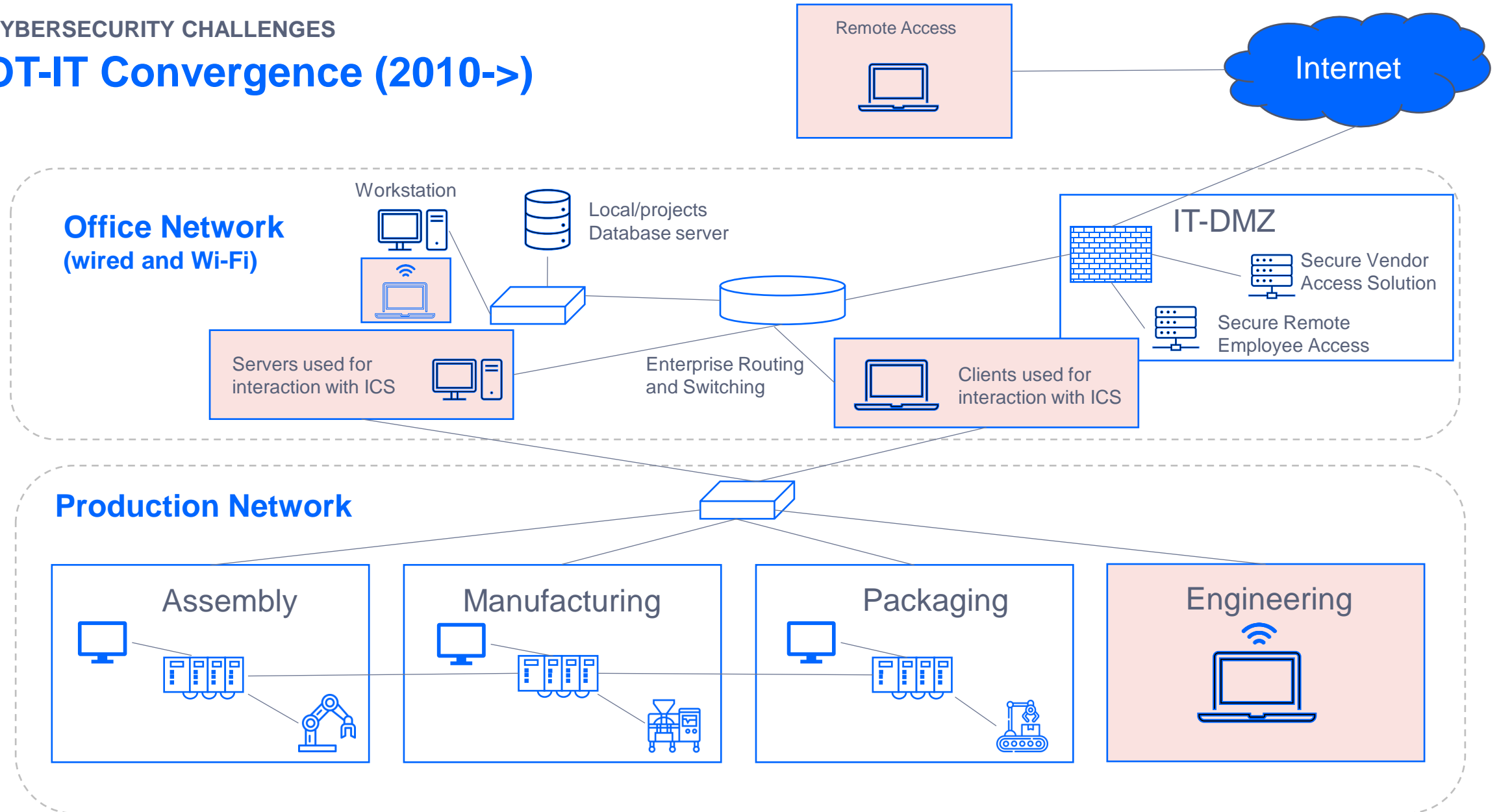


## Production Network



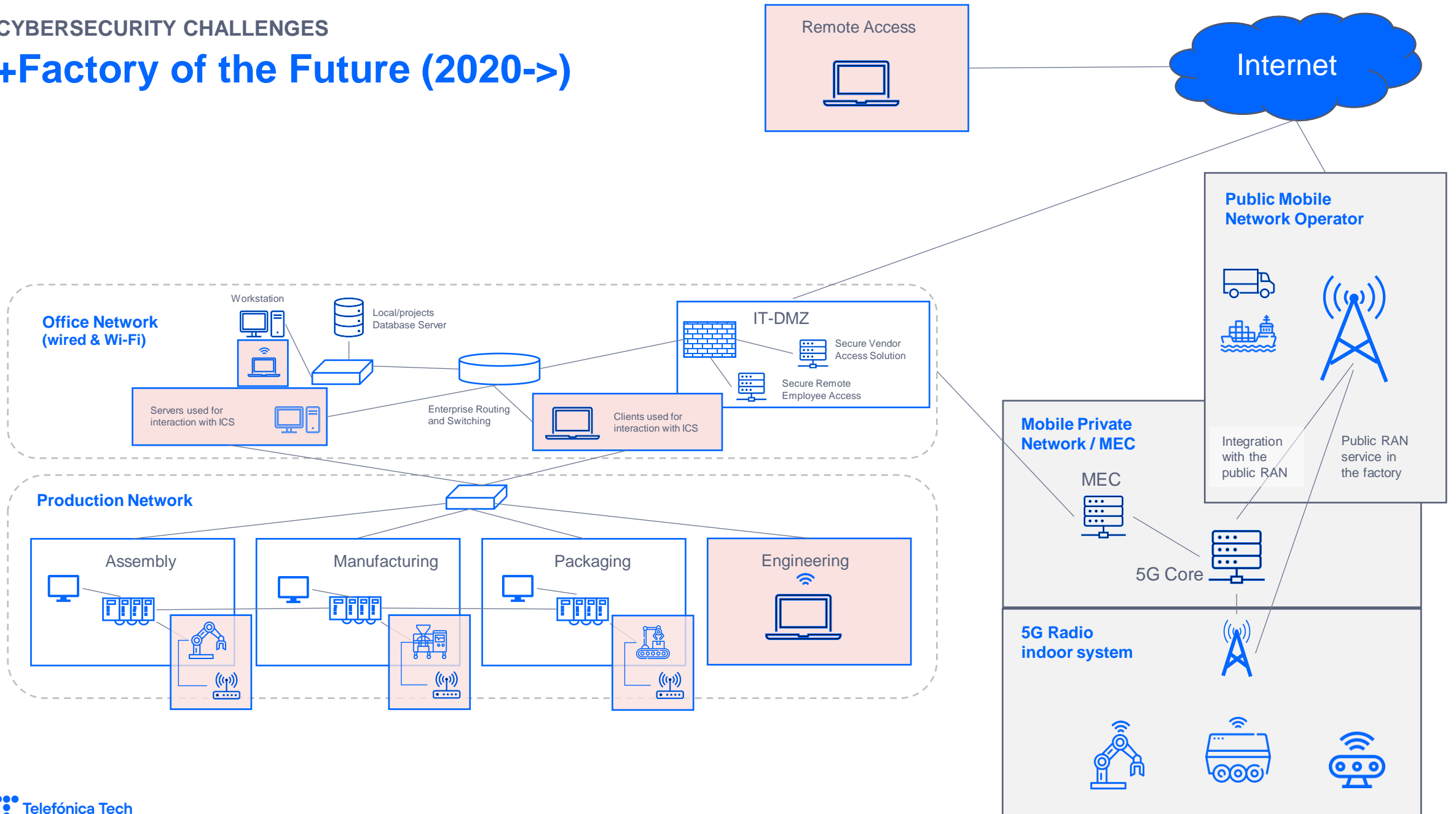


# OT-IT Convergence (2010->)



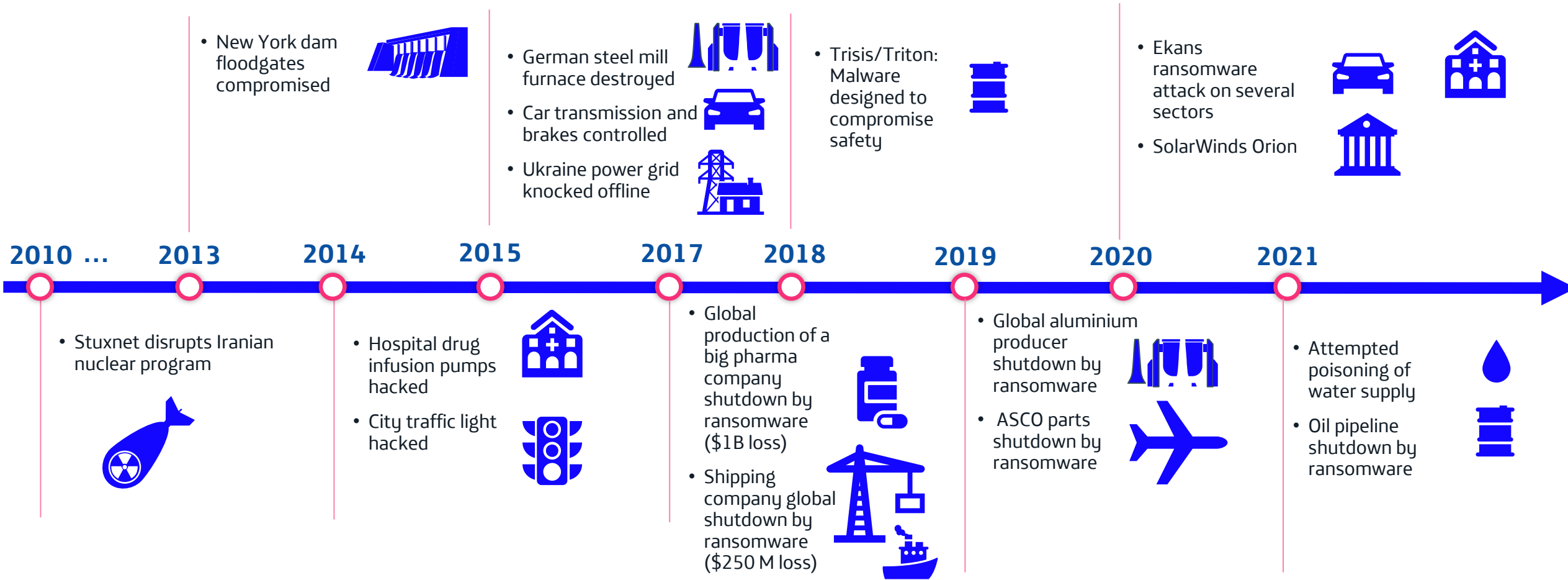
# CYBERSECURITY CHALLENGES

## +Factory of the Future (2020->)





# Summary of the most relevant incidents affecting industrial infrastructures



# Cybersecurity challenges of industrial organizations: our experience



## Short-term challenges

What do I have in the factories?  
What risks is my organization exposed to?



## Medium-term challenges

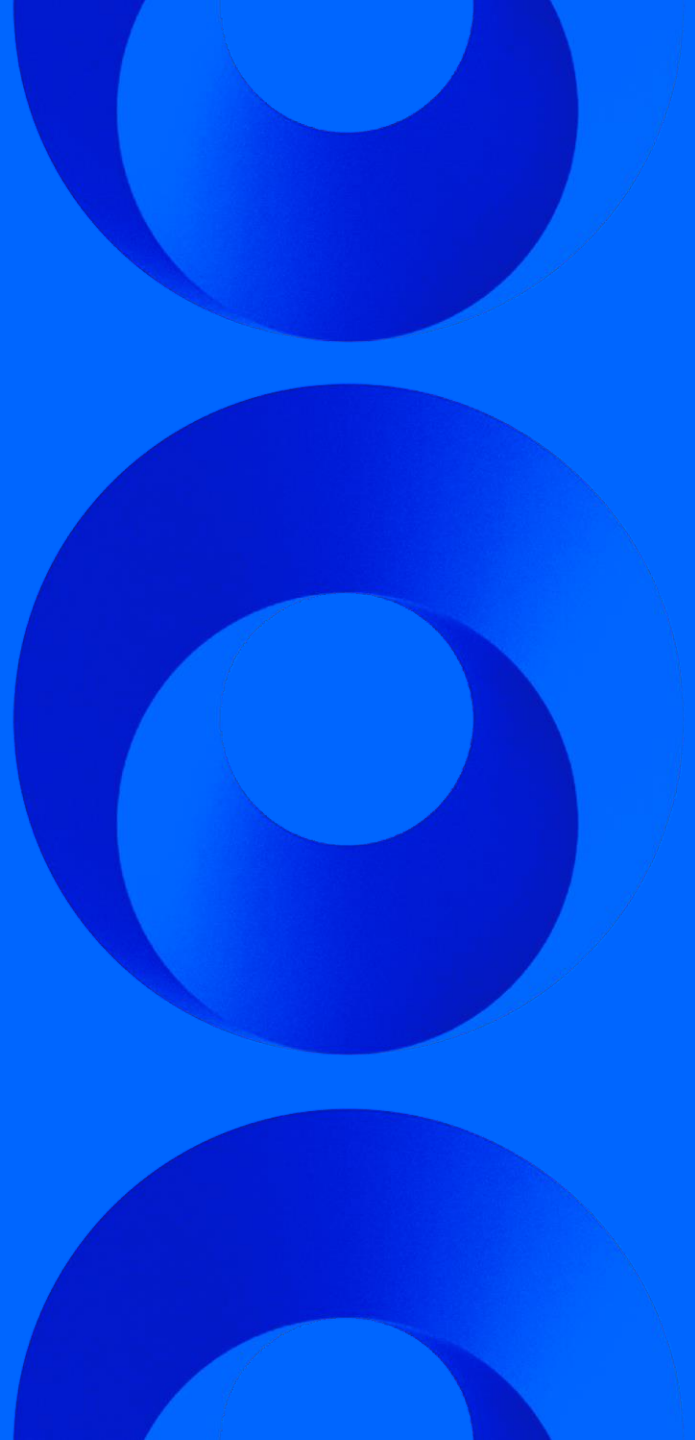
What can I do to be more resilient?  
What cybersecurity solutions do I start with?



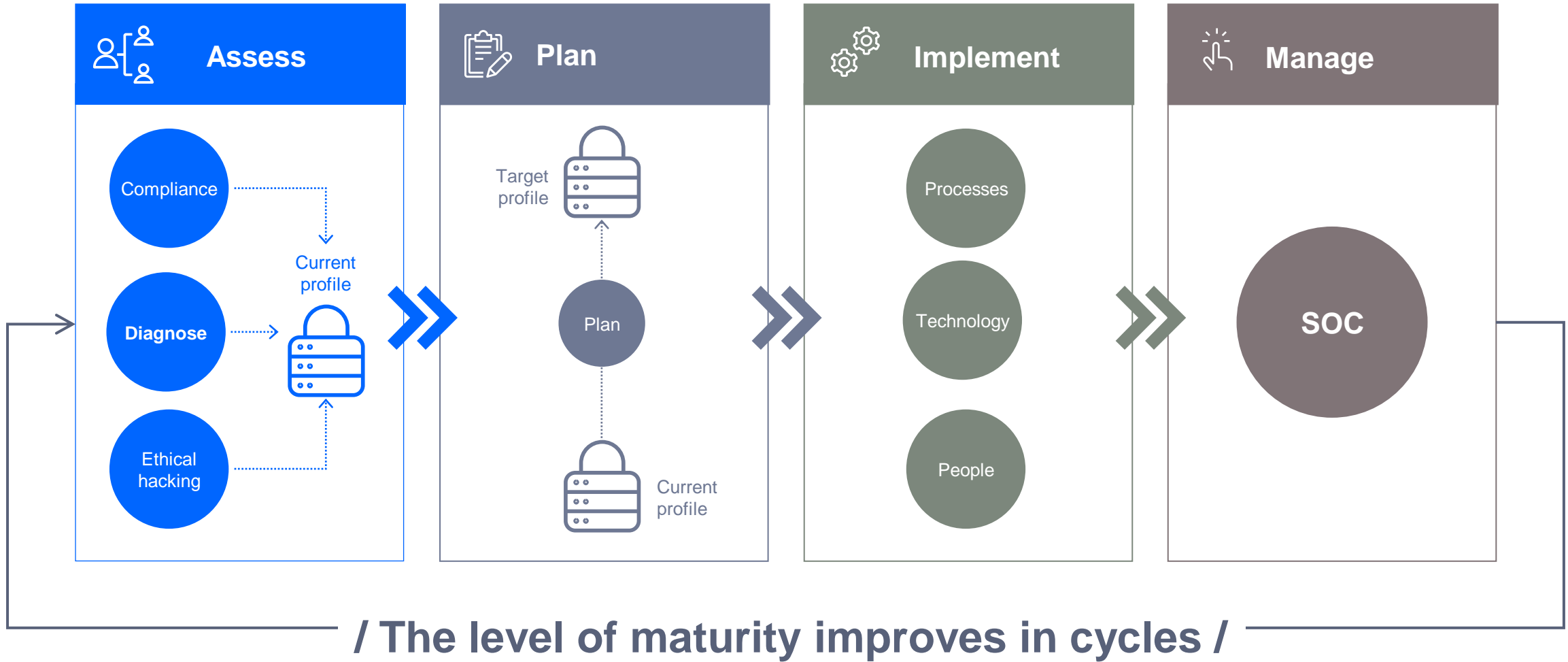
## Long-term challenges

What security requirements must be met by these services that are not yet 100% defined?  
How can I meet my budget?

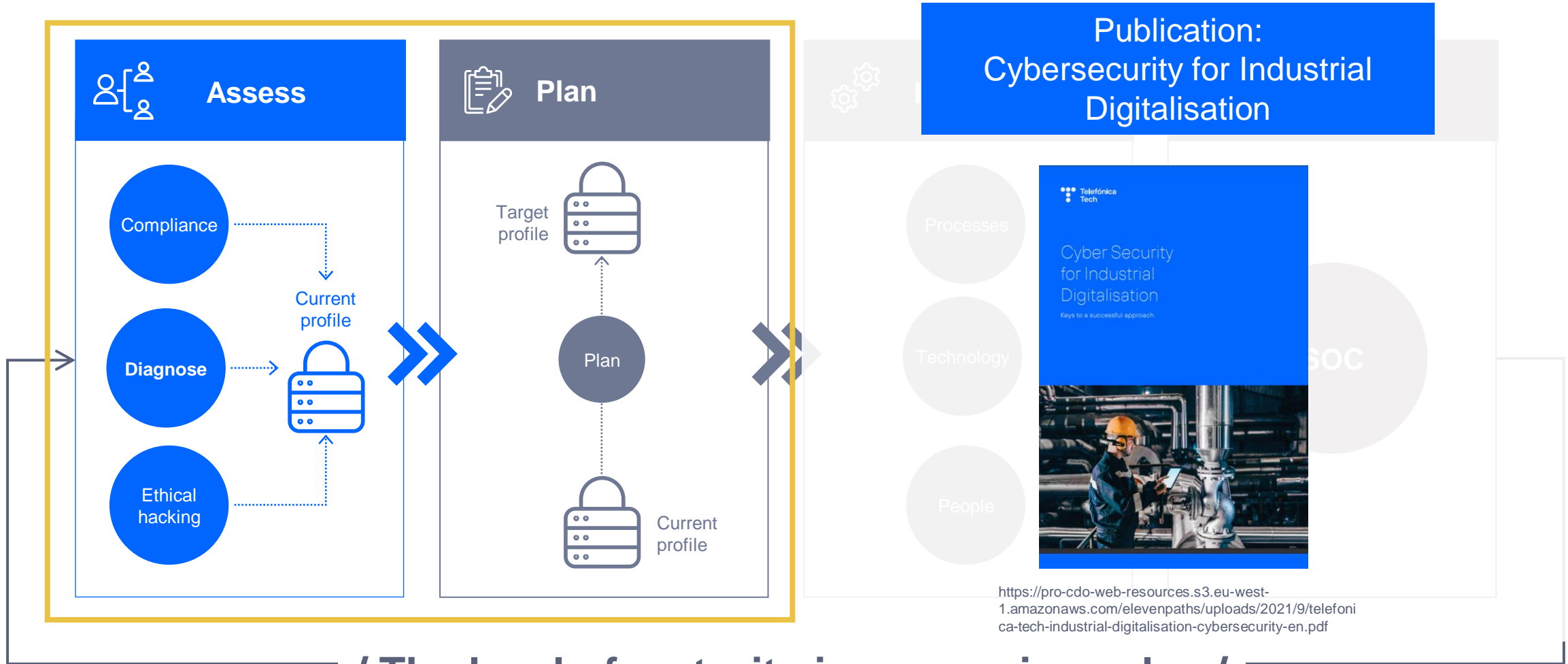
**Solutions**



# How we approach cybersecurity in industrial sectors



# Start by knowing your infrastructure and assessing your security posture



/ The level of maturity improves in cycles /

<https://pro-cdo-web-resources.s3.eu-west-1.amazonaws.com/elevenpaths/uploads/2021/9/telefonica-tech-industrial-digitalisation-cybersecurity-en.pdf>

# An example of a Cybersecurity assessment report

## Index of contents

1. Introduction.....	6
2. Goals.....	7
3. References.....	8
4. Methodology for OT Cybersecurity Assessment.....	9
4.1. Methodology framework.....	9
4.2. Purdue reference model.....	9
4.3. Assessment tools.....	11
5. Executive summary.....	14
6. Global security status.....	19
6.1. Context.....	19
6.1.1. Supplied services.....	21
6.1.2. Arquitectura de red.....	21
6.2. Gathering of information.....	24
6.2.1. Information about identification and authentication.....	24
6.2.2. Information about access control.....	27
6.2.3. Information about system integrity.....	32
6.2.4. Information about Communication flows.....	34
6.2.5. Information about system control.....	37
7. Network traffic analysis.....	40
7.1. Introduction.....	40
7.2. Executive summary.....	43
7.3. Inventory and use.....	44
7.3.1. Assets.....	44
7.3.2. Network protocols.....	48
7.3.3. Communication flows.....	51
7.4. Security findings.....	53
7.4.1. Use of insecure protocols.....	53
7.4.2. Vulnerable assets.....	54
7.4.3. Use of weak or unencrypted passwords.....	56
7.4.4. Network design issues.....	56
7.4.5. Malware activity and network attacks.....	57
7.4.6. Connectivity problems.....	59
7.4.7. Configuration issues.....	60
8. Recommendations.....	61
8.1. Introduction.....	61
8.2. Corrective measures.....	62
8.2.1. To change default and weak passwords.....	62
8.2.2. To check user accounts on industrial systems.....	63
8.2.3. To check malware activity and network attacks.....	64
8.2.4. To update firmware and software.....	64
8.2.5. To use secure protocols and versions.....	65
8.2.6. To solve identify vulnerabilities.....	65
8.2.7. To check and disable unnecessary communication flows.....	66
8.2.8. To label the wiring.....	66
8.2.9. To unplug free ports in the switches.....	67
8.2.10. To create physical and logical diagrams.....	67
8.3. Preventive measures.....	68
8.3.1. Administrative measures.....	69
8.3.2. Technical measures.....	75
8.3.3. Complementary services.....	83

### Asset inventory in the plant:

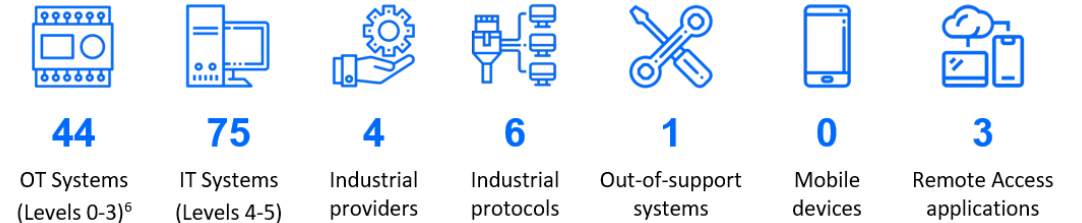


Figure 5. Collection of inventory and use of assets in the plant XXXX (Summary).

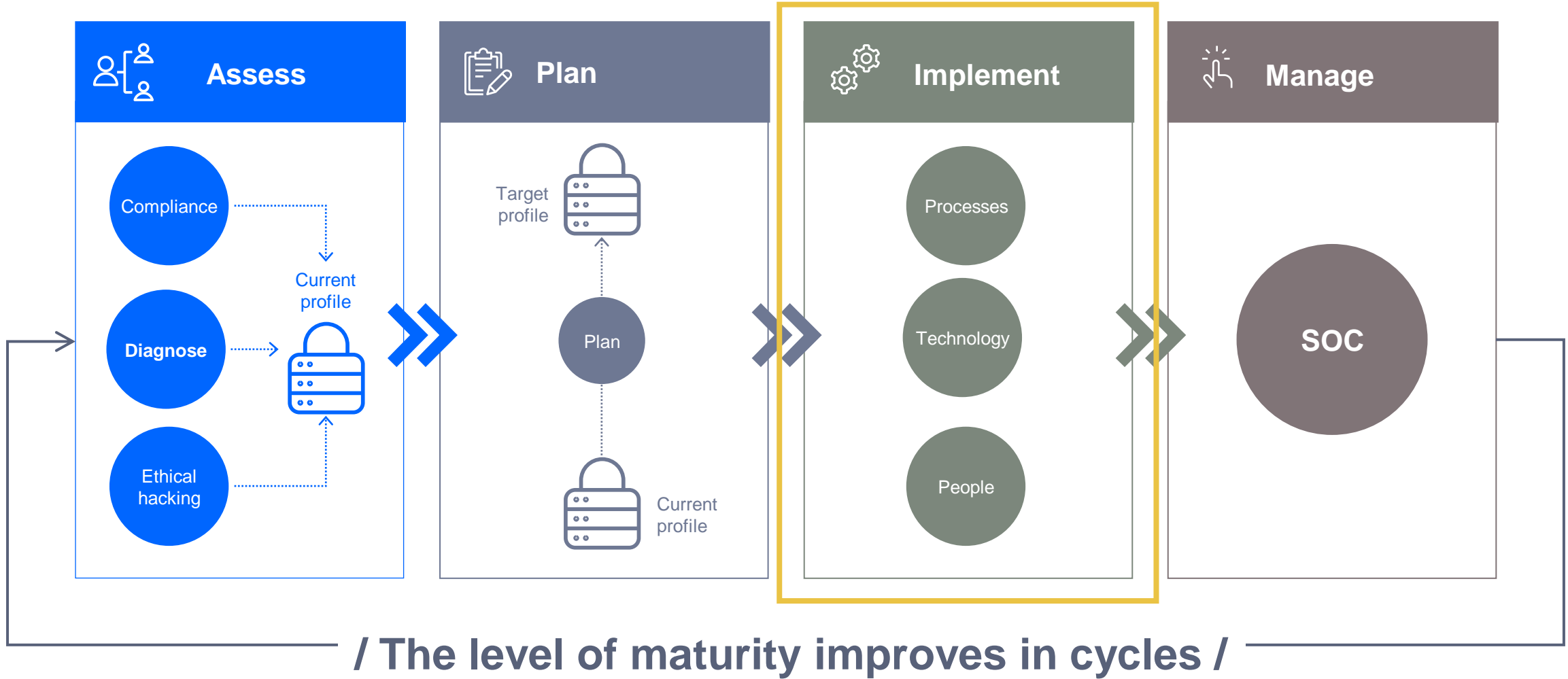
### Security findings in the plant:



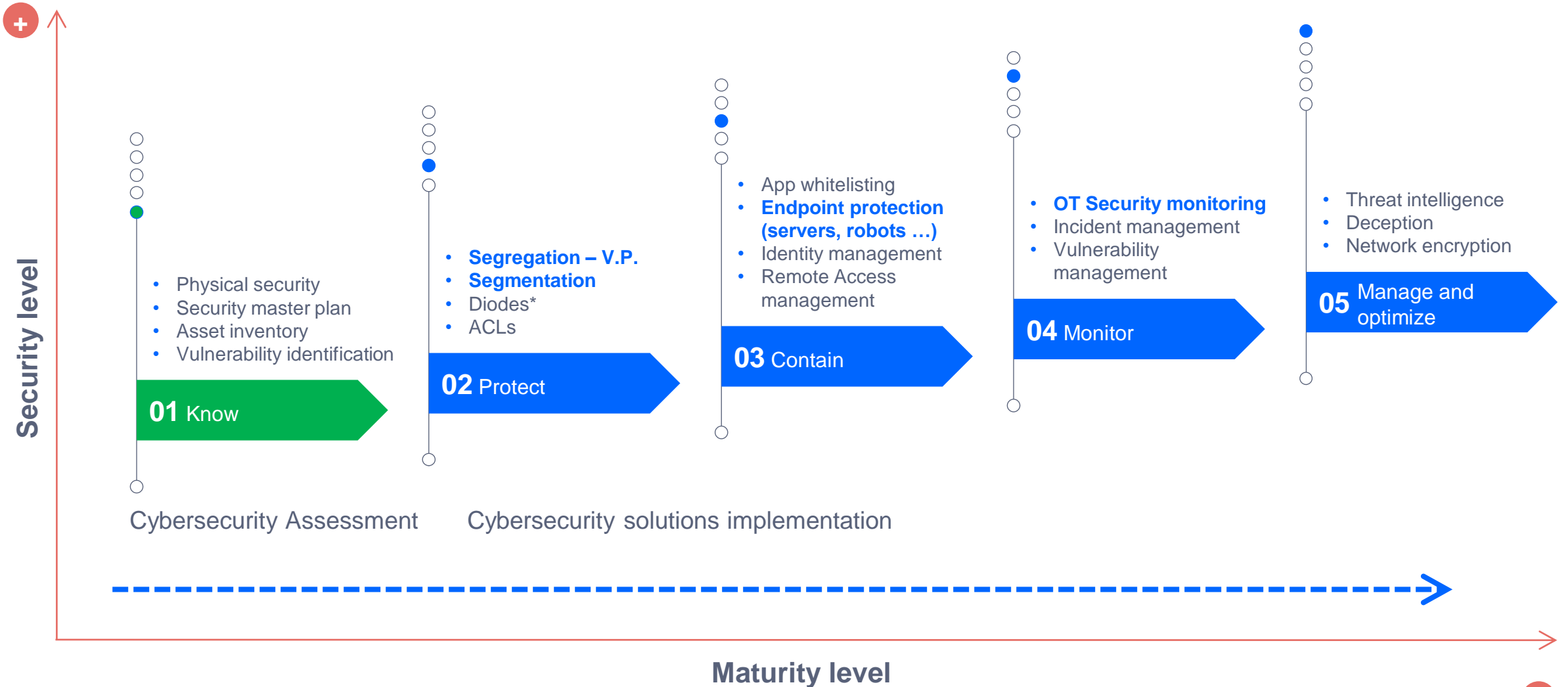
Figure 6. Collection of security findings in the plant (Summary).



# How we approach cybersecurity in industrial sectors



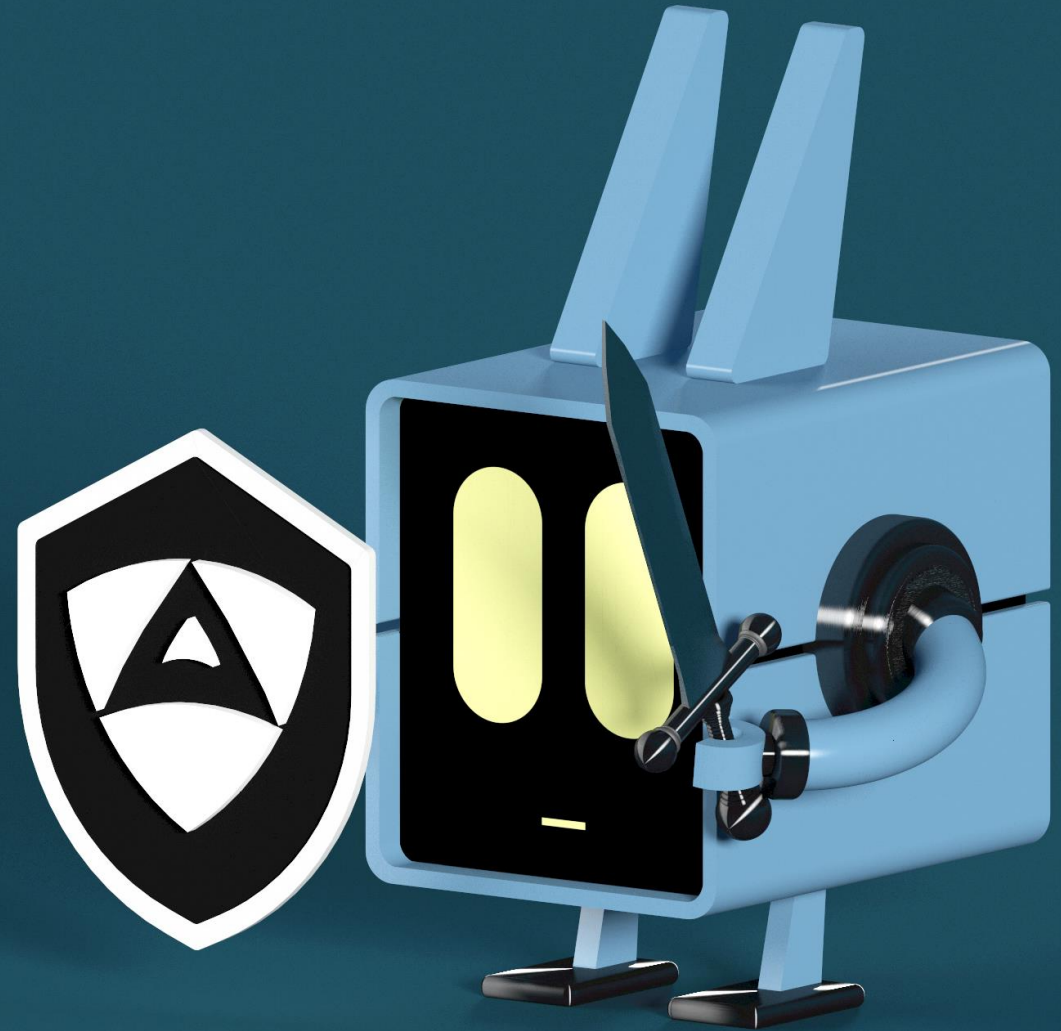
# Define a plan that starts by “Fixing the basics”





# ALIAS ROBOTICS

**Alias Robotics** is a robot cyber security firm. Founded upon previous experiences in robotics, we take a roboticists' approach to cyber security and deliver security solutions for robots and their components.





# OUR JOURNEY



BIRTH OF ALIAS ROBOTICS



PRE-SEED ROUND



RIS ANNOUNCEMENT



RIS DEPLOYMENTS



PARTNERSHIP WITH TELEFÓNICA



CS4R INITIATIVES

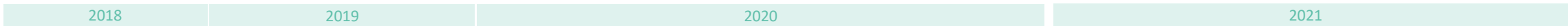


PARTNERSHIPS AND LARGE CUSTOMERS

Clients Services EUROPE

Clients Services USA

Clients Services APAC



## ACKNOWLEDGMENTS

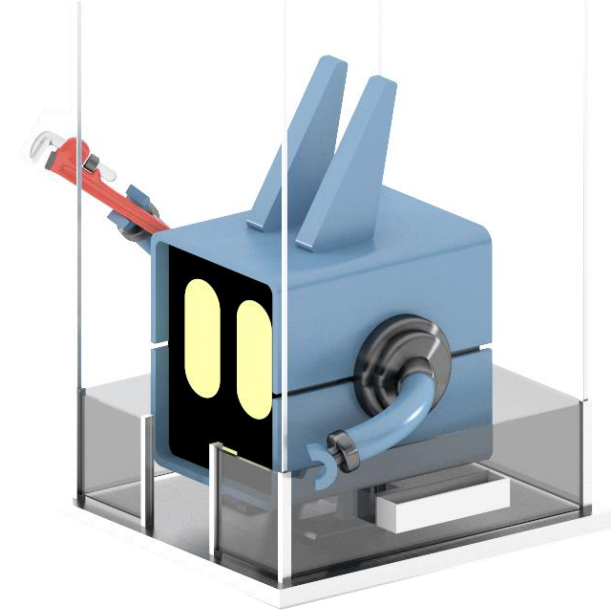
2018  
SOUTH SUMMIT WINNER  
Among the 100 best startups in the world

2019  
"EL REFERENTE" AWARD  
Top 5 startups Spain

2020  
CVE NUMBERING AUTHORITY (CNA)  
Recognized as the only Spanish CNA, together with Incibe.

2021  
QUALITY INNOVATION AWARD  
International winner in the category "Innovation in SMEs".

# LEADING ROBOT CYBERSECURITY



1K+

20

ACTIVE  
VULNERABILITIES

COMPANIES WHERE  
WE HELP SECURE  
ROBOTS

<https://github.com/aliasrobotics/rvd>

aliasrobotics / RVD Public

Code Issues 221 Pull requests Discussions Actions Security Insights Settings

master 11 branches 0 tags Go to file Add file Code

File	Description	Commit
rdv-bot (automatic)	Update README.md	#5ad429 on 30 May 942 commits
.github	Fix issue management action	16 months ago
deprecated	Backup flows and clean issue management one for now	2 years ago
docs	Update TAXONOMY.md	2 years ago
examples	Add CLI tool files	2 years ago
rdv_tools	Fix unnecessary args	12 months ago
training	Update training again, do not use title	2 years ago
.gitignore	Update list --fromdate to include label	15 months ago
LICENSE	Add GPLv3 license	2 years ago
MANIFEST.in	Add first prototype for CVE file generation	2 years ago
README.md	(automatic) Update README.md	4 months ago
alurity.yml	Add alurity.yml file for short demonstration	15 months ago
setup.py	Merge pull request #3338 from aliasrobotics/dependabot/pip/pyyam...	4 months ago

README.md

vulnerabilities 221 bugs 0 unmerged 0 tags 0 duplicates 0

### Robot Vulnerability Database (RVD)

**ALIAS ROBOTICS**  
Robot Cybersecurity

This repository contains the Robot Vulnerability and Database (RVD), an attempt to register and record robot vulnerabilities and bugs.

Vulnerabilities are rated according to the [Robot Vulnerability Scoring System \(RVSS\)](#). For a discussion regarding terminology and the difference between robot vulnerabilities, robot



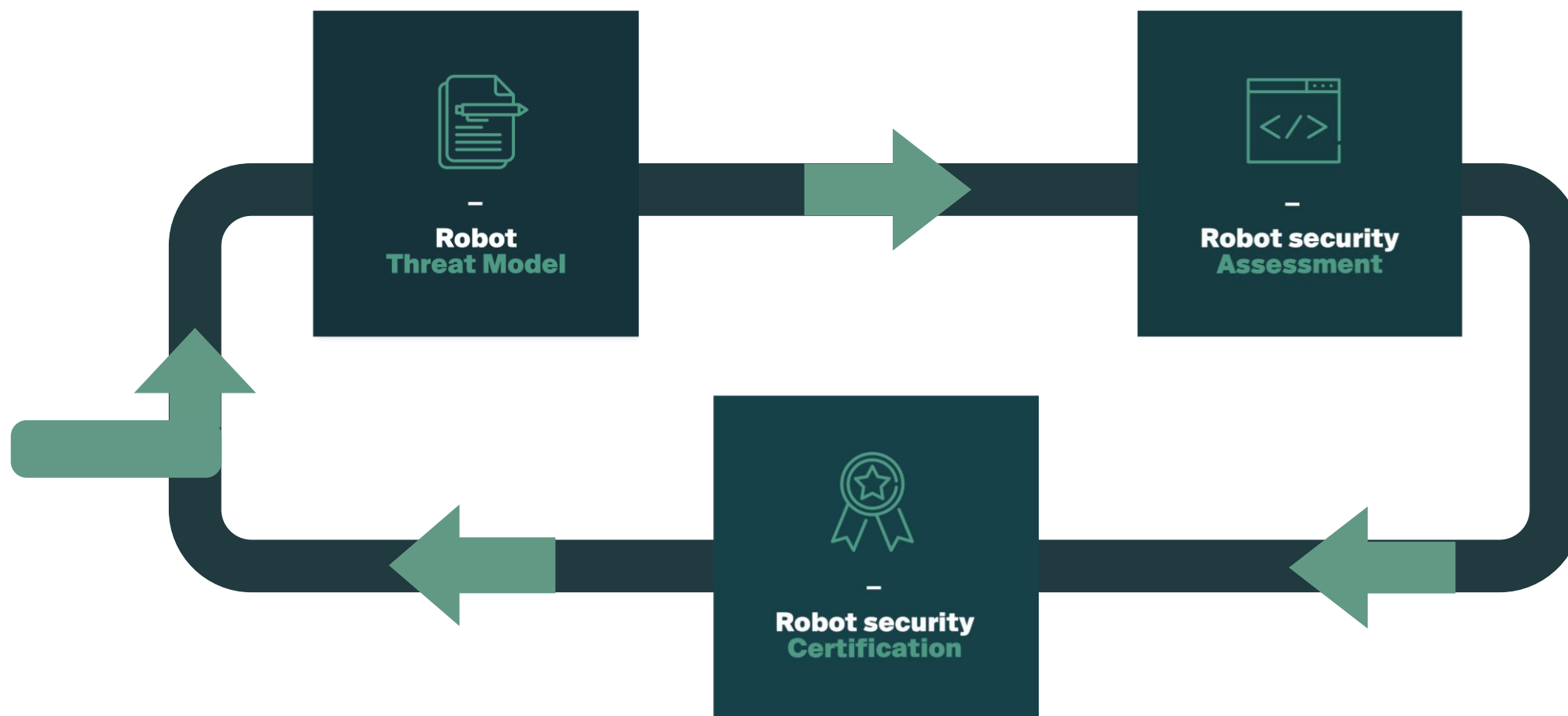






# OUR OFFERING

# SECURITY IS A PROCESS





PRODUCT



# RIS

by **ALIAS ROBOTICS**

The Robot Immune System (RIS) is a software solution that protects robots and robot components against malware.

Inspired by nature, it gets installed directly into your robotics systems delivering an integrated suite of protection technologies that protect them from the inside, as it evolves and adapts like the human immune system.

## **ROBOT IMMUNE SYSTEM**

Robot cyberattacks & malfunctions



CONNECTING...





IF YOU WANT TO GO FAR  
GO ALONE.  
IF YOU WANT TO GO FAR

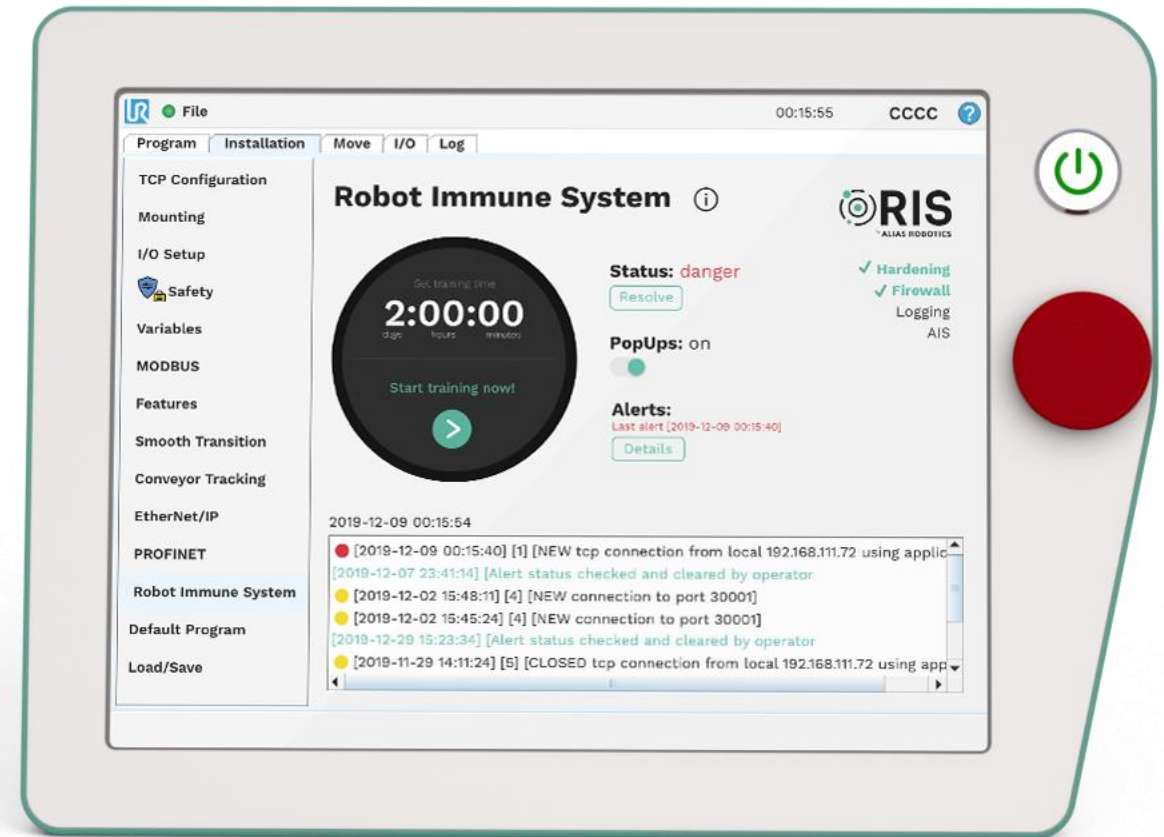




# HOW DOES IT WORK

## Robot Immune System (RIS)

RIS is a Robot Endpoint Protection Platform (REPP), an integrated suite of endpoint protection technologies for robots. RIS gets deployed directly into your robot or robot component. —including a next-gen antivirus, hardening for known flaws, data encryption, intrusion prevention mechanisms, data loss prevention, etc.— that detects, prevents, stops and informs on a variety of threats that affect the robotic system.





CONNECTING...



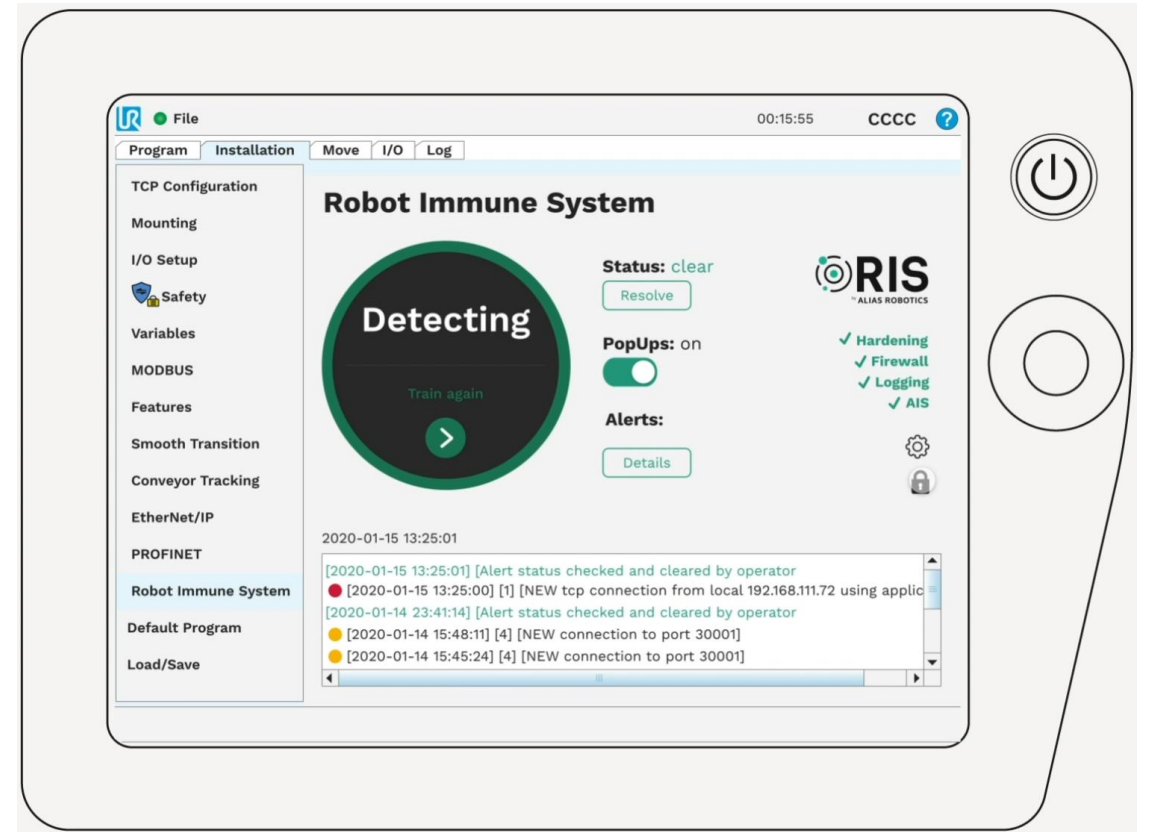


IF YOU WANT TO GO FAR  
GO ALONE.  
IF YOU WANT TO GO FART





kaspersky





# INDUSTRIAL ROBOT PROTECTION

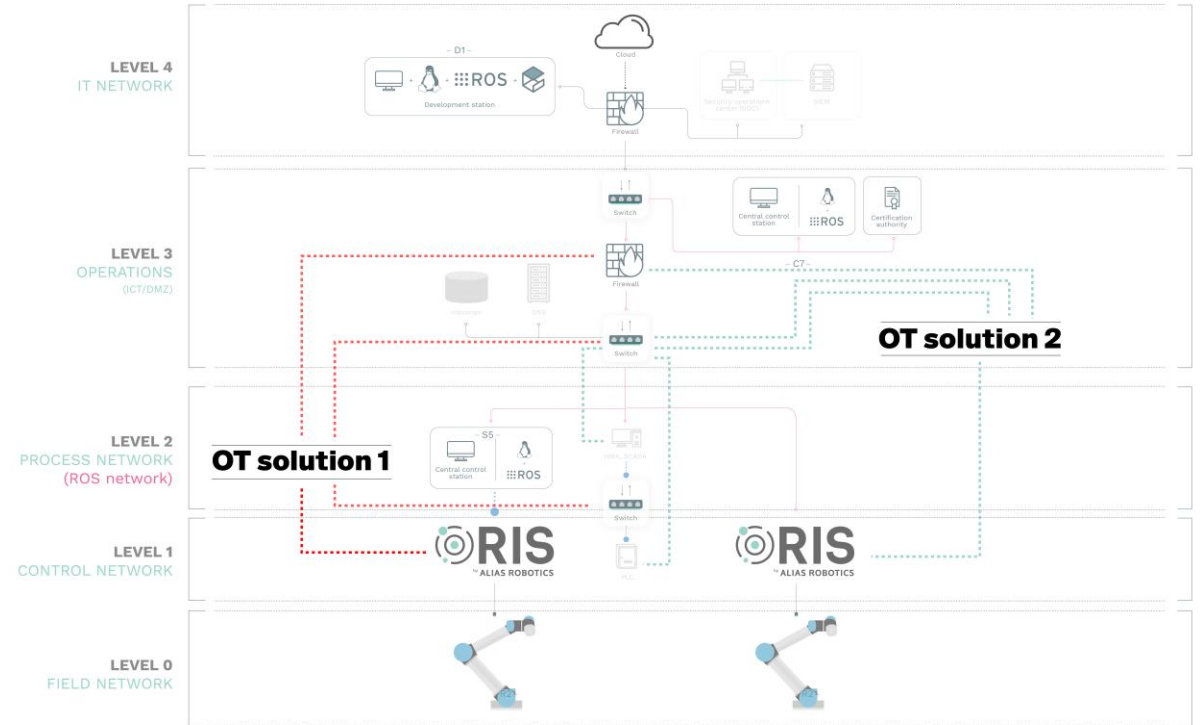


RIS connects seamlessly to existing market lead OT security solutions

A dedicated layer to provide security and visibility to robots  
Our product advocates for a **security in depth** paradigm

and **zero -trust** robotics

**Increased** compliance with IEC 62443



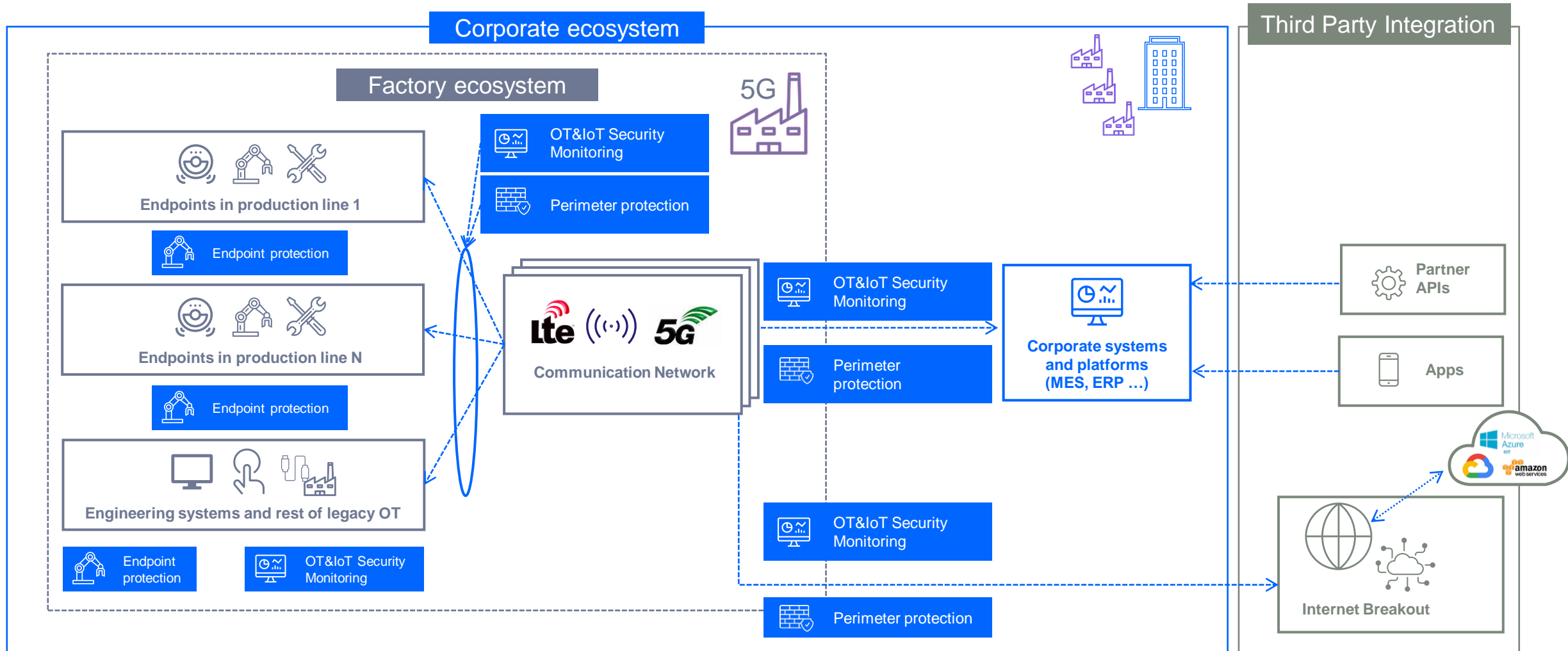


# RIS TIER 1 AUTOMOTIVE CLIENT



# SUMMARY

## An overview of the cybersecurity solutions for the Factory of the Future



Professional Services: Consulting, Assessment & Pentesting

