Orange Cyberdefense

Industrial cybersecurity

Protection of industrial systems

Industrial systems in all their diversity have been undergoing an unprecedented digital transformation in recent years.

This inevitable and necessary digital transformation is at the heart of industrial process, delivering flexibility, agility, efficiency of production tools, computing power, connectivity but also, and unfortunately, exposure to new cyber threats.

Regardless of the company size and sector, managers are now very aware of the risks and impacts of digital malware, which are here to stay, with competitive, criminal or terrorist aims.

To face these risks, Orange Cyberdefense supports you with awareness, consulting, auditing, engineering, integration of security solutions but also monitoring to ensure:

- Reliability
- Availability
- Maintainability
- Safety

Industrial systems are everywhere

- Aerospace
- Defense
- Automotive
- Cement & Glass
- Chemicals & Materials
- CPG, Food & Beverage
- Electric power & smart Grid
- High tech & medical devices
- Logistics & transportation
- Metals & Mining
- Oil & Gas
- Pulp & Paper
- Smart Cities
- Smart Building
- Water & Wastewater

360-degree support to secure industrial systems
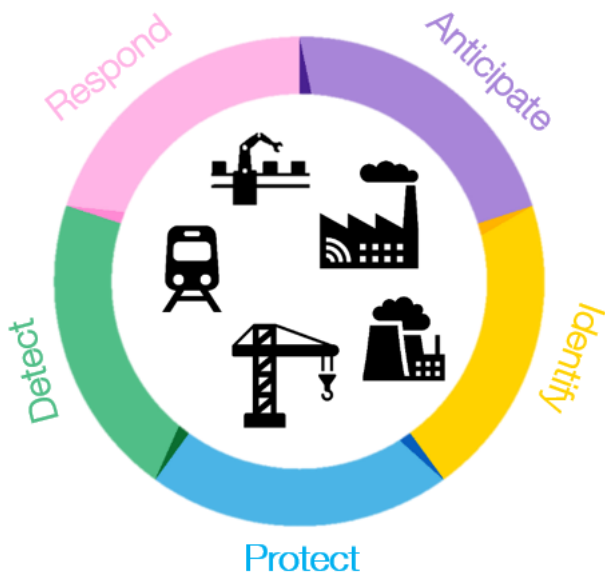
Step 1
Analyze, raise awareness, train, inventory

Step 2
Back-up / restore, segment, secure access

Step 3
Deploy, monitor, alert

Step 4
Incident response team, analyze, remediate

Step 5
Monitor, pen test, mock-up

Our assets

Dedicated support according to your activity sector in order to set up a security approach

A hybrid team: OT/IT experts
Transportation, building, energy and automation specialists, industrial systems integrators and machine builders, cybersecurity experts

Proprietary tools developed in-house
including OT asset mapping

A portfolio adapted to address both stakeholders: IT and OT
(automation, maintenance, process engineering, quality, etc.)

Industrial Security Demo Center
A place dedicated to our customers to test and validate their security solutions in a simulated environment, to raise awareness to cyberattack and to train both OT and IT staff