Operational Technology Maturity Risk Assessment

Trusted partner for your **Digital Journey**

Atos

The context

Because of their role in the global economy, industrial companies are attractive targets for cybercrimes. Industrial facilities face unique cybersecurity challenges, given their distributed, decentralized governance structures and large operational technology (OT) environment.

The lack of visibility on critical Industrial control systems assets is a real challenge. Previously considered as independent objects, they become more connected and more complex. New potential vulnerabilities and entry points for hackers are then created.

The challenges

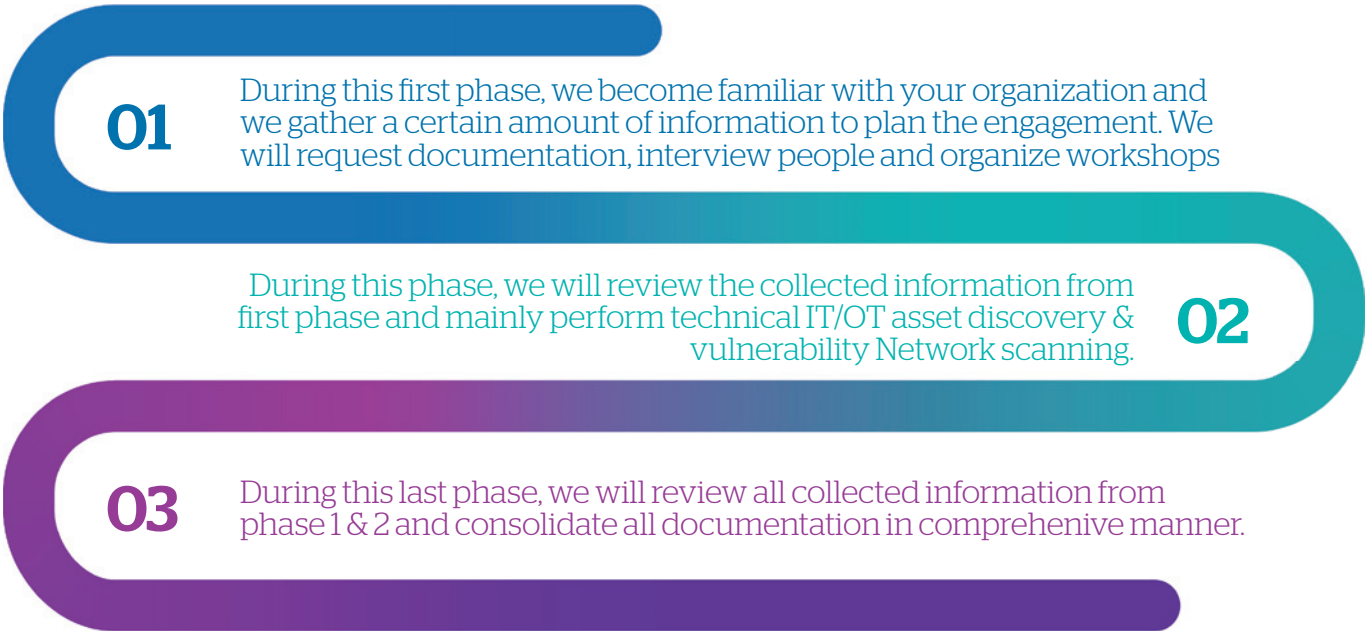
1. Lack of clear cybersecurity governance between IT & OT
2. Human error due to a lack of cybersecurity awareness
3. Lack of visibility on critical Industrial assets and their potential vulnerabilities
4. Missing resources covering cross knowledge between IT & OT
5. Increased amount of regulations to take into consideration
6. Use of off-the-shelf technology like Ethernet, TCP/IP and Windows in the OT sector introducing threats from the IT world
7. Difficulty to identify abnormal behaviors and detect advanced persistent threat
8. Risk of infections through unsafe mobile devices such smartphones and laptops (on-site and for remote working)
9. Insufficient access control for both physical and logical access
10. Lack of IIoT security for connected devices collecting data
11. Industrial control systems components such as HMI's (Human Machine Interface) and PLC's (Programmable Logical Controller) designed to be reliable and safe, often overlooking security
12. Older control systems units in facilities still prevalent and easy to exploit
13. Difficulty or impossibility to patch devices due to conflicting industry-specific regulations as well as configuration/warranty considerations
14. Remote maintenance of ICS components and entire systems is carried out without implementing security and access control measures by various operators (company maintenance team, third-party integrators or machine manufacturers)

Atos assessment's methodology

Our assessment starts by understanding the current situation and by identifying people, process and technologies across your company. We ensure common understanding across your main IT/OT stakeholders through interviews and awareness workshops.

We have designed 3 comprehensive work packages:

1. Initial project phase **2. Current state analysis** **3. Reporting/roadmap**



Deliverables covered in approach

With the Atos Operational Technology Maturity Risk Assessment, you will be provided with following examples of deliverables:

- RACI matrix, Scope statement, Engagement planning
- Initial discovery & Maturity assessment interview output
- Technical OT AS-IS: Asset discovery, Vulnerability list and high-level Network diagram
- High-level Technical Security review
- Master Security roadmap including people, process and technologies measures
- Executive Summary presentation/report

Why Atos?

With 120,000 professionals at work in 73 countries, we've created one of the most multicultural, multi-disciplined, diverse and responsive work environments in the world. Open, informal, flexible communication sets the tone in our company. We work together to deliver the top-quality, tailored solutions our clients expect, all around the world. Solutions that can only come from teams bringing fresh ideas, different perspectives and individual flair.

Our clients know they can count on us not only to be versatile and inventive, but also to work continually to create a deeper understanding of their business.

The number 1 in Europe and a global leader in cyber security

With a global team of over 4,500 security specialists and a worldwide network of Security Operation Centers (SOCs), Atos offers end-to-end security partnership. We integrate the best security technologies and offer a full portfolio of security solutions – helping you turn risk into business value.

Our experience

In today's more interconnected world, companies need to adopt the right people, process and technologies to get closer to the market and become more competitive. Industrial systems and IT information systems are exchanging more and more information. Systems are often decentralized, and assets dispersed throughout the territory.

Atos has led several projects in this field, each requiring specialist in IT and OT knowledge. Whether we are dealing with well-established legacy systems or with projects driven by digital transformation, we constantly seek to boost efficiency and enhance security for our clients.

Here are a few examples of implementation projects we have carried out after the recommendations phase of the Risk Assessment:

- Improve IT/OT overall Security architecture
- Enforce IT/OT policies, Standards, Guidelines and procedures
- Implement new Governance model including IT & OT
- Improve security of IIoT sensors for better data trust & transmission
- Improve Access control for IT/OT convergence to centrally control and monitor access to unconnected systems
- Segmentation OT Network including new gateways implementation
- Monitor OT Network including Asset discovery and anomaly detection
- Integrate the monitoring of the OT assets in the company Security information Management System (SIEM)
- Development of dedicated OT Security Operation Center (SOC).

We have carried such projects for several Operators of Essential Services (OES) like Energy, Transport and water suppliers and distribution companies but also for critical manufacturing companies such as Pharma, FnB, medical devices and car manufacturers.

Atos key differentiators

Unique Cybersecurity career path to certify Atos workforces as OT Security practitioners

Specific OT SOC capabilities and development for customers including people, process and technologies integration

Being agnostic from the technology vendors to provide the best solution to our customers upon their industrial context

Projects experience achievements for several Operators of Essential Services (OES) and critical manufacturers

OT Security Global leaders working at Atos*

*Example of an Atos leader and OT Security expert: Eyal Asila, Director, head of Global Cyber Security Consulting Group. Relevant Projects and experience (over 22 years' experience), OT SME and former CISO of an International manufacturing company.

About Atos

Atos is a global leader in digital transformation and in Managed Workplace Services with 110,000 employees, including 15,000 workplace experts, in 73 countries and annual revenue of € 12 billion. European number one in Cloud, Cybersecurity and High-Performance Computing, the Group provides end-to-end Orchestrated Hybrid Cloud, Big Data, Business Applications and Digital Workplace solutions, where workplace solutions are positioned as a Leader by Gartner in its Magic Quadrant for Managed Workplace Services for both Europe and North America earlier in 2020.

In the UK & Ireland Atos delivers business technology solutions for some of the country's largest public and private sector organisations The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and operates under the brands Atos, Atos|Syntel, and Unify. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

For more information: **https://atos.net/en/solutions/cyber-security**