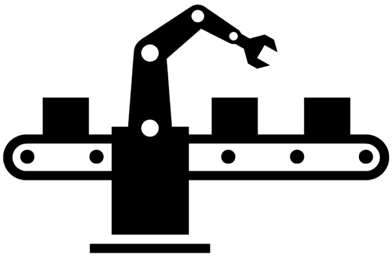
Cyberdefense

Industrial Cybersecurity

Securing the digital transformation of your business



Industrial Security in the Connected Era: Protecting critical systems and infrastructure

Especially in production, OT systems were traditionally thought to be protected by an air-gap separating them from the highly connected (and thus highly vulnerable) IT-world. This is no longer the case as the connectivity of IT and OT environments, which has already progressed for quite a while, was accelerated by the increasing use of IT technologies in industrial systems. This fusion brings with it a completely new world of benefits, efficiency, and flexibility. But it also opens plants, shop floors, production facilities and vital infrastructure to the darker world of traditional IT threats.

With proper security mechanisms implemented for industrial networks, organizations can increase their competitive edge and benefit from the efficiencies when interconnecting environments. Effective OT security protects business-critical processes, systems and people, and reduces security vulnerabilities and incidents.

Orange Cyberdefense works with customers in many different industries, with similar challenges related to the use of industrial control systems, SCADA environments, health and medical equipment, etc. Our Industrial Security Services are designed to help you meet compliance requirements with regulations such as NIST 800, IEC 62443, NIS 2.

> **“From 2019, we derive that incidents involving sophisticated attacks against OT systems have increased exponentially, peaking in 2023. The increase in incidents involving both IT and OT systems after 2019 suggests that the boundaries between IT and OT are becoming increasingly blurred.**
>
> **The diversity of attacks, ranging from the crude to the sophisticated, shows us that threat actors are adapting and diversifying their methods of exploiting IoT systems.”**
>
> **Source:** Security Navigator 2024

Are you prepared?

To ensure high levels of security for your industrial systems, there are some pivotal factors that you should take into consideration:

- **Understand your environment**
  You can’t protect what you don’t know. Getting visibility on your OT environment fosters a data-driven approach to security.
- **Secure your networks and assets**
  Securing the connectivity of IT and OT networks starts with the protection of your critical endpoints.
- **Detect threats from your IT and OT networks**
  The threat landscape changes as fast as digital transformation does. It is important to extend threat detection to OT.
- **Be prepared to respond to security incidents**
  Security incidents will happen and can impact your operations. Be prepared to limit the impact.

Find out more on OT security on our website:
www.orangecyberdefense.com/global/industrial-cybersecurity

Our OT security approach is powered by our dedicated OT teams and our intelligence-led services

Build a risk-based OT security program with embedded threat intelligence.

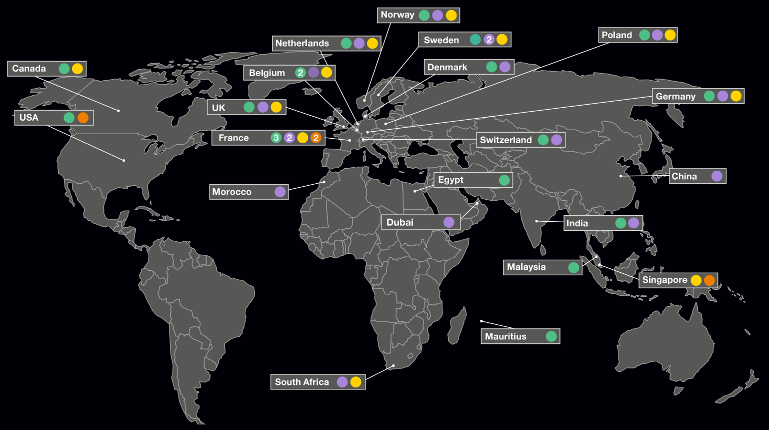
Securely connect your IT and OT networks and protect assets from evolving complex threats.

Detect threats in your IT and OT networks and build integrated response capabilities.

Be prepared for security incidents with the right specialists on hand to respond.

About Orange Cyberdefense

- Orange Cyberdefense is a European leader with global footprint and proven OT security expertise.
- Our end-to-end security solutions are designed to secure your business's digital transformation.
- Together with our services, we provide dedicated OT security specialists and specialized OT managed security service delivery teams.
- We have cross-industry experience and know-how of industry standards.
- Our strong partnerships with market leading OT security vendors are part of our success factors.
- We are recognized by Gartner in the OT Market Guide.



Build a safer digital society

www.orangecyberdefense.com