Mandatory holistic cybersecurity for Industry 4.0

Industry 4.0 is transforming the manufacturing and industrial landscape by integrating advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and cloud computing. While these innovations provide immense benefits, they also ramp up the risk of cyberattacks due to increased connectivity and a larger attack surface. This allows cybersecurity risks such as malware to invade the industrial environment, which is traditionally less security oriented.

Securing industrial environments requires implementing security measures that control system access and enable secure data exchange and analysis. To fully benefit from Industry 4.0, businesses must prepare for cybersecurity challenges, including ensuring compliance with regulatory requirements and securing the entire digital supply chain.

With the right cybersecurity measures in place, Industry 4.0 can create a secure, smarter, more connected, and sustainable manufacturing industry that is ready for the future.

orange™ Business

Challenges for industrial cybersecurity

1 Visibility

Unlocking the power of comprehensive OT visibility.

Comprehensive visibility is the foundation of a robust OT security strategy. Without understanding your assets and their interconnections, vulnerabilities and threats go unnoticed, exposing your organization to potential cyberattacks and operational disruptions.

Monitoring and managing assets effectively become challenging without detailed location, type, and configuration information. Blind spots can emerge, leaving your industrial environments vulnerable and your operations at risk.

Comprehensive visibility into the Operational Technology (OT) environment is crucial for organizations to manage risks, optimize operations, and ensure the safety and reliability of critical systems in industrial environments throughout the supply chain.

Investing in asset discovery and management tools, network security monitoring solutions, and vulnerability scanners allows organizations to identify, classify, and map interconnections of assets. Continuous monitoring of asset behavior ensures timely threat detection.

Prioritizing asset management empowers organizations to gain valuable insights and proactively safeguard their infrastructure against cybersecurity threats.

2 Digital transformation

Seize the power of secure digital transformation.

In the era of digital transformation, safeguarding your organization is paramount. A comprehensive security approach is essential as technology advances, covering every aspect of your digital infrastructure – cloud, IT, OT, Industrial IoT (IIoT), and physical security environments.

With increased interconnectivity, cyber threats spread rapidly, posing risks to organizations' operations and reputations. Strengthening the security measures is crucial.

A resilient security strategy is built on multiple layers, including secure architecture, cutting-edge detection, monitoring, analytics, robust authentication, secure remote access controls, encryption, and responsive incident handling. Prioritizing cybersecurity awareness and training for organizations' workforces equips them to be vigilant against evolving threats.

Organizations can confidently embrace digitalization and unlock its full potential while mitigating security risks by taking a holistic approach to cybersecurity across all digital domains.

3 Compliance

Empowering compliance for resilient OT/IoT security.

Cybersecurity threats demand unwavering compliance to safeguard OT/IoT infrastructures and ensure uninterrupted business continuity. Regulatory standards like NIS 2, NIST, IEC 62443, and IEC 21434 provide effective measures for securing critical infrastructure and industrial control systems.

Establishing a robust cybersecurity program is essential for compliance. It comprises risk assessments, governance, security policies, incident response plans, and continuous monitoring and detection services.

Prioritizing compliance safeguards organizations' OT/IoT infrastructure, ensures seamless business continuity and upholds the trust of valued stakeholders.

How we secure operational environments

Together with Orange Cyberdefense, we offer a comprehensive suite of managed industrial security services to increase the level of security maturity across the enterprise and supply chain.

Our services include identifying and detecting threats in OT and IT with threat intelligence capabilities, implementing OT/IoT security combined with industry security standards, and consulting services to enhance organizations' security posture. Additionally, we help industrial clients anticipate future threats by providing vulnerability intelligence services and tailored training programs to ensure all stakeholders are aware of potential risks.

Our consulting services help safeguard operational environments. Our cybersecurity experts provide comprehensive OT/IoT security assessments to identify potential vulnerabilities and risks. We work with clients to develop a customized security strategy tailored to their specific needs.

Our consulting approach emphasizes the importance of developing a robust multilayered OT/IoT cybersecurity architecture designed to meet clients' unique needs. We can define a feasible OT-baseline to establish a benchmark for normal activity in OT/IoT environments and network segmentation to ensure higher risk mitigation in case of an incident.

Our Managed Industrial Security Services

Empower your OT security with Orange Cyberdefense Managed Industrial Security Services

Orange Cyberdefense provides Managed Industrial Security Services to take care of an organization's OT/IoT cybersecurity risks, safeguarding your critical industrial infrastructures. This includes providing up-to-date asset and security information, reliable risk management, and cybersecurity programs. Our integrated approach covers IT and OT/IoT threat detection, leveraging Orange Cyberdefense threat intelligence. Gain full visibility into the organization's cybersecurity landscape, ensuring effective protection for their industrial infrastructures.

Managed Industrial Security [identify] Services

Turning visibility in data-driven OT security.

Orange Cyberdefense Managed Industrial Security [identify] Service provides timely and relevant security information on OT/IoT assets, empowering organizations to proactively manage cybersecurity risks and safeguard their industrial infrastructures.

With our fully managed OT/IoT security platform, we continuously gather data on assets to maintain an up-to-date inventory. This ensures that your organization has complete visibility into your assets and can focus on protection efforts.

The prioritized action advisory and reporting enables your organization to make informed decisions to reduce the risk of exposure.

Benefit from seamless integration with our Managed Firewall service for virtual patching of vulnerable OT assets and our Managed Vulnerability Intelligence service for risk-based vulnerability management.

Managed Industrial Security [detect] Services

Detecting threats in OT environments.

Orange Cyberdefense Managed Industrial Security [detect] Services provides a technology agnostic and integrated IT and OT threat detection. Organizations gain full visibility of the cybersecurity landscape to protect industrial infrastructures effectively.

Our fully-managed OT/IoT security platform provides continuous threat detection, security event management, and timely escalation of qualified security incidents by dedicated OT security experts.

Integrate with our Managed Threat Detection [log] services for combined IT and OT threat detection, incident investigation, and proactive threat hunting. Additionally, leverage our Managed Firewall service to ensure a fast and secure response to security incidents.

Why Orange Cyberdefense?

Orange Cyberdefense, the expert cybersecurity business unit of the Orange Group, provides comprehensive and innovative cybersecurity services for our clients to operate safely and securely in the digital world.

Orange Cyberdefense is Europe's leading security provider. We have more than 10 years of experience supporting industrial customers on their OT security journey, making OT security a strategic objective. With our multidisciplinary team, we support our industrial customers with consulting, professional service, and managed security services on all dimensions of OT security.

As Europe's leading security provider, we strive to build a safer digital society. We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats.

- **25-plus year track record in information security**
- **3,000 plus global experts**
- **250-plus researchers and analysts**
- **18 SOCs**
- **14 CyberSOCs**
- **8 CERTs distributed across the globe**
- **4 scrubbing centers to mitigate DDoS attacks**
- **Sales and service support in 160 countries enables us to offer global protection with local expertise**

Why Orange Business?

Orange has 2,200 global data experts available to help you deliver a data-driven strategy. This will allow you to maximize plant energy efficiencies, provide faster resolutions, seamlessly exchange data, enhance safety and quality control, track components across the value chain, and ensure on-time delivery. Our offering includes:

- **A consultancy-led approach to transforming data and creating value for the business**
- **Auditing data assets and analytics maturity to create an overarching data-driven strategy**
- **Design and build a central Unified Namespace (UNS) as a centralized repository for structured data to make it meaningful to all components in the enterprise**
- **Data governance expertise to ensure the quality of data and manage its use**
- **Help you focus on areas of your business where technology and a data-driven approach will have the greatest impact**
- **Create easy-to-use dashboards so employees can track and optimize product quality and efficiently manage all manufacturing-related costs**

orange™ Business

orange™ Cyberdefense