orange Business | cisco Partner

Creating a high-performance environment

Secured by

orange Cyberdefense

Mandatory holistic cybersecurity for Industry 4.0

Safeguarding the physical environment is as critical for sporting endeavors as it is for manufacturing output.

Elite athletes cannot perform at their best unless they are sure that the field of play holds no concerns for their physical safety. Equally, nothing is more damaging to the factory environment than cybersecurity attacks that can halt production and result in millions of dollars lost from the bottom line.

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. In today's industrial environment, cybersecurity is therefore crucial for business resilience.

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.

The advent of generative AI (Gen AI) further complicates the cybersecurity landscape. While Gen AI enhances threat detection and response capabilities, it also empowers malicious actors to launch sophisticated attacks. Industrial organizations face challenges in adopting the necessary cybersecurity solutions due to legacy system vulnerabilities, compliance requirements, and a shortage of skilled professionals.

However, 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.

A playing surface free from threat: challenges for industrial cybersecurity

The traditional separation between Operational Technology (OT) and Information Technology (IT) is dissolving as industries undergo IT/OT conversion to maintain competitiveness and enhance process efficiency.

However, this transformation also opens the door for cyber criminals. The convergence of OT and IT introduces complex vulnerabilities, expanding the attack surface for cybercriminals. Industry 4.0 accelerates this risk, with connected systems increasing the severity of breaches. Attacks can disrupt operations, damage assets, and endanger safety.

In 2025's evolving industrial landscape, several cybersecurity trends demand urgent attention to protect operational resilience and ensure business continuity.

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.

4. Generative AI

Balancing innovation with security and ethical use through strong AI governance frameworks

Generative AI (Gen AI) adds another layer of complexity. While AI can dramatically improve visibility and threat response, it also presents new risks, such as A I-generated attacks or misuse of autonomous decision-making systems.

In the era of AI, industrial automation systems face heightened risks from sophisticated cyber threats. Special measures to harden these systems include the deployment of AI-powered cybersecurity tools that analyze vast volumes of data in real-time, identifying subtle anomalies and detecting malicious activity.

Your welfare is our priority: how we secure operational environments

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

Our assessment services provide industrial customers with a clear view of their cybersecurity posture, while our design and implementation services support the deployment of cybersecurity architectures purpose-built for OT environments. Our managed 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.

Zonal defense: A full spectrum of cybersecurity services

As industrial environments become increasingly interconnected, the protection of Operational Technology (OT) systems from cyber threats has become a strategic priority. Industrial cybersecurity services play a critical role in securing Industrial Control Systems (ICS), critical infrastructure, and complex networked environments. Orange Cyberdefense, a leading Managed Security Service Provider (MSSP), delivers a full spectrum of services across the three foundational domains of cybersecurity:

- Assessment,
- Design and Implementation, and
- Managed Services.

These services provide the structure and expertise required to safeguard OT networks in a rapidly evolving threat and regulatory landscape.

1

Our Assessment Services

Through asset identification, risk assessments, compliance audits (e.g., IEC 62443, NIS2), and penetration testing, these evaluations provide actionable insights into vulnerabilities and misconfigurations, enabling tailored remediation strategies that align with industrial needs and compliance demands.

2

Our Design and Implementation Services

These include network segmentation, secure remote access, and industrial-grade firewalls and IDS/IPS solutions. Orange Cyberdefense also assists in the creation of incident response plans, security policies, and targeted staff training. These services help maintain operational resilience while ensuring compliance with regulatory frameworks like the EU NIS2 Directive and the Cyber Resilience Act (CRA).

3

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.

Gaining visibility into data-driven OT security.

Our fully managed OT/IoT security platform provides timely and relevant security information on their industrial assets, empowering organizations to proactively manage cybersecurity risks and safeguard their infrastructures. We continuously gather data on assets to maintain an up-to-date inventory and ensure that your organization has complete visibility into your assets and can focus on protecting them.

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

Detecting threats in OT environments.

We provide a technology-agnostic and integrated IT and OT threat detection service that provides effective protection of industrial infrastructures by giving organizations full visibility of the cybersecurity landscape. Our platform provides continuous threat detection, security event management, and timely escalation of qualified security incidents by dedicated OT security experts.

You can integrate with our Managed Threat Detection [log] services for combined IT and OT threat detection, incident investigation, and proactive threat hunting. Additionally, you can 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 you with a secure back line through comprehensive and innovative cybersecurity services that allow you to operate safely and securely in the digital world.

Orange Cyberdefense is Europe's leading security provider, with more than 10 years of experience supporting industrial customers on their OT security journey, making OT security a strategic objective. Orange Cyberdefense empowers industrial leaders to secure their OT environments through expert-driven, end-to-end cybersecurity services that meet today's elevated regulatory and threat landscape.

With our multidisciplinary team, we support our industrial customers with consulting, professional services, 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 perform at your best by delivering 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**