Cyberdefense

Why your business can’t afford to ignore OT Security

Securing Operational Technology

A strategic guide

What decision-makers need to know about improving protection of OT in a rapidly evolving threat landscape.

From assessment to action: Building a strategic OT roadmap

21

17

Thinking ahead: How to future-proof OT Security

Cyberdefense

OT Security **is no longer** an emerging concern - it's a business-critical priority

Morten Skogvold
Managing Director
Orange Cyberdefense Norway

Mårten Toll-Söderblom
Managing Director
Orange Cyberdefense Denmark

Kåre Nordström
Managing Director
Orange Cyberdefense Sweden

Across the Nordics, industrial and critical infrastructure sectors are undergoing rapid digital transformation. As more organizations embrace connectivity and automation, the systems that control physical operations – Operational Technology (OT) – are becoming deeply integrated with IT networks. This offers tremendous opportunities but also exposes organizations to new and growing cyber risks.

While IT Security has matured significantly over the past decades, OT Security often remains overlooked and becomes the blind spot in the organization's cyber strategy. Yet a successful attack on OT systems can cause real-world consequences – from halted production to compromised public services and safety hazards. In this evolving threat landscape, OT Security is not just a technical issue. It's a strategic imperative that deserves the full attention of business leaders and boards alike.

In an era where cyber threats can paralyze physical infrastructure, OT Security is no longer just an IT-issue – it's a core business risk.

Regardless of your industry, securing Operational Technology is critical to protecting revenue, reputation, and resilience. This guide offers strategic insights, real-world examples, and actionable recommendations to help you make informed decisions that strengthen your organization's long-term security posture.

It's not about knowing every technical detail – it's about understanding what's at stake and taking the lead on what must be done.

Whether you're just starting your journey or looking to strengthen existing efforts, we hope this guide will inspire action and support your strategic roadmap toward shaping more resilient organizations.

The time to act is now.

The key to business continuity

In today's hyper-connected world, Operational Technology (OT) is more vulnerable than ever before. As organizations embrace digital transformation communication between IT- and OT-systems increase dramatically.

This exposes the digital core of many critical infrastructures to a whole new range of cybercriminal threats. While IT Security has gradually matured and become a familiar topic in top management, OT Security often remains overlooked despite its very direct impact on business continuity.

In the following we will provide you with important OT Security insights, address the business risks involved, and share practical steps any organization can take to increase the protection of their OT environments to bridge the gap between OT and IT Security, offering decision-makers a deeper understanding of OT Security without requiring extensive technical knowledge.

If OT Security is on your agenda - then this is for you

Whether you are a C-suite executive, OT leader, OT decision-maker, or cybersecurity strategist – responsible for risk management, operational technology, governance, or the overall cybersecurity strategy in your organization across any vertical or industry – building resilient organizations in an increasingly connected and complex world starts with understanding OT Security and safeguarding your business.

With this guide, we offer you essential practical advice, expert insights, and real-world examples to help you strengthen your organization's ability to withstand disruption, avoid financial loss, and protect your reputation so you can build a more secure and sustainable OT environment.

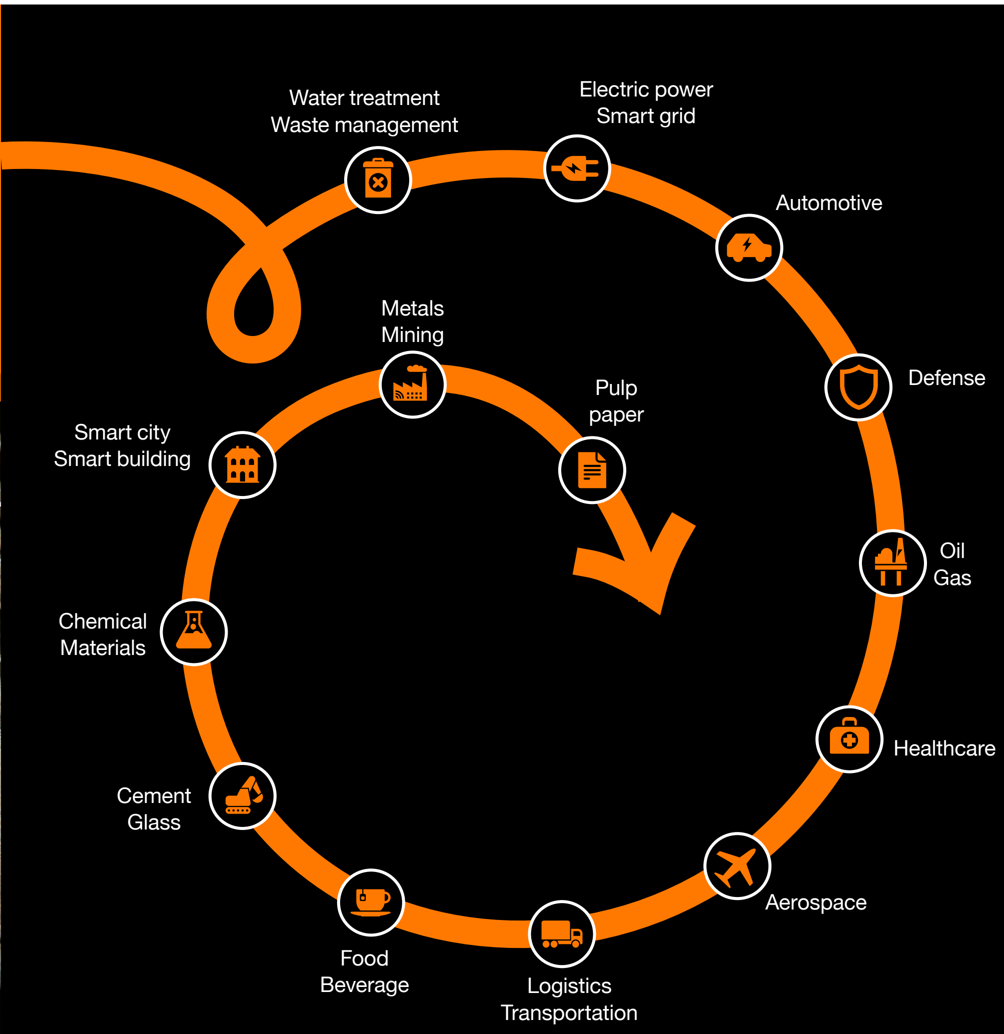
By the end of this guide, you will:

- Understand what OT Security is and why/how it differs from IT Security.
- Recognize the business risks associated with insufficient OT Security.
- Learn how cyberattacks can impact OT.
- Understand typical internal challenges of implementing OT Security.
- Explore practical solutions to strengthen your organization's cyber resilience.
- Discover how Orange Cyberdefense can support your OT Security journey, including hands-on insights from our OT Showroom in Lyon.

So, let's dive into the subject of OT Security and uncover why it is on track to become one of the most critical business priorities of the modern era.

OT systems are everywhere

We often tend to think of "Operational Technology" as technologies controlling industrial processing and production – the very name implies this. But the field of OT is far wider than that. In fact, OT systems can be found in any kind of industries and organizations.



OT Security: Understanding the basics

What is OT Security?

Operational Technology refers to the hardware and software needed to control physical processes and assets – often referred to as Cyber Physical Systems.

Unlike traditional IT systems that exclusively handle data and applications, OT systems are directly involved in the control and monitoring of physical operations. They can be found everywhere within both the public and private sector. For instance, in connection with production, control of electricity, energy, water treatment, ventilation, heating, cooling, compressed air, and many more.

OT Security focuses on protecting these systems from cyber threats that could cause operational disruptions, equipment failures, or safety hazards. Higher levels of OT Security are also needed to comply with new legislation like NIS2 and DORA.

How and why IT and OT Security differs

While the two areas may seem similar, they also differ significantly:

	IT Security	OT Security
Availability requirement	Medium, delays accepted	Very high
Real-time requirement	Delays accepted	Critical
Component lifetime	3-5 years	Up to and over 20 years
Applications of patches or changes	Regular / scheduled	Slow / infrequent / requires maintenance window
Security testing / audit	Scheduled and mandated	Scheduled and mandated
Security awareness	High / mature	Increasing

Because of these fundamental differences, IT and OT Security also have different scopes, requirements and challenges. Understanding this is key for decision-makers to implement the right OT Security strategies.

Primary focus	Data protection, confidentiality	Safety, availability
Environment	Office networks, cloud systems	Production and operation networks, legacy automation environments, operational support systems
Risks	Data breaches, system downtime	Equipment failure, production downtime, physical and environmental safety risks
Security approach	Scheduled patching, micro-segmentation, automated response actions.	Limited patching, system segmentation, human reviewed response actions

Typical OT Security risk factors

No two companies are the same, but there are similarities. Here are some of the most common challenges in OT Security.

Legacy systems

Many **OT-systems run on outdated software** whick lack modern security protections Also, these systems are not easily patched or updated, which makes them even more vulnerable.

Security as an afterthought

Historically, many OT-systems have been developed to **maximize operational availability and efficiency** – not to provide a high level of security.

Lack of visibility

Few or no efforts have been made to establish sufficient visibility across implemented security measures.

Lack of awareness of regulatory demands

The focus is typically on availability and **“keeping the production running”** above all. This often leads to gaps in governance or policy enforcements and non-compliance with industry standards (e.g., NIST SP 800-82, IEC 62443, NIST CSF 2.0, ISO 27001/2).

Lack of definition of OT

Secondary systems with a critical role in operations **are often overlooked and insufficiently protected.** This includes, for example, Windows servers used by OT systems, OT-related Wi-Fi networks, server room cooling systems, MES systems, or Building Management Systems.

Limited or no patching capabilities

Unlike IT systems, most **OT-systems cannot be subjected to frequent software updates** due to operational constraints. Some OT systems simply can’t be patched because there’s a **risk of disruption** if patches are applied without appropriate testing.

Remote access vulnerabilities

Growing connectivity with partners and through supply chains **exposes OT networks to cyber threats**.

Physical consequences

Attacks on OT can lead to safety hazards, environmental damage, or complete shutdown of operations.

With these risks in mind, organizations must adopt a tailored security approach that balances protection with operational efficiency.

Additionally, a lack of cybersecurity awareness among employees can lead to unintentional risks, and ransomware attacks pose a serious threat to production continuity. To mitigate these risks, it is essential to implement a comprehensive cybersecurity strategy that include regular assessments, employee training, and robust incident response plans.

Why OT Security is more critical than ever

Traditionally, cybercriminals have learned to exploit weaknesses in IT Security to penetrate outer security and search for valuable digital assets to encrypt, steal or damage. Valuable digital assets and intellectual property such as customer data, or critical infrastructure systems are also high risk target points. We also see, that highly sensitive and essential OT environments are becoming obvious targets due to increased communication between IT and OT networks.

High-profile attacks, such as the *__Colonial Pipeline ransomware attack__, highlight the devastating impact of OT Security failures. The financial, reputational, and regulatory consequences make OT Security a business-critical priority.

As requirements for OT Security – such as in NIS2, IEC 62443, NIST CSF, ISO 27001/2, and CIS – compliance is no longer optional. Organizations must proactively implement security measures to meet these evolving regulatory demands – increase resilience and build trust to avoid operational disruptions, ensure business continuity, avoid penalties, and avoid reputational damage and loss of stakeholder confidence.

For obvious reasons, failure to secure OT environments can lead directly to:

- **Costly operation downtime**
  Well-coordinated cyberattacks can halt operations, resulting in significant revenue loss and damage and reputational damage.
- **Safety hazards**
  Attacks on OT systems can cause physical harm to employees or lead to environmental damage.
- **Regulatory fines**
  Non-compliance with security regulations may result in financial penalties and reputational harm.
- **Disruption of critical societal infrastructure**
  Cyberattacks targeting OT systems in vital sectors can cause major operational breakdowns, physical damage, and societal impact by disabling essential services such as electricity, water, or transportation.

*The Colonial Pipeline ransomware attack in 2021 forced the shutdown of a major fuel pipeline in the United States, causing widespread disruption to fuel supplies. It demonstrated how cyberattacks on OT-systems can lead to real-world, physical disruption and how OT vulnerabilities can have great economic consequences.
See more detailed explanation of the attack on page 13.

Our customers say it best...

Renova Miljö

> **We get an updated overview of the OT environment and find opportunities for improvements in OT Security. At the same time, we now see great potential for both simplification and improvement in the management and use of several different systems in a relatively simple and economical way. Truly a "win win" for everyone.**
>
> **Patrick Gillmor, Automation and Process Engineer, Renova Miljö AB**

Renova Miljö AB – combined heat and power plant

Renova Miljö AB is a company specializing in waste management and environmental services. They focus on sustainable waste collection, recycling and disposal solutions to support environmental protection and resource efficiency. Renova is a critical business that have higher demands on OT security.

In preparation for NIS2 compliance Renova tasked Orange Cyberdefense with an assessment of OT Security maturity to gain recommendations for improvements and raise management awareness.

The predominant challenges in OT Security

Unforeseen downtime with heavy financial impact

For many organizations relying on OT, uptime is directly tied to revenue. Cyberattacks most often occur via interconnected IT systems, but there is a growing number of cases, where OT is being targeted directly by cybercriminals.

If successful, they can halt production, delay supply chains, and inflict contractual penalties. Unlike IT incidents, which may “only” cause data loss, OT Security failures can physically disrupt manufacturing lines and critical infrastructure.

In the public sector a lack of OT Security can cause disruption of vital societal functions with cascading consequences. Cyberattacks on public infrastructure are becoming increasingly sophisticated, often exploiting the convergence between IT and OT. If successful, such attacks can disable power grids, contaminate water supplies, halt public transportation, or paralyze emergency services.

One way to reduce this risk is by gaining a clear understanding of how IT and OT systems are interconnected. This knowledge enables organizations to continue operating critical OT functions even during IT-related security incidents.

Lack of skilled OT Security specialists

The demand for OT Security experts far exceeds the available talent pool. Many organizations struggle to find professionals who understand both cybersecurity and industrial processes, making it difficult to implement effective OT Security measures.

The IT-OT communication gap

One of the biggest challenges in securing OT environments is the disconnect between IT and OT teams. While IT security professionals focus on data integrity and confidentiality, OT teams prioritize system availability and safety.

These fundamental differences often result in:

- Misaligned security priorities
- Deeply rooted organizational challenges
- Critically delayed incident response
- Lack of responsibility and ownership of OT cybersecurity
- Differing risk perspectives and technical constraints
- Limited cross-domain cybersecurity expertise
- Lack of unified governance and accountability

Supply chain risks and third-party vulnerabilities

OT environments typically rely on complex supply chains, including partners, third-party vendors, contractors, and legacy equipment suppliers. Attackers often exploit such external connections to gain access to OT networks.

Therefore, organizations must:

- Create/update purchasing requirements and TS (Technical Specifications) regarding OT Security requirements.
- Check and improve service agreements with third-party stake holders to introduce accountability for OT Security in connection with deliveries, maintenance, implementation of on-site changes and such.
- Ensure that third parties follow the security policy and fulfills security responsibilities in documentable ways.
- Implement strict access controls for third parties.
- Establish sufficient security visibility and monitor for anomalies that could indicate supply chain compromises.
- Require a Software Bill of Materials (SBOM) from suppliers to gain visibility into the software components included in delivered systems and products – this facilitates vulnerability management, improves incident response, and reduces the risk of supply chain attacks.

Meet one of our Nordic OT Security specialists

Andreas Jacobsson | OT Solution Architect

Andreas Jacobsson has over 25 years in the food industry. He specializes in maintenance, project management, and ICS/OT network security. Andreas Jacobsson designs secure OT infrastructures that support both operational needs and business objectives. He conducts comprehensive security assessments and ensures compliance with industry standards. He is a frequent keynote speaker at cybersecurity events, where he brings clarity to complex OT challenges. His hands-on expertise makes him a trusted voice in the world of operational technology security.

Stronger OT Security starts with local responsibility and global standards

A good strategy involves appointing local employees responsible for on-site OT security, while also establishing a global OT security team to develop policies, procedures, and standards in close collaboration with IT.

Key elements of an effective OT Security strategy:

- **Establish separate but closely coordinated security policies for OT and IT.**
- **Provide cross-disciplinary communication and collaboration.**
- **Encourage regular communication between OT and IT teams.**
- **Conduct joint IT/OT risk assessments to uncover shared vulnerabilities.**
- **Align incident response plans across IT and OT teams.**
- **Crosstrain IT and OT staff to build mutual security awareness.**
- **Set security goals and KPIs for IT and OT.**
- **Standardize secure protocols and authentication in OT systems where applicable.**

> ”
>
> In today’s interconnected world, OT Security is no longer just an operational concern – it’s a strategic imperative. Therefore, leaders must prioritize resilience, foster collaboration between IT and OT, and embed security into the very fabric of their digital transformation.
>
> **Andreas Jacobsson | OT Solution Architect**

Bridging the gap:
Aligning IT and OT for better security

Diligent Risk Management is the backbone of any good security strategy. This goes for IT and OT alike – both areas should be view in context of each other. However, this can be easier said than done, as IT and OT Security in most cases are at quite different levels of maturity.

In fact, OT Security is often built almost from scratch, whereas IT Security is more refined after decades of development. This fundamental difference is further enhanced by a historical divide between IT and OT teams.

The importance of OT-specific governance

As OT differs from IT in many critical ways, a straightforward copy-paste of IT Security measures is not an option.

Instead, an OT-specific governance framework is essential for managing OT Security risks effectively.

> As digitalization accelerates, the true strength of an organization lies in its ability to protect its critical infrastructure. For C-suite executives, embracing a holistic, risk-based OT Security strategy is essential – because the cost of inaction is simply too high. The future belongs to those who act now.

Morten Skogvold | Managing Director

Cyberdefense

A strong and contemporary OT framework should include:

- A clearly definde methodology for management-level oversight of OT Security practices.
- Continuity planning for OT systems, including disaster recovery strategies.
- Implementation of local OT-specific documents:
  - OT Security Policy
  - Disaster Recovery Plan
  - Incident Response Plan
  - Business Continuity Plan
- Regular risk assessments in OT environments to identify vulnerabilities and prioritize mitigations.
- Asset inventory and classification of all OT systems to support risk-based decision-making.
- Security awareness training tailored to OT personnel to foster a strong cybersecurity culture.
- Monitoring and anomaly detection systems designed for OT-specific traffic patterns and protocols.
- Change management processes adapted to OT environments to ensure secure and controlled updates.
- Appointment of a Designated OT Security Officer (DSO) responsible for overseeing the OT cybersecurity strategy. The DSO must have both the authority and the necessary resources to perform this role effectively.
- Establishment of local OT responsibility roles and continued development of a central/global OT Security Team. This team should maintain and evolve security blueprints, policies, procedures, naming conventions, etc., and collaborate closely with production sites and IT.
- Implementation of a dedicated OT Site Responsible role, tasked with overseeing the entire site production network. This role should include a clearly defined mandate, resources, and a strong focus on security as a top priority.

OT Security in action:
Attack vectors and best practices

OT environments often evolve through organic expansion where new systems and components are continuously added without a cohesive, overarching security architecture.

This organic development process makes it difficult to maintain visibility, consistency, and control over the full attack surface, which is typically compromised by attack vectors like:

- Phishing via mail sent to IT devices also used for OT
- Social Engineering
- Supply Chain Attacks
- Unpatched IT systems integrated with OT
- Insufficient network segmentation
- Poorly protected wireless networks
- Malware and ransomware
- Removable media
- Remote access misconfigurations, unauthorized Remote Access
- Insider threats

Best practices

Strong OT Security depends on risk-based identification of all mission critical technology. In this process support systems can easily be overlooked. Say a production line is completely dependent on a server farm. Then these servers are OT too. But can they operate without server room cooling? No? Well, then the cooling system should be considered mission critical OT as well – and protected as such.

So what can you do to reduce the risk against your complex OT environments and avoid the most common attack vectors to stay ahead of threats while building a resilient OT Security posture? Start with these nine best practices.

Know your OT systems

Any device designed for maintaining/controlling production, availability and safety must be identified and protected as OT.

Visibility is key

With good visibility throughout your OT Security, you can spot irregular data patterns and suspicious events much faster. It also makes it far easier to implement efficient segmentation and asset management. Good visibility should also include all OT dependencies. That is, any systems with potential to interrupt OT operations. This can be anything from billing systems to Wi-Fi-networks, servers or server room cooling.

Segment your networks

Separating IT and OT networks reduces the attack surface, preventing cyber threats from spreading between environments. Any segmentation of OT networks should be based on extensive risk assessment.

Strengthen remote access controls

Adopt multi-factor authentication (MFA) and role-based access to limit exposure to unauthorized users.

Implement procedure to handle vulnerabilities

Have an efficient procedure in place to handle vulnerabilities. Either through patching, mitigation or feature removal. Patching is not always the only way of mitigating vulnerabilities.

Continuous monitoring and threat detection

Deploy OT-specific monitoring solutions to detect anomalies and potential threats in real time.

Implement an OT risk management framework

Schedule and plan for regular risk assessments. Regular risk assessments are required for OT systems to identify vulnerabilities and threats, ensuring continuous adaptation to new risks.

Harden devices

Many devices in OT have unused features enabled, which enlarger their attack surface to no benefit. They may also have disabled security features, which decrease control. Optimizing the configuration of these devices in a standardized way can lead to a quick and effective increase in OT Security.

Define roles and responsibilities

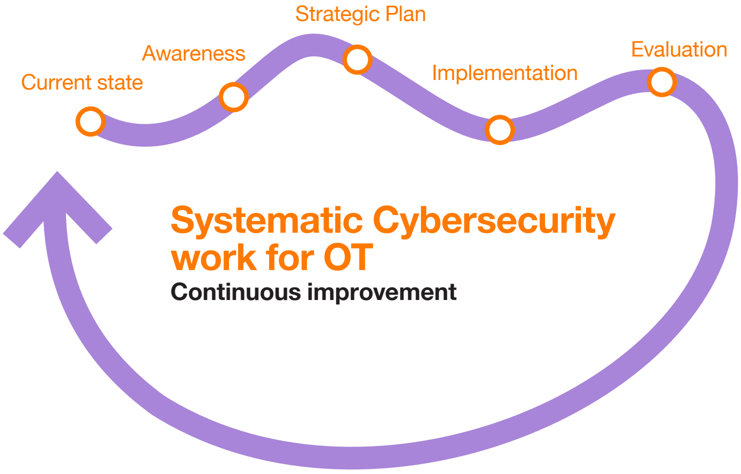
Effective OT Security requires clearly defined roles and responsibilities. Who owns security in the OT environment? Is there a process in place to handle incidents? Ensure that both IT and OT teams share a common understanding of security objectives and collaborate to achieve them. Clear accountability increases efficiency and reduces the risk of critical actions being overlooked.

Key steps to proactive and holistic OT Security

As we have seen in IT-related cybercrime, the threat level against OT will gradually increase too. Today, most attacks are not exclusively targeting OT – they start in IT and expand from there. But this will not be the case forever. Dedicated OT malware has already been detected in the wild – especially in the wake of armed conflicts.

For obvious reasons, OT is a desirable target, and modern organizations should act accordingly as they increase the data exchange between IT and OT. A reactive stance – which is to respond only after being attacked – is a dangerous strategy likely to result in significant damage. Both operationally, environmentally, financially, and by loss of image.

While dedicated OT attacks may still be much less frequent than attacks on IT, a wise strategy would be to consider this as a window of opportunity to focus on stronger prevention against what is to come. **Here are some of the most important focus areas:**



Use an established security framework

One of the most effective ways to ensure robust OT Security is by adopting established security frameworks such as CIS, NIST CSF 2.0, ISO 27001/2, ISO 27005, and IEC 62443. They provide a structured approach to securing Industrial Control Systems (ICS).

These frameworks help organizations identify vulnerabilities, implement risk management processes, and ensure a consistent security posture across their OT environments – even in multinational scenarios. They also provide common language and standardized procedures, which are essential in bridging the communication gap between IT and OT teams.

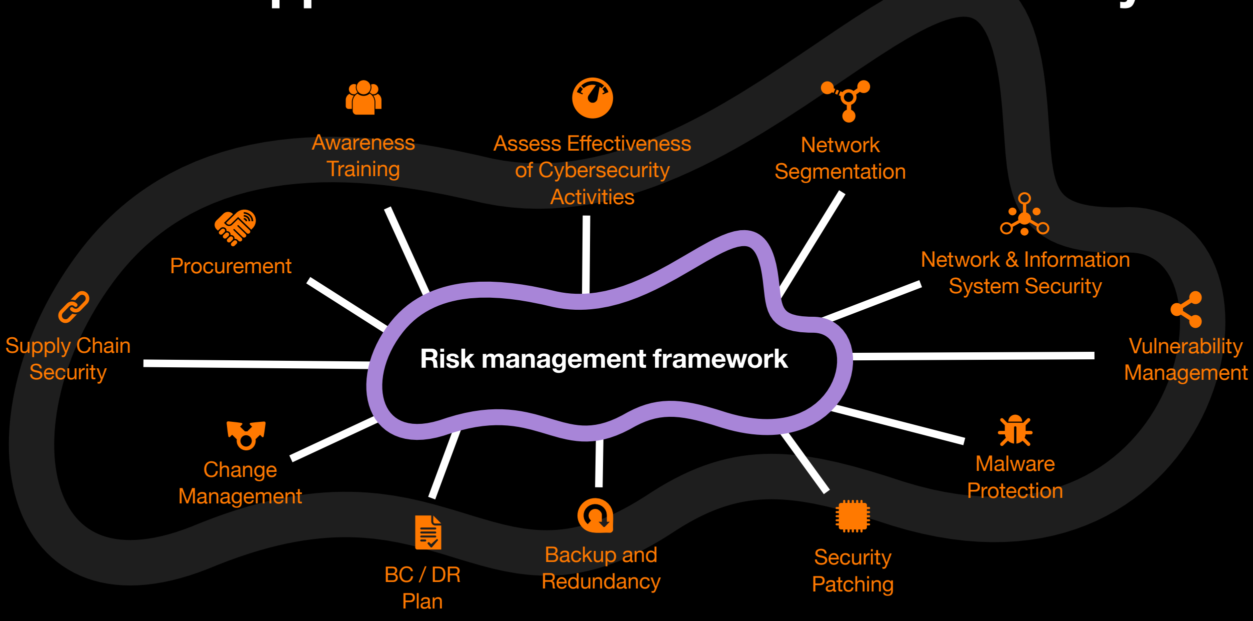
Base your OT Security on Risk Management

Understanding how to grade the level of security according to business goals and available resources is key to success.

Ideally, this should include:

- **Continuous monitoring and improvement** of the OT Security posture to ensure alignment with evolving threats and business objectives.
- **Inventory of all OT assets** to identify and grade critical systems and vulnerabilities.
- **Assessment of risk levels** by determining the potential impact of cyber threats on critical operations.
- **Prioritizations of all security investments** based on risk assessments to protect the most critical and vulnerable assets sufficiently.

A risk-based approach is essential for OT Security



Secure remote access and third-party integrations

Many cyberattacks originate from unsecured remote connections or third-party vendors. To mitigate these risks, organizations should:

- Choose only one remote access solution for all support and remote configuration.
- The solution should have supervised access and the ability to record all sessions with logging, approval flow, and support of Multi-Factor Authentication (MFA).
- Segment access based on roles and actual need.
- Limit remote access to time-bound sessions.
- Inventory and risk-classify all third parties with OT access.
- Remote access solutions should also be used for internal communication from the IT network to the OT Systems.
- Enforce MFA for remote access.
- No network access – use only application access.
- Monitor remote access for suspicious activity.
- Use approval flow for remote access.

Deploy network segmentation and multiple layers of defense

Traditional flat OT networks are highly vulnerable to cyber threats as they typically allow access to all assets. Implementing network segmentation and layered security controls significantly reduces risk:

- Ensure deterministic communication paths between segments to preserve real-time performance and safety integrity.
- Create security zones to limit lateral movement and isolate critical assets.
- Separate IT and OT networks to minimize attack surfaces.
- Use firewalls, Intrusion Protection System (IPS) designed for OT and Intrusion Detection Systems (IDS) to monitor and control network traffic.
- Deploy role-based access controls (RBAC) to restrict unauthorized access to critical systems.

Focus on employee awareness and training

Human error remains one of the largest vulnerabilities in OT Security. Continuous education and training programs help employees recognize and respond to threats effectively:

- Implement OT cybersecurity awareness training.
- Regular training and awareness programs for personnel managing OT systems are required, ensuring that they can recognize and respond to potential threats effectively.
- Develop clear incident response protocols to guide employees in case of an attack.
- Use tabletop exercises.

Continuously monitoring and proactively use of threat intelligence

A proactive approach to OT Security requires real-time monitoring and intelligence-based threat detection. These are the cornerstones to stay ahead of threads. This approach includes:

- Monitoring OT systems for anomalies, threats, and performance as this is critical to early detection detecting.
- Regular testing and auditing of OT systems to ensure they remain secure and resilient.
- Passive scanning, and if possible, active detection using the same monitoring tool for passive scanning on OT devices.
- Monitoring for malicious code should also be introduced – especially on assets with high risk of infection.
- Monitoring for unauthorized connections and devices to ensure the full visibility while it's important that the tool sees all traffic.
- Monitoring and logging of network and infrastructure activity to detect potential security breaches.
- Monitoring for unauthorized software installations or usage on OT systems.

Prepare your crisis management and plan for recovery

Time is crucial – especially in OT, where any good security strategy must include plans for getting back on track as fast as possible. To ensure that, the key action points are:

- Develop a well-defined incident response plan to detect, respond to, and recover from cyber incidents.
- Identify, assess, and analyze risks to understand threats, vulnerabilities and potential impacts – not only from cyberattacks but also from natural disasters, workplace violence, data breaches, and more.
- Appoint key stakeholders responsible for incident response and crisis management.
- Define clear procedures for responding to specific incidents, including steps for identifying the incident, containing it, assessing the impact, communicating with stakeholders, and recovering operations.
- Report any significant cybersecurity incidents affecting OT systems to relevant authorities.
- Establish communication protocols for the incident response team, stakeholders, employees, customers, and the media. Clearly define who is responsible for communicating during a crisis, what information will be shared, and how.
- Test the incident response plan regularly to identify any weaknesses or gaps. Conduct tabletop exercises and simulations to test the effectiveness of your plan. Update the plan based on results, lessons learned, and any changes in your organization or industry.

The Colonial Pipeline ransomware attack: A stark warning for OT Security

On May 7, 2021, the hacker group DarkSide gained access to the network of US company Colonial Pipeline.

Reportedly, the attack was initiated by use of a compromised VPN password with no multi-factor authentication.

100 gigabytes of data were stolen, and the group then proceeded to deploy ransomware, encrypting crucial files, including those related to billing and accounting.

A wake-up call:

Lessons learned and measures taken since the Colonial Pipeline attack

The Colonial Pipeline attack exposed critical vulnerabilities in the convergence of IT-and OT environments, particular highlighting the severe consequences of weak access controls and insufficient and inadequate authentication measures. This incident demonstrated how cybercriminals can exploit IT systems to disrupt essential OT operations, causing widespread operational and ecomomic impact. A key takeaway was the urgent need to implement strong multi-factor authentication (MFA) across all remote access points, particularly VPNs, to reduce the risk of credential compromise.

In response, both government agencies and private organizations have taken concrete steps to strengthen OT security, underpinned by official directives and expert guidance:

Strengthened regulatory requirements:
Shortly after the attack, the U.S. government issued an Executive Order on Improving the Nation's Cybersecurity, mandating enhanced cybersecurity standards for critical infrastructure. This includes stricter requirements for zero trust architecture, MFA implementation, encryption, incident reporting, and improved risk management specifically addressing OT environments.

Enhanced guidance from CISA:
The Cybersecurity and Infrastructure Security Agency (CISA) has published multiple advisories emphasizing the importance of investing in network segmentation, multi-factor autentifikation, real-time monitoring tools, and robust access controls in OT networks to help limit malware spread, reduce attack surfaces, and enable continuous threat detection to rapidly identify anomalous behavior.

Law enforcement recommendations:
The FBI has highlighted the growing ransomware threat to OT systems and urges organizations to adopt strong access management, incident response planning, and regular cybersecurity awareness training as part of their OT Security strategies to ensure staff responsible for OT Security receive better education about emerging threats and best practices.

Different measures focusing on collaboration between government agencies, industry groups, and cybersecurity providers have been implemented to facilitate faster response and better recovery during incidents. Coordinated response frameworks have also been developed to improve preparedness and resilience.

All these efforts aim to reduce the likelihood and impact of future attacks, emphasizing the vital importance of treating OT Security as a business-critical priority.

Overall, these developments mark a significant shift toward recognizing OT security as an essential aspect of organizational risk management. The Colonial Pipeline attack served as a wake-up call, prompting tangible improvements in cybersecurity posture across industries managing OT environments.

Understand AI’s role in a connected industry

Intelligent protection

Industry 4.0 brings increased connectivity and complexity, as the physical and digital worlds merge through cloud services, data analytics, and autonomous systems. In this evolving landscape, artificial intelligence (AI) is no longer optional – it’s a strategic necessity. For OT security to keep pace, this means we must shift from static controls to intelligent, learning-based protection.

AI enables real-time analysis and decision-making in ways traditional methods cannot. Rather than relying on predefined rules and manual reviews, AI learns what “normal” looks like and flags deviations that may signal a cyberattack, malfunction, or insider threat. This becomes especially important as operational systems become more self-optimizing and less reliant on human oversight.

Yet we must also recognize that AI is being used by threat actors to create malware that evades detection, adapts to its environment, and targets critical infrastructure with precision. To stay ahead, defenders must embrace AI with the same ambition, applying it to detection, response, and strategic forecasting.

Key takeaway

Without forward-thinking security, the promise of Industry 4.0 becomes a risk. But with the right application of AI, OT environments can become more resilient, adaptive, and secure than ever before.

Going forward, industrial and critical infrastructure leaders must ask:

- How can we ensure our security is learning, not just monitoring?
- How do we train AI on the right data – and protect that data from manipulation?
- What happens when decision-making is automated – and how do we maintain traceability and control?
- How can we use AI to reduce response times while under standing the full impact?
- How do we secure digital twins, autonomous systems, and self-optimizing factories?

Our customers say it best...

> **Orange Cyberdefense’s long pedigree in OT was invaluable – their deep understanding fostered trust, encouraging open dialogue and engagement throughout the assessments, which naturally led to upskilling and an accurate ‘as-is’ of our industrial environment.**

Fawzi Aiboud Nygren, BISO, Volvo Group Trucks Operations

VOLVO

Volvo Group Trucks Operations

Volvo Group Trucks Operations is a division of the Volvo Group that manufacture and sell commercial trucks and handle logistics and spare parts under several global brands, including Volvo, Mack Trucks and Renault Trucks. The business provides a wide range of heavy-duty and medium-duty trucks for various transport and logistics applications.

Faced with new NIS2 legislation Volvo Group Trucks Operations decided to let Orange Cyberdefense assess OT Security maturity at ten strategically selected sites. The goal was to get better insights of the current OT environment to work more systematically with a risk-based approach across the organization.

This is how we help strengthen your OT Security

At Orange Cyberdefense, we understand the critical nature of OT and the fundamental differences between OT and IT Security. Due to their fundamental differences, a direct copy/paste approach is not feasible.

Managed OT Security Services

Our managed OT Security Services are designed to offer continuous protection, real-time monitoring, threat detection, and incident response, all while ensuring that your OT systems remain secure.

This include:

- Managed Firewall for OT
- Managed Industrial Security [Identify]
- Managed Industrial Security [Detect]
- Managed Threat Detection [log] IT /OT Patterns
- Managed Endpoint protection for OT

Our expertise extends across various verticals and sectors, and we provide a range of services developed to safeguard both physical and digital aspects of OT environments to the highest market standards.

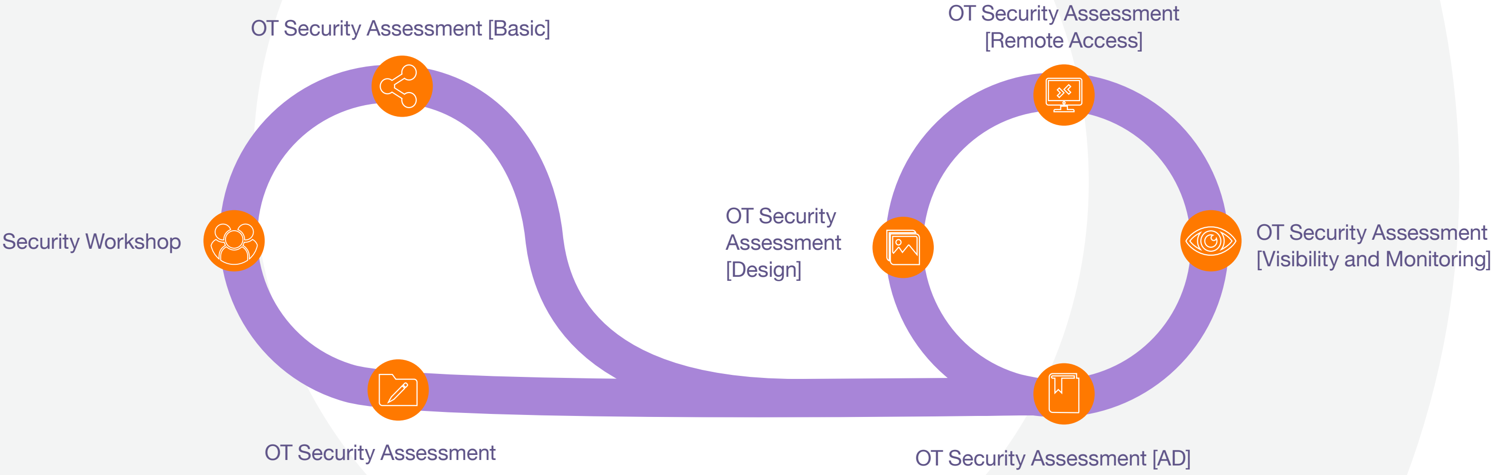
Advisory OT Security Services

At a time where many organizations struggle to recruit and retain highly skilled OT Security specialists, we offer a different approach. Across the Nordics we have built a strong team of experienced OT Security consultants ready to help increase your defenses significantly.

Key offerings from our OT Security consultants:

- GRC for OT
- OT Security Officer as a Service

We conducts the following OT Security Assessments:


OT Security Assessment [Basic]
Security Workshop
OT Security Assessment
OT Security Assessment [Remote Access]
OT Security Assessment [Design]
OT Security Assessment [Visibility and Monitoring]
OT Security Assessment [AD]

Meet one of our Nordic OT Security specialists

Martin Blak | Senior Trusted Advisor

Martin Blak has been working with critical infrastructure for many years. He specializes in enterprise security architecture that spans IT, OT, and cloud environments. Martin takes a holistic approach to security, helping enterprises implement solutions that are business-enabling and tailored to their specific needs. He has supported multiple large companies in implementing visibility and segmentation within their OT environments and brings broad knowledge of various technologies to the table. Grounded in the belief that automation is key to efficient operations, Martin helps customers streamline procedures through coding and AI, enabling smoother and more resilient IT operations.

OT Security Assessment – an important first step in the right direction

While IT Security has had several decades to mature, the need for OT Security often rests on a much less standardized basis of unmonitored legacy systems and low network transparency.

What communicates with what and why? This is essential knowledge to get off on the right foot.

> The path to a resilient and secure future is paved with strategic vision and decisive action. OT Security is not just an IT issue – it's a core business risk that demands leadership, collaboration, and a forward-thinking mindset.

Martin Blak | Senior Trusted Advisor

OT Security assessment
Security posture and recommendations

You should consider doing an OT assessment if you want?

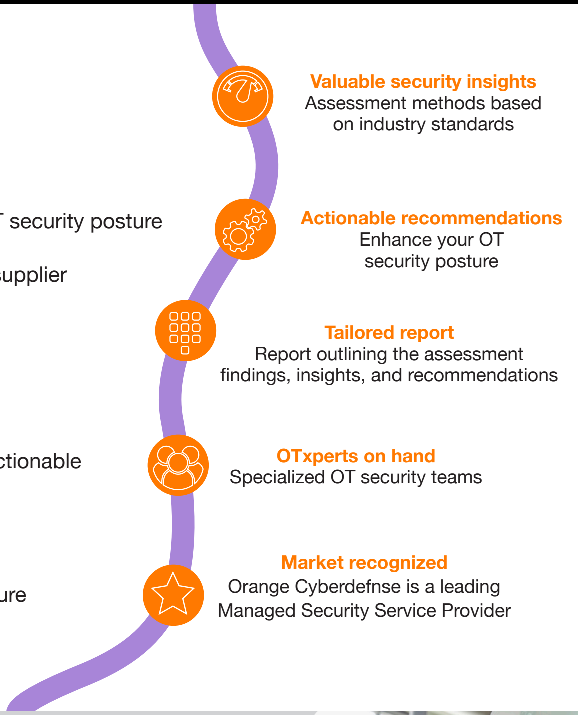
- Deeper insights into your security posture and most urgent security needs
- To takt the next steps into identity and prioritize on how to best improve your OT security posture
- A security analysis of your OT network communication
- To understand the security awareness and maturity level of your emplyees and supplier

What we do:

- Initial kickoff meeting with your responsible experts
- Extended collection of information through interviews and document reviews
- Site walkdowns
- Review of OT network security design bases on gathered information
- Detailed assessment repprt including list af assets, vulnerabilities, threats and actionable recommendations with regards to people, processes and technology

What will you get?

- Insight of your OT security posture
- Data-driven analysis with actionable insights to enchance your OT security posture
- Assessment report containing the identified status of your security posture



Valuable security insights
Assessment methods based on industry standards

Actionable recommendations
Enhance your OT security posture

Tailored report
Report outlining the assessment findings, insights, and recommendations

OTxperts on hand
Specialized OT security teams

Market recognized
Orange Cyberdefnse is a leading Managed Security Service Provider

The OT Showroom Experience in Lyon

At Orange Cyberdefense's OT Showroom in Lyon we offer an extensive, tailormade, interactive, hands-on experience where decision-makers can witness OT Security in action. This unique facility showcases the latest OT Security technologies and provides a real-time demonstration of how our solutions work to defend critical systems. Visitors can engage in practical exercises, observe simulated cyberattacks, and learn how to address security challenges in their own environments.

Read more

Thinking ahead:

How to future-proof OT Security

As companies and organizations continue to digitalize and adopt new technologies, OT Security will need to adapt to meet emerging threats from the rapidly changing threat landscape. Here are some of the key trends, as we see them, liable to impact the future of OT Security.

Deeper integration of IT and OT

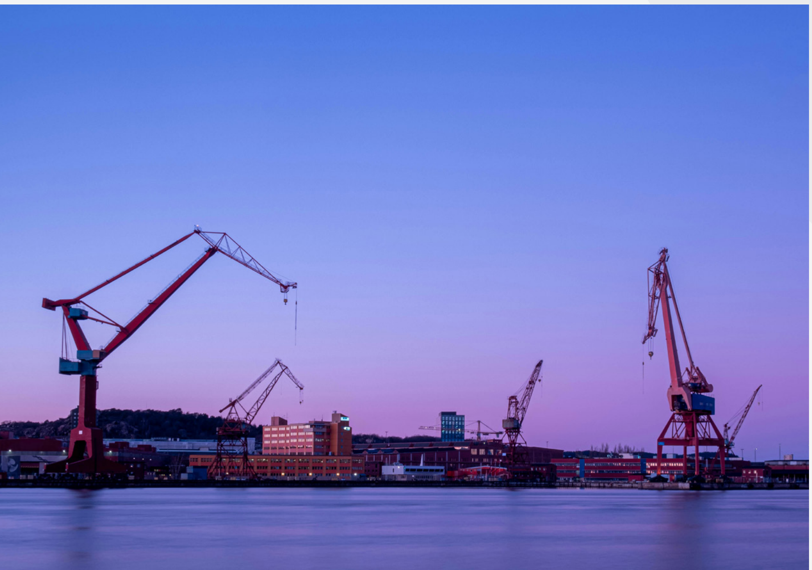
As businesses increase communication between IT and OT environments for greater efficiency and data sharing, **the security risks associated with this integration are growing.** Effective security strategies will need to bridge both worlds seamlessly.

Stricter regulatory requirements

Future regulations are placing increased demands on **security in OT environments.** Organizations must act not only to protect operations but also to **meet legal and compliance requirements.**

Skills gap and training

As OT security becomes more complex, the need for specialized expertise grows. Organizations must invest in training and recruiting personnel with knowledge across both IT and OT domains.



Architectural changes

Concepts such as **Zero Trust are starting to be applied in OT environments** as well. This requires both technical and organizational adjustments to ensure that no device or user is implicitly trusted with access to critical resources.

Rise of IoT and industry 4.0

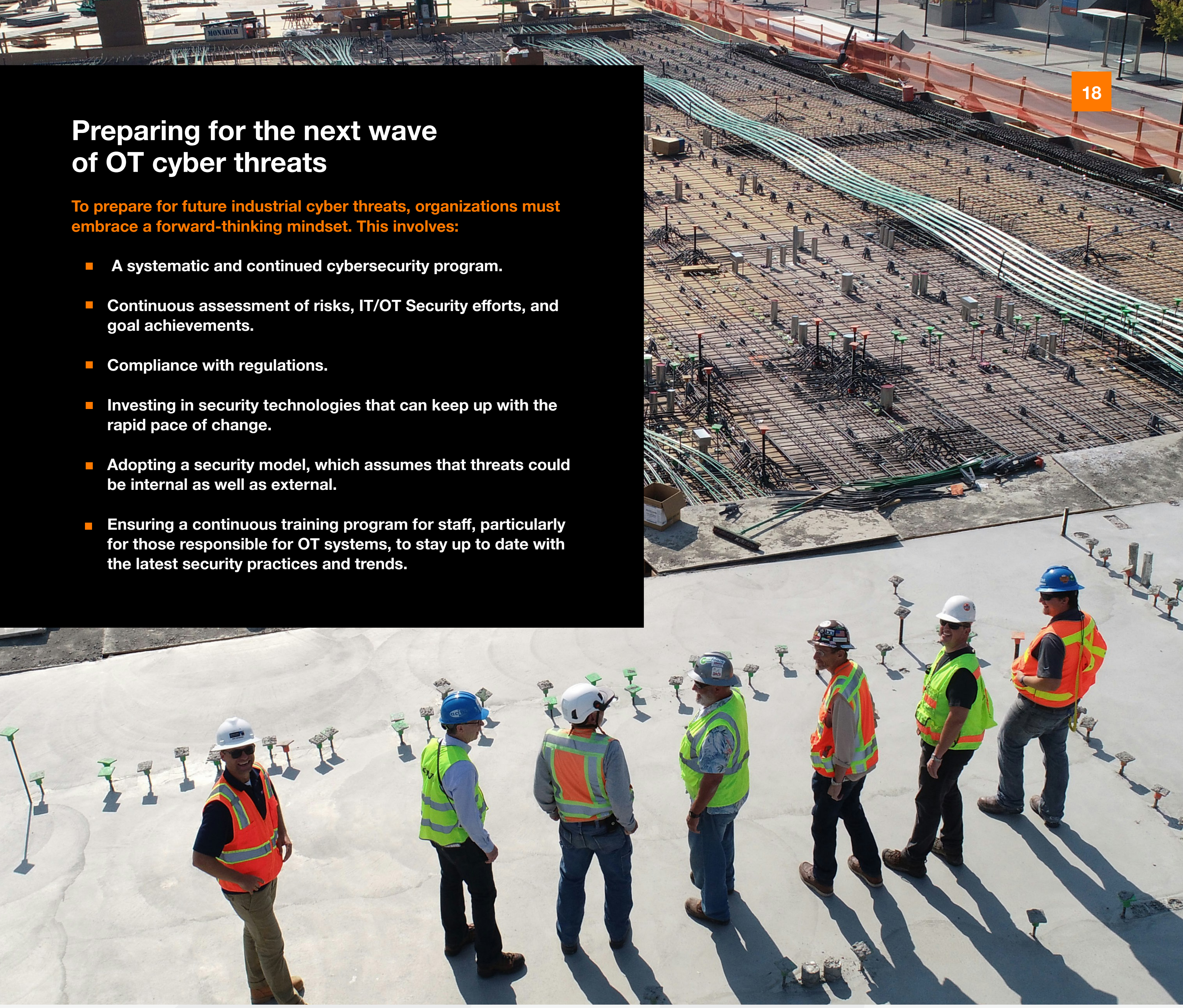
The growth of Internet of Things (IoT) devices in industrial settings presents new challenges for OT Security. **With more connected devices, the attack surface expands**, requiring advanced protection measures.

Advanced threats and attack vectors

Cybercriminals are becoming more sophisticated, using advanced techniques like ransomware and supply chain attacks to target OT environments. Future **OT Security systems must be equipped to deal with these evolving threats**.

The Impact of AI and IoT on OT Security

AI and IoT are double-edged swords in OT Security. While they enable greater operational efficiency, they also **introduce new vulnerabilities**. AI-driven predictive maintenance and IoT-enabled devices can be exploited if not adequately secured. As IoT devices proliferate across industrial environments, **securing these endpoints will become increasingly critical**.



Preparing for the next wave of OT cyber threats

To prepare for future industrial cyber threats, organizations must embrace a forward-thinking mindset. This involves:

- A systematic and continued cybersecurity program.
- Continuous assessment of risks, IT/OT Security efforts, and goal achievements.
- Compliance with regulations.
- Investing in security technologies that can keep up with the rapid pace of change.
- Adopting a security model, which assumes that threats could be internal as well as external.
- Ensuring a continuous training program for staff, particularly for those responsible for OT systems, to stay up to date with the latest security practices and trends.

Our customers say it best...

EcoDataCenter

> **Conducting a security assessment is not just about identifying security gaps - it's about building a resilient foundation for the future. By evaluating our OT Security practices, we've been able to implement meaningful improvements, ensuring stronger defenses and compliance with evolving standards like NIS2 and NIST.**

Julian Beauregard Camp, Subject Matter Expert OT, EcoDataCenter

EcoDataCenter

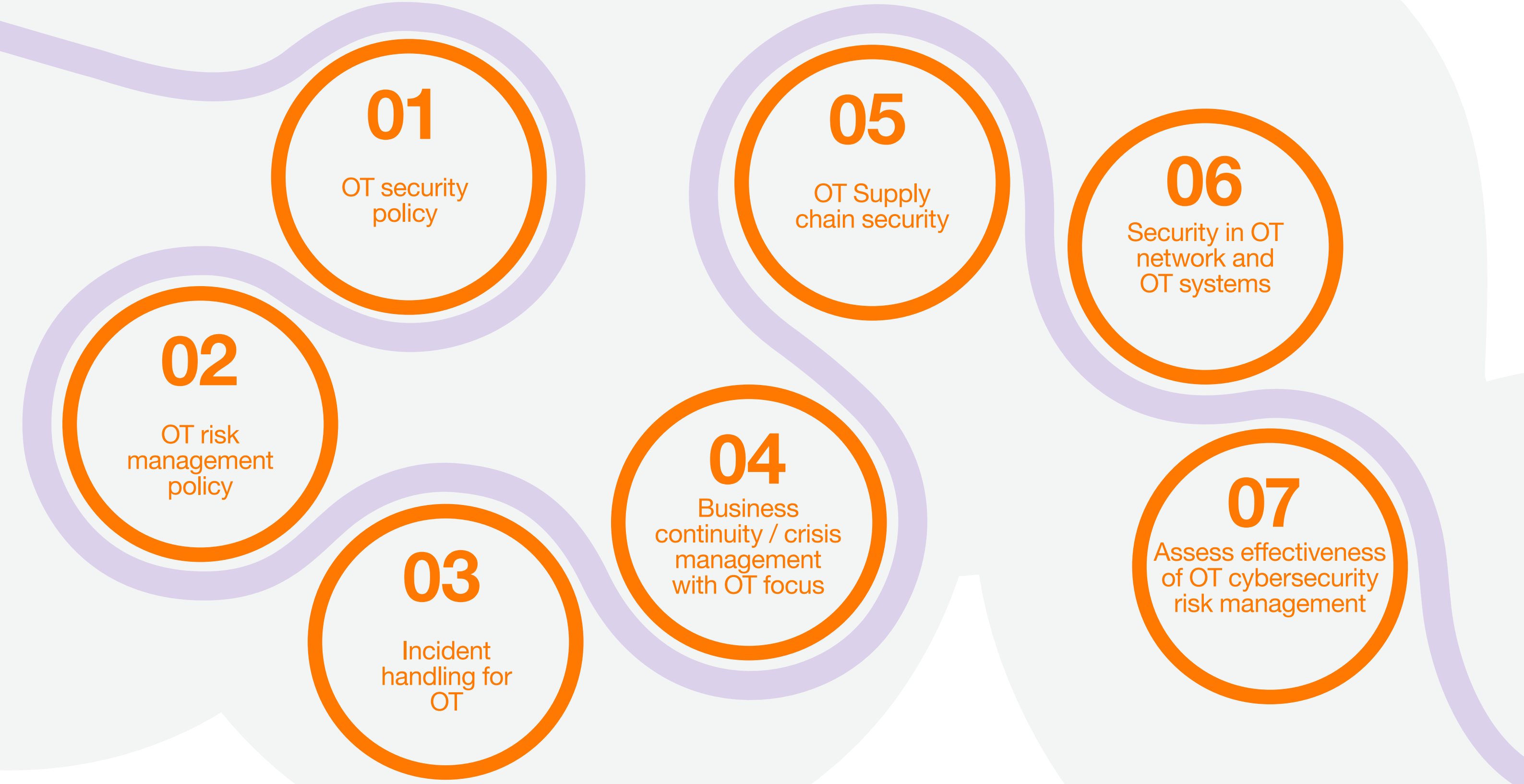
EcoDataCenter is a data center provider focused on sustainable and energy-efficient infrastructure. They offer secure, reliable hosting solutions with an emphasis on minimizing environmental impact through renewable energy use and innovative cooling technologies.

In 2021 EcoDataCenter asked Orange Cyberdefense to assess it's OT Security and used this knowledge to carry out improvements. The assessment process was repeated in 2024 to evaluate and get a new current state of maturity.

How NIS2 drives the need for mature OT Security

To strengthen IT- and OT Security across Europe, the EU has issued the NIS2 directive. The directive has been implemented into national law by the 27 EU countries. As the directive is particularly focused on organizations working with critical infrastructure, it has a strong emphasis on OT Security requirements.

Technical and methodological requirements - from an OT perspective:



01 OT security policy

02 OT risk management policy

03 Incident handling for OT

04 Business continuity / crisis management with OT focus

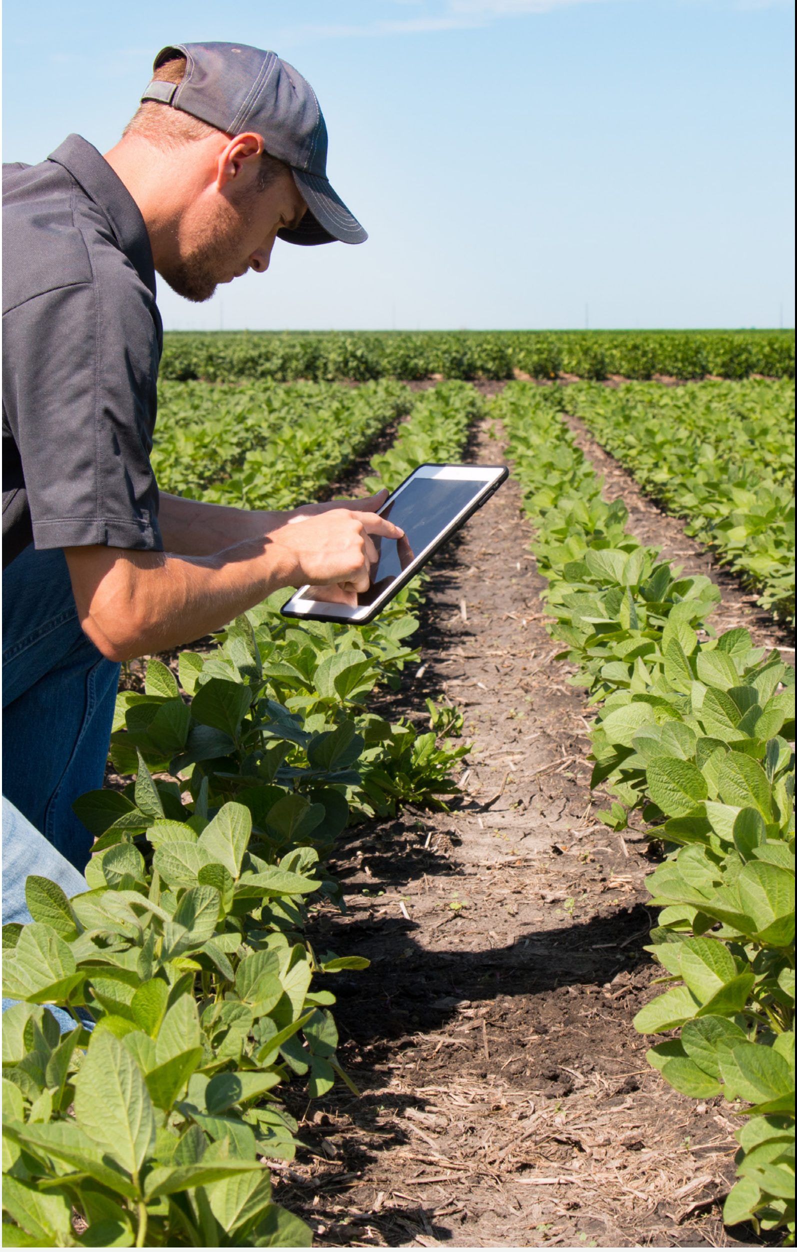
05 OT Supply chain security

06 Security in OT network and OT systems

07 Assess effectiveness of OT cybersecurity risk management

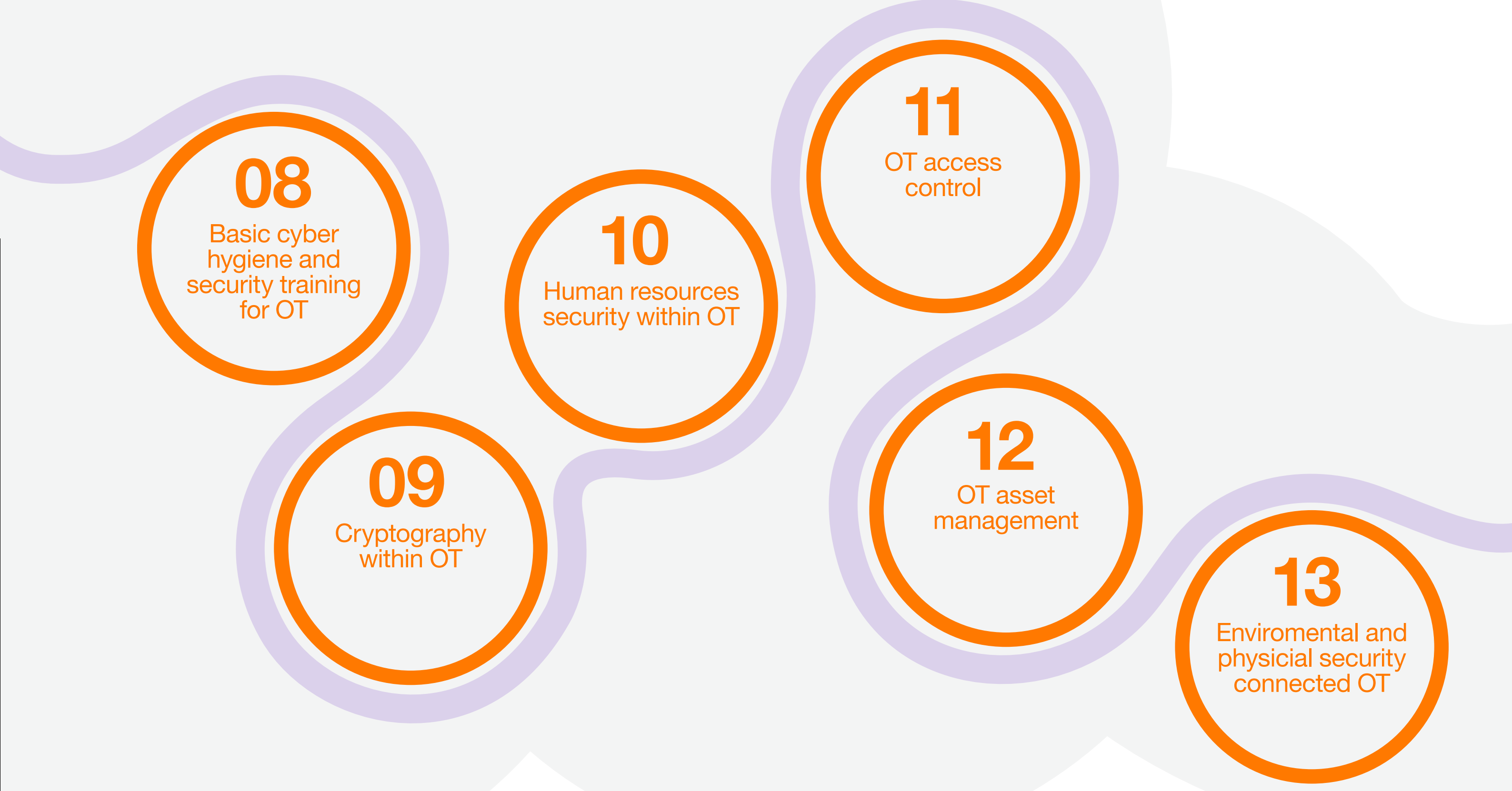
Meet one of our Nordic OT Security specialists

Carsten Lyth | Business Area Manager, OT Security
Carsten Lyth has more than 30 years of experience working with OT systems in the industrial sector. He has held various roles, including project engineer, engineering manager, and leadership positions where he has led technical projects and organizations in complex and demanding industrial environments. His extensive background in the industry has given him a deep understanding of customers' diverse processes, technical environments, and business-critical needs – from the shop floor to executive level. He has also worked as Head of Standardization, focusing on industrial collaboration and the development of common guidelines and technical standards. For the past three years, Carsten has served as Business Area Manager for OT Security at Orange Cyberdefense, where he helps clients understand, protect, and develop their industrial systems in an increasingly digitalized and threat-exposed world.



> Effective OT Security is a business enabler, not just a technical necessity. It requires visionary leadership, proactive risk management, and a unified approach across all levels of the organization. Those who lead with foresight will safeguard their operations and secure their competitive advantage.

Carsten Lyth | Business Area Manager, OT Security



08 Basic cyber hygiene and security training for OT

09 Cryptography within OT

10 Human resources security within OT

11 OT access control

12 OT asset management

13 Enviromental and physicial security connected OT

From assessment to action: Building a strategic OT roadmap

Any successful OT Security strategy should be built on a clear, strong and resilient roadmap that includes short-term and long-term objectives.

Start by building a strategic roadmap

This roadmap should align with the business goals, address key vulnerabilities, and set out the steps needed to achieve a secure OT environment.

Start by assessing the current security posture, identifying critical assets, and implementing a risk management framework. Over time, the roadmap should evolve to accommodate new technologies, business needs, and emerging threats.

Key takeaways for decision makers

For decision-makers, understanding the importance of OT Security is the first step toward creating a resilient, secure industrial environment. Key takeaways include:

- OT Security is not optional - it is critical to business continuity and risk management.
- A collaborative approach between IT and OT teams is essential for success.
- Future-proofing OT Security requires ongoing investment in technology, training, and incident response.

How to get started with OT Security

If you're just starting your OT Security journey, the first step is to assess your current risk landscape. Work with experts to identify potential vulnerabilities and begin implementing the necessary solutions to safeguard your OT environment. Leverage resources like OT Security Assessments, Ethical Hacking, and Managed Security Services to accelerate your security strategy.

Strengthening OT Security through compliance and leadership

With the introduction of the NIS2 Directive, requirements for OT Security are becoming significantly more stringent – particularly in governance, risk management, compliance, and incident handling. For many organizations, this means addressing legacy industrial environments that were never designed with today's cybersecurity standards in mind.

Even with investments in new technologies and operational efficiencies, the existing OT infrastructure often remains vulnerable. This makes leadership commitment a critical success factor. Organizations that approach OT Security as a strategic, board-level priority experience fewer breaches, faster response times, and better control over their risk landscape.

At the same time, integrating OT systems with IT environments can unlock enormous business value, but it also introduces new security challenges. By embedding OT Security into your overall corporate governance, you not only comply with regulations like NIS2, but also strengthen resilience and reduce the number of incidents. The most mature organizations consistently report far fewer security events – proving that a strategic, leadership-driven approach pays off.

Key takeaways include:

- NIS2 sets stricter requirements for OT Security, especially around governance, compliance and risk management.
- Legacy OT environments increase vulnerability and demand proactive security measures.
- Leadership-driven OT strategies result in fewer incidents and stronger resilience.
- Integrating OT and IT systems creates business opportunities but also new security risks that must be managed.

Why is it important so to approach OT Security the right way?

Mistakes in the inital stages can lead to vulnerabilities that are difficult to correct later.

- Risk identification and Prioritization
- Prevent Costly Mistakes
- Ensureing Safety
- Maintaining Operational Continuity
- Compliance and Regulation
- Building a Strong Security Culture

Accreditations and industry recognitions

In the cybersecurity industry, recognized standards and certifications are essential indicators of expertise and reliability. As a market leader within Managed Security Services, Orange Cyberdefense holds numerous industry certifications and recognitions, validating our commitment to excellence.

Recognised leadership

Orange Cyberdefense has consistently been ranked by top industry analysts, including Gartner, Forrester, IDC, Omdia, and Everest Group, as a leader in Managed Detection and Response (MDR). This recognition underscores our technical capabilities, customer satisfaction, and operational excellence.

Proven standards of service

We are committed to following global standards such as ISO, SOC2, and CREST. These certifications ensure that we maintain rigorous security practices, covering everything from incident management to ongoing threat intelligence and response. Our proven compliance with these standards demonstrates our dedication to delivering reliable, high-quality security services that you can trust.

A trusted partner

Partnering with Orange Cyberdefense means aligning with a security provider recognized for its integrity, expertise, and dedication to protecting clients worldwide. Our long-standing relationships with global security organizations demonstrate our commitment to the highest standards in cybersecurity.

We're aiming for the highest standards of excellence.

But don't just take our word for it.

Gartner®

Gartner listed Orange Cyberdefense as a Representative Vendor in the Market Guide for Managed Detection and Response, Managed Security Services, Digital Forensics & Incident Response, Threat Intelligence and Operational Technology Security.

OMDIA

Omdia views Orange Cyberdefense as a leader in global IT security services: "The provider has demonstrated considerable commitment, strategic vision and solutions capability across various end-to-end security service categories including cloud, endpoint, OT, SASE, infrastructure and security intelligence".

FORRESTER®

Forrester ranks Orange Cyberdefense as a leader. According to the Forrester report: "Orange Cyberdefense delights its customers with high quality technical services. Orange Cyberdefense continues to extend its capabilities in cloud security and managed detection and response capabilities."

IDC

IDC positions Orange Cyberdefense in the Leaders category in the IDC Marketscape: European Managed Detection and Response Services 2024 Vendor Assessment. "Orange Cyberdefense provides an extensive range of managed and professional security services, enabling it to help organizations comprehensively mitigate cyber-security risk."

Everest Group
RESEARCH

The Everest Group recognized Orange Cyberdefense as a leader for Managed Threat Detection. In the researcah, Everest Group assesses 27 MDR service providers globally featured on the MDR Services PEAK Matrix® Assessment.

orange™ Cyberdefense - who are we?

Global positioning

Orange Cyberdefense is a leading European cybersecurity and Managed Security Service Provider with over 25 years of experience. We specialize in delivering consulting, solutions, and services to our customers worldwide. We are recognized as a leading MSS provider by information technology research and advisory companies such as Gartner, Forrester, and IDC.

We have a global Threat Intelligence department, and 250+ analysts spread across **17 SOCs, 15 CyberSOCs, 11 CERTs,** and **4 scrubbing centres** to mitigate DDoS attacks which collect and analyze global data from over **500 information sources 24/7.**

Local presence

In the Nordics, our team consists of **500 employees** across Denmark, Norway, and Sweden. Our Nordic offices are located in Copenhagen & Aarhus (Denmark), Stockholm, Malmo, Gothenburg & Sundsvall (Sweden), and Oslo (Norway).

Our customers include multinational companies, public organizations, and government authorities.

Our growth journey

We have over **3,100 employees** globally and 50,000 customers worldwide of which 6,000 are large enterprises. We have experienced stable economic growth and progress over the years. In 2024, our global revenue was **€1.2 billion.**

Part of Orange Group

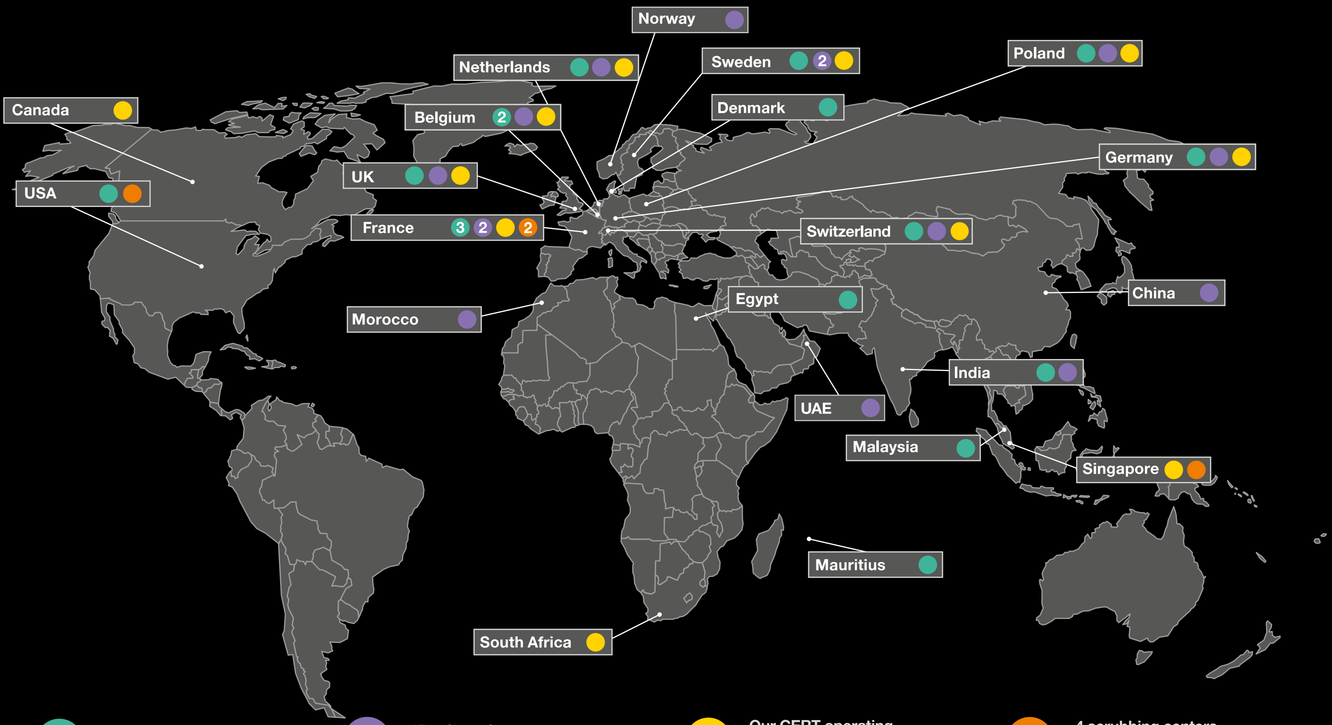
Orange Cyberdefense is part of the global French telecommunications group **Orange,** which has 137,000 employees and **296 million customers** worldwide. In 2024, **Orange Group** had a global revenue of **€40,3 billion.**

For more information, visit:
orangecyberdefense.com/no

Contact us

✉ **info@no.orangecyberdefense.com**

☎ **+47 67 57 37 37**



● 17 points of presence of our SOC

● 15 points of presence of our CyberSOC

● Our CERT operating continuously from 11 countries

● 4 scrubbing centers to mitigate DDoS attacks