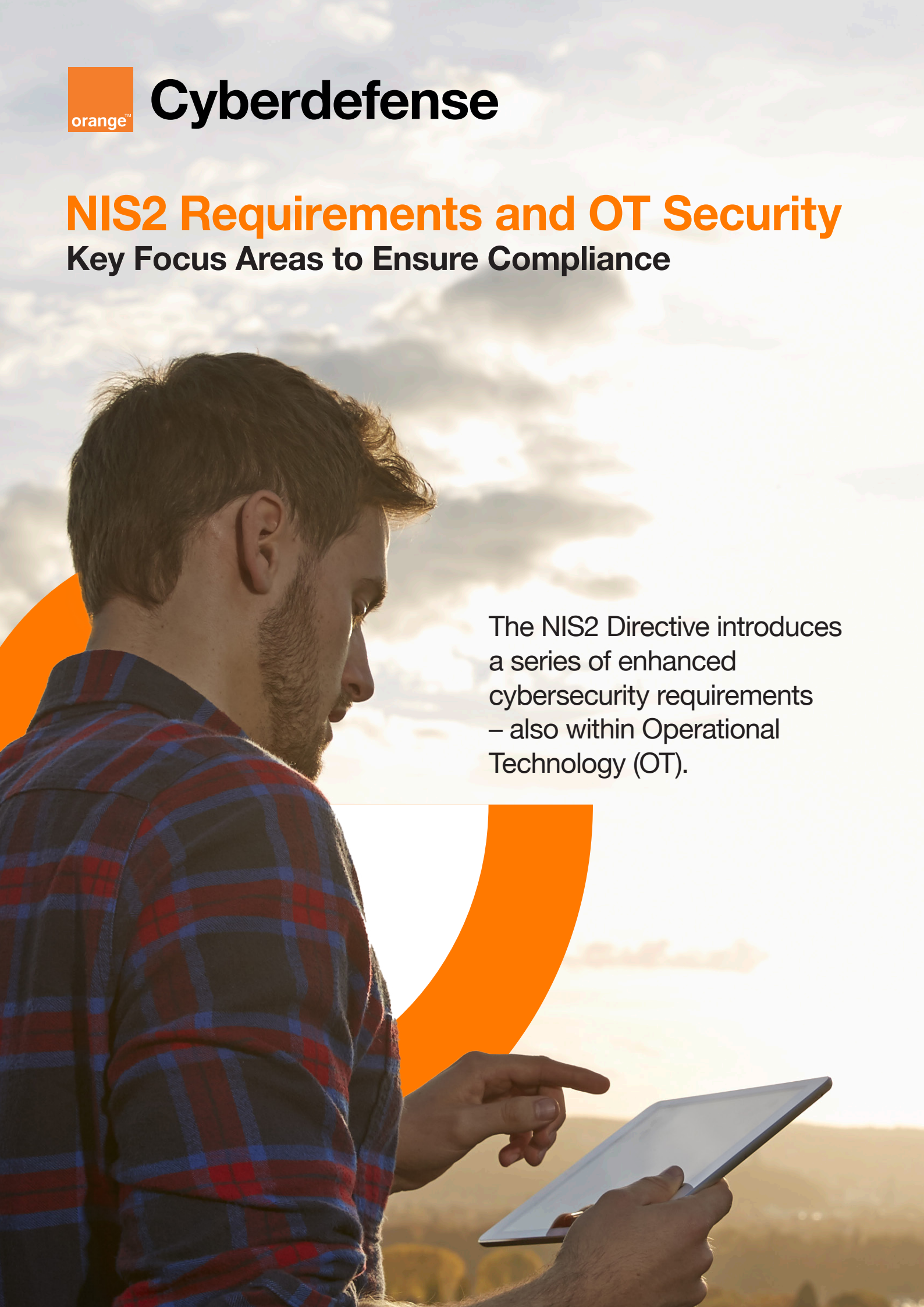
Cyberdefense

NIS2 Requirements and OT Security

Key Focus Areas to Ensure Compliance



The NIS2 Directive introduces a series of enhanced cybersecurity requirements – also within Operational Technology (OT).

1. Governance in OT environments
2. Risk management in OT environments
3. Supply chain-wide risk management
4. Incident response & crisis management in OT environments
5. Access control in the OT environment
6. Asset management in the OT environment
7. Monitoring & testing of the OT environment
8. Vulnerability management in the OT environment
9. Security by Design in the OT environment
10. Training and awareness for all OT personnel
11. Physical security of the OT environment

This overview outlines the key focus areas you should prioritize.

Each area is essential as it helps build the necessary resilience in your cyber defense and strengthens your ability to withstand cyberattacks — all while ensuring compliance with the requirements of the NIS2 directive.

1. Governance in OT Environments

Strengthen visibility, accountability, and control over security in your OT environment.

- Implement clear governance frameworks for cybersecurity in your OT environments, and ensure that management has a solid overview of your security practices and a clear understanding of who is responsible for OT security.
- Make sure your disaster recovery strategies and contingency plans for restoring OT systems are in place, so operations and production can continue even during a cyberattack.
- Develop and implement the following local OT governance documents:
  - OT Security Policy
  - Disaster Recovery Plan
  - Incident Response Plan
  - Business Continuity Plan
- Appoint a dedicated OT Security Officer (DSO) responsible for implementing the cybersecurity strategy and managing risks. Ensure the DSO has relevant experience, the required competencies, and the necessary resources to carry out the role effectively.
- Designate a local OT lead and strengthen the global OT security team responsible for developing and maintaining blueprints, policies, procedures, naming standards, etc. Ensure close collaboration with your production environment leaders and the IT department.
- Ensure that each site has a designated OT lead with full oversight of the entire production network, where cybersecurity is the top priority. This person must have a clear mandate and the resources required to secure the entire OT environment.

2. Risk Management in OT Environments

Integrate risk management into daily operations and make it part of your regular routines.

- Develop and implement a strategy that serves as a framework for managing risks in your OT environment.
- Plan and conduct ongoing risk assessments. It is essential to perform regular assessments of your OT systems to identify vulnerabilities and threats and to ensure continuous adaptation to emerging risks.

3. Risk Management Across the Entire Supply Chain

Ensure security throughout the value chain — including your suppliers.

- Continuously assess the security of your OT-related supply chains, and ensure that suppliers and third-party providers adhere to consistent and up-to-date OT cybersecurity requirements to reduce the risk of external vulnerabilities.
- Ensure appropriate measures are in place to manage risks from third-party vendors — especially those interacting with OT systems, such as equipment manufacturers and software providers.
- Require all suppliers and subcontractors to meet the same security standards applied internally, including implementing the technical and organizational measures needed to strengthen the security and resilience of their network and information systems.
- Conduct due diligence on your suppliers and subcontractors to verify that they have adequate security controls in place.
- Introduce cybersecurity requirements into all contracts with suppliers and subcontractors, making them contractually obligated to meet your standards.
- Require suppliers and subcontractors to notify you of any security incidents. They must report any events that could significantly impact the security of your OT systems and environment.

4. Incident Response and Crisis Management in OT Environments

Be ready to act — quickly and effectively.

- Develop a well-defined incident response plan specifically tailored to OT environments, enabling rapid detection, response, and recovery from cybersecurity incidents.
- Conduct a risk assessment based on the current threat landscape to identify potential incidents you may face, such as cyberattacks, natural disasters, physical sabotage, data breaches, and other types of security violations.
- Establish a cross-functional incident response team consisting of key personnel responsible for managing incidents and crises across the organization.
- Define clear procedures for handling any potential incident. These procedures should include steps for identification, response, containment, impact assessment, communication, and recovery.
- Establish clear protocols for both internal and external communication. These should clarify the roles of management and key personnel in reporting significant cybersecurity incidents affecting your OT systems to relevant authorities, employees, customers, and the media.
- Regularly test your incident response plan to identify weaknesses. Conduct frequent training sessions, simulations, and tabletop exercises — and update the plan as needed.
- Familiarize yourself thoroughly with the NIS2 directive — both the legal requirements and the specific obligations around reporting security incidents to relevant supervisory authorities, as well as leadership responsibilities related to governance, risk, and compliance. Being unprepared during a cyberattack could lead to enforcement actions and significant fines.

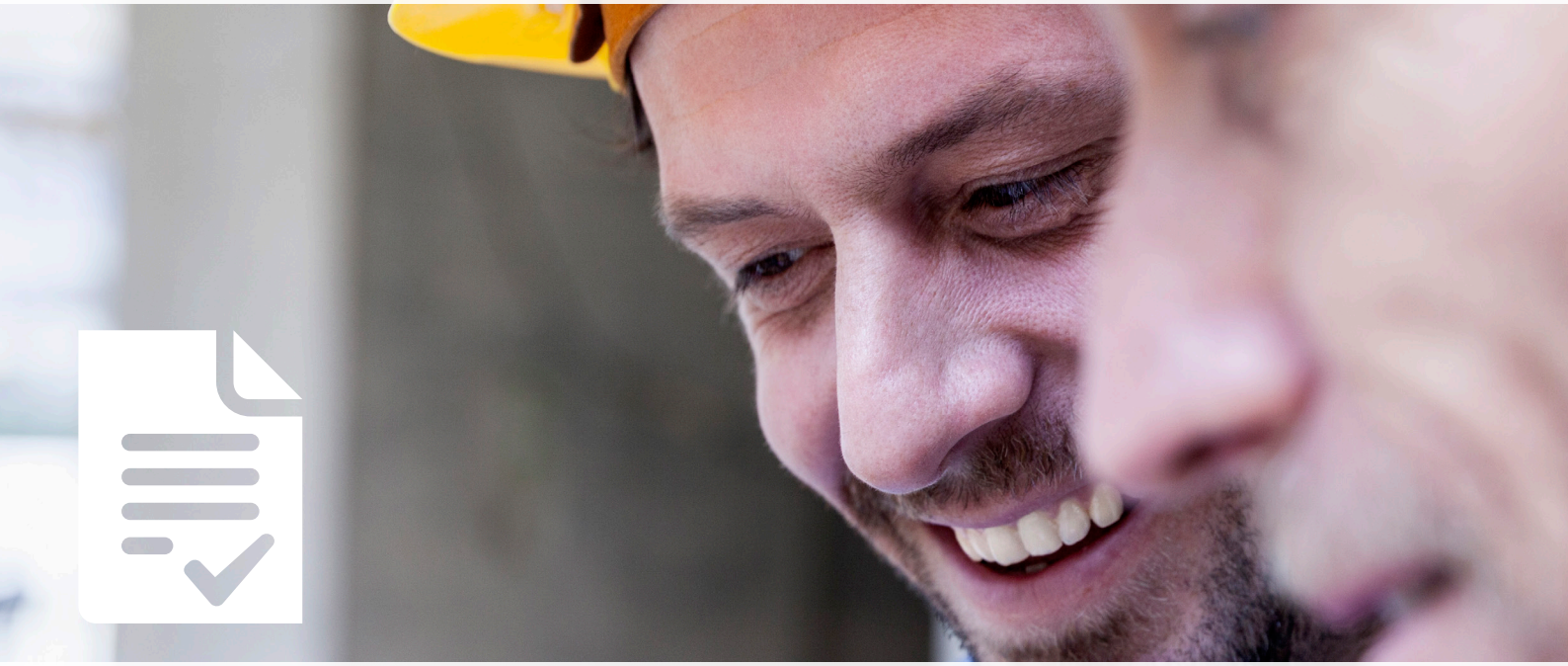
5. Access Control for the OT Environment

If everyone has access, nothing is secure. Gain control over your OT environment's security through access management and control – and keep the threats out.

- Implement strong identity and access management controls to restrict and monitor access to your OT systems.
- Ensure that access to OT infrastructure is granted exclusively to authorized personnel through appropriate access controls, making sure that only those who need access to your OT network and infrastructure actually have it.
- Ensure that there is only one remote access solution for all support and remote configuration.
- Make sure the solution supports monitored access with logging and session recording capabilities.
- The remote access solution should also be used for internal communication from the IT network to the OT systems.

6. Asset Management in the OT Environment

Gain visibility into your assets and ensure they are always optimally protected.



- Identify your critical OT assets, including Industrial Control Systems (ICS), SCADA systems, and other key OT components.
- Create and maintain an up-to-date inventory of OT networks and systems. Ensure that there is only one remote access solution for all support and remote configuration.
- Implement appropriate asset management practices to ensure proper handling and protection of assets.
- This may include regular vulnerability assessments, patch management, and configuration management of devices.

7. Monitoring and Testing the OT Environment

Make sure you can detect threats in time – before they cause damage.

- Continuously monitor your OT systems and keep a close watch for anomalies, threats, and performance issues. Early detection of irregularities is critical for effectively responding to cyber threats.
- Conduct regular testing and audits of OT security to ensure systems are robust and resilient against attacks.
- Use passive scanning as the standard method for monitoring your OT systems. Supplement with active detection – especially on Windows-based OT devices – if feasible.

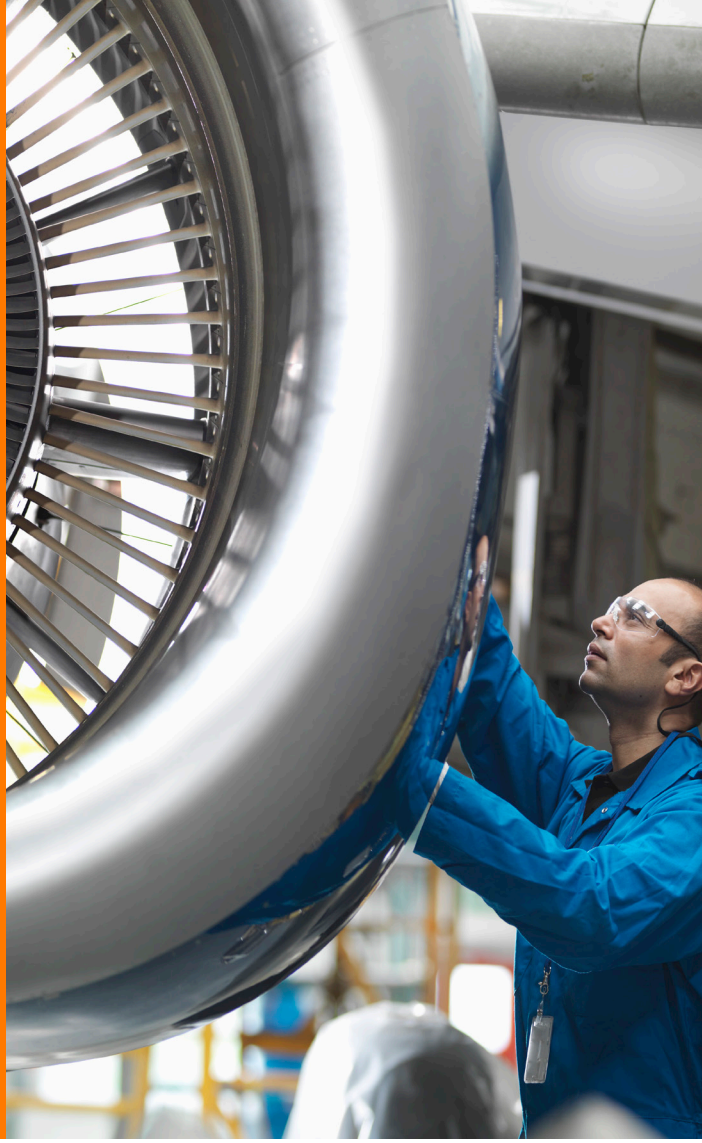
Pay particular attention to monitoring the following areas:

- Malicious or harmful code – at a minimum on your most exposed assets.
- Unauthorized connections and devices – your monitoring tool must be capable of viewing and analyzing all network traffic.
- Network traffic, infrastructure activity, and infrastructure changes – logging is essential for detecting potential security breaches.
- Unauthorized software.

8. Vulnerability Management in the OT Environment

Address weaknesses before they are exploited.

- Implement a process for managing vulnerabilities in your OT networks and systems.
- Perform regular updates and patching during scheduled maintenance windows. It is essential to prioritize patch management and allocate the necessary time for open service windows – even when it may be challenging.
- If patching is not possible, conduct a risk assessment and implement appropriate mitigation measures and other necessary actions.



9. Security by Design in the OT Environment

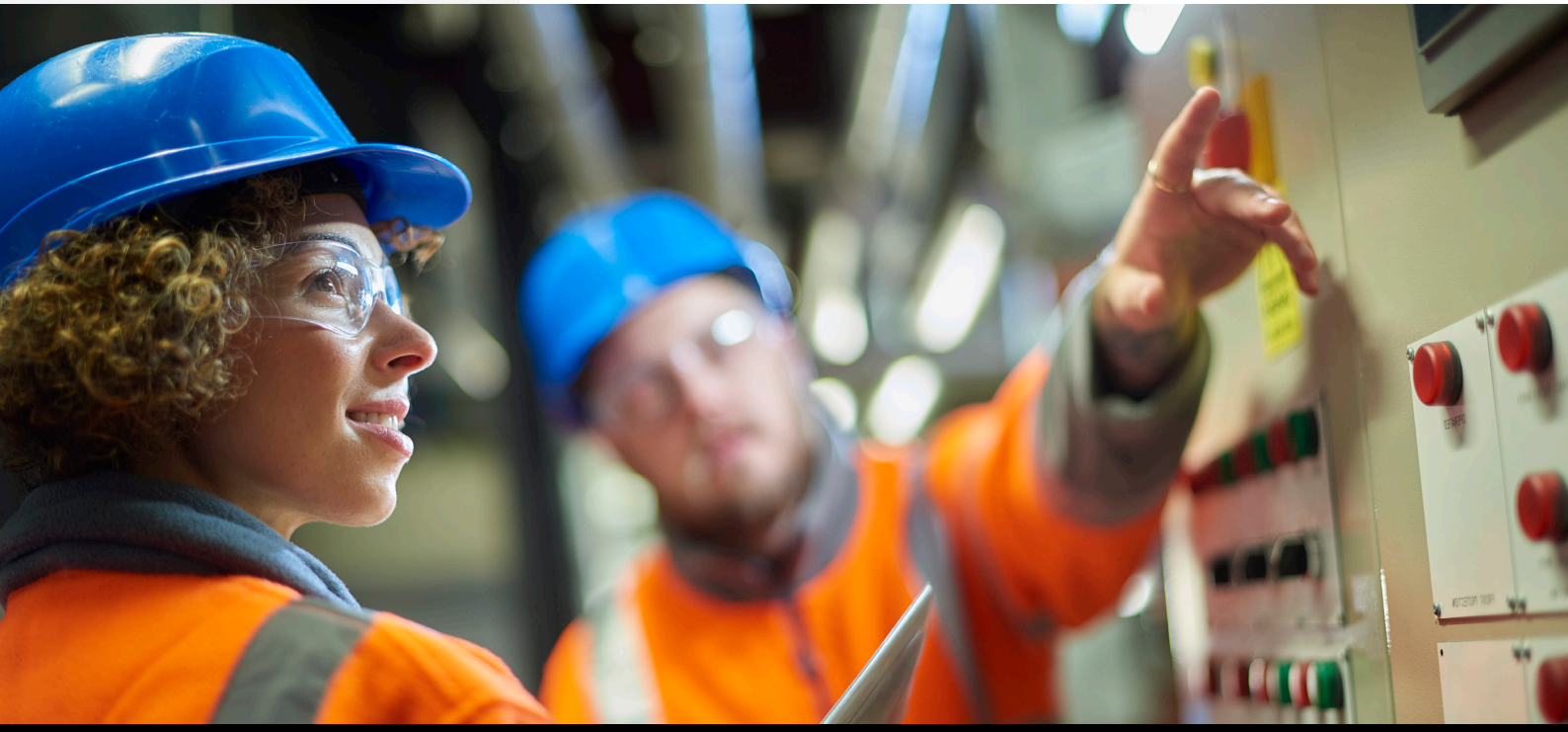
Always build security into your OT systems from the start.

- Implement Security by Design in all new OT systems and consistently follow the principles whenever new OT systems are deployed.
- Establish processes to ensure the proper configuration of your OT networks and systems, and verify that configuration changes are handled correctly.
- Introduce appropriate security measures such as access control, secure network architectures, and secure device configurations for both devices and software.
- Implement appropriate segmentation and isolation of your OT networks and infrastructure to prevent unauthorized access.
- Protect your OT systems from network-based attacks such as DDoS by deploying suitable security solutions.
- Segment and isolate OT networks and infrastructure to prevent unauthorized access.
- Implement malware protection such as antivirus and intrusion detection systems to safeguard your OT systems from network-based threats and malware attacks.
- Establish robust backup and recovery procedures to ensure your OT networks and systems are resilient to attacks and disruptions.
- Perform regular, automated backups with short intervals. OT backups should be stored on the OT network, and offline backups should be regularly performed for all devices.
- Use tools for automatic backup of PLC projects with version control and comparison of online and offline versions.
- Monitor and document all backup procedures, verify existing backups, and establish regular routines for periodic checks.

10. Training and Awareness for All OT Personnel

Security starts with knowledge.

- Implement awareness programs for all employees working with Operational Technology in your OT environments.
- Ensure that all employees responsible for your OT systems receive regular awareness training and are capable of recognizing and responding effectively and correctly to threats.



11. Physical Security of the OT Environment

Protect the physical environment – not just the digital one.

- Physical security is crucial, so you should ensure strong access control, such as biometric authentication, restricted access to sensitive areas, and security personnel with appropriate clearances. These controls can prevent unauthorized individuals from gaining physical access to your critical OT infrastructure.
- Strengthen perimeter security by securing your outer areas with fences, barriers, and surveillance cameras to prevent unauthorized access to your critical OT infrastructure.
- Enhance monitoring, control, and patrolling with tools such as video cameras, intrusion detection, and security guards, which can help you detect and respond quickly to deviations, illegal intrusions, and security incidents.

Contact

Do you need help assessing your maturity in relation to the security of your OT environments – compared to NIS2 requirements – and how to ensure you reach your goals to become compliant?

Contact us for advice and support in implementing the necessary measures.

info@dk.orangecyberdefense.com
+45 70 20 03 32

orange™ Cyberdefense