Radiflow

NIS2 is Coming to OT
Are you Ready?

December 2023

Radiflow

Radiflow

Table of Contents

Executive Summary

The Network and Information Systems Directive-2 (NIS2) is the latest legislation that provides guidance and legal measures to boost cybersecurity and resilience within organizations of the European Union. The new Directive expands the scope of its predecessor (NISD) to include EU-based organizations involved in a wide assortment of critical products and services, as well as others doing business in the EU. Compliance requirements have been fortified and penalties for non-compliance have been made much more severe.

With NIS2 going into effect in October 2024, OT organizations have less than a year to get their cybersecurity house in order, obtaining top management buy-in, allocating budgets and resources, instituting processes and programs, and acquiring mandated cyber solutions and services. There isn't a moment to waste.

Impacted OT organizations need to start getting ready NOW!

Compliance with NIS2's rigorous requirements on Cybersecurity and Risk Management[1], and stringent Incident Reporting Obligations[2] require a significant investment. The alternative can lead to:

- Non-monetary remedies (compliance orders, binding instructions, security audit implementation orders, and threat notification orders to customers)
- Significant administrative fines in the millions of euros
- Criminal sanctions (making compliance violations public. making public statements that identify the natural and legal persons responsible for a violation. and banning individuals from holding management positions)

Non-compliance is not an option!

[1] Article 21, https://www.nis-2-directive.com/NIS_2_Directive_Article_21.html
[2] Article 23, https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html

Radiflow highly recommends that NIS2-impacted OT organizations immediately institute programs to improve their capabilities in the areas of:

- Asset Inventory
- Threat Detection
- Network Segmentation
- Risk Assessments
- Continuous Risk Management Process
- Incident Response and Reporting
- Management, Engineer, & Employee Cyber Awareness and Technical Training

Radiflow offers leading compliance solutions and services in all of these areas. We encourage OT companies to reach out to us to find out how to bolster their current operational cybersecurity, risk management programs, IR capabilities, and cyber awareness pronto!

How We Got Here

The EU has noticed the growing threat of cyber incidents to critical infrastructure and the well-being of its citizens. In 2006, it created *The European Programme for Critical Infrastructure Protection* (EPCIP) to establish a framework for improving the protection of critical infrastructure across EU States in all relevant sectors of economic activity.

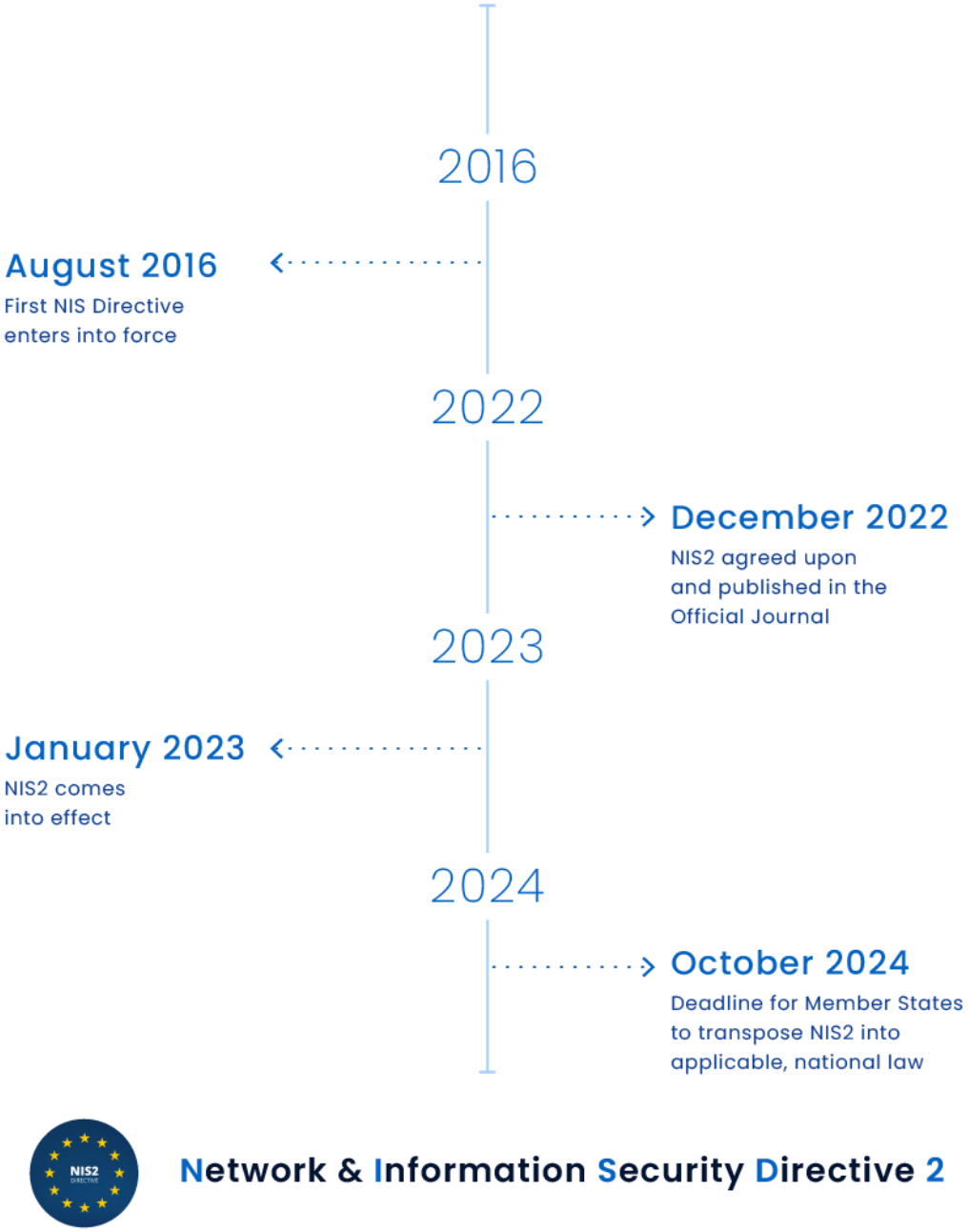
In 2016, the EPCIP attempted to enhance the resilience of critical infrastructure and essential services against cyber threats by publishing the original NIS Directive (NISD). However, almost right away, it became apparent that this first attempt was ill-suited to cope with the growing threat landscape and it was too weak – it granted too much compliance autonomy to member states. While NISD addressed sectors like healthcare and energy, many industries remained outside of its scope. Enforcement was inadequate and not uniformly applied across countries and industries. The European Union Agency for Cybersecurity (ENISA) came to the conclusion that, in the wake of the expanding threat landscape and proliferation of technology, e.g., IoT devices, Industry 4.0, NISD could not provide adequate protection for critical products and services.

Going back to the drawing board, NIS2, a significant evolutionary descendant of the original NISD, was created. Like its predecessor, NIS2's goal is to enhance the resilience of critical infrastructure and essential services against cybersecurity threats, but, this time, with a broader, stricter, and more uniform approach.

NIS2 builds upon NISD but introduces several significant changes. NIS2 modernizes the existing legal framework to keep pace with increased digitization and the rapidly evolving cybersecurity threat landscape. Expanding the scope of the cybersecurity rules to many new sectors and entities, it extends governance to a much wider array of public and private entities.

When it goes into effect in October 2024(!), NIS2's jurisdiction will include a great many EU-based companies as well as others doing business in the EU. Businesses identified as operators of essential and important services (described below) will be required to take appropriate security measures and notify relevant national authorities – mandated national Computer Security Incident Response Teams (CSIRTs) – of serious incidents.

While both IT and OT organizations come under NIS2 jurisdiction, the main impetus is to secure critical infrastructure and services. Thus, OT operations are the major concern. The directive aims to mitigate risks and ensure that operators of essential services take steps secure their networks, but these steps may be inadequate for OT networks and systems, especially where the impact of a cyberattack could be calamitous. Compliance with NIS2 does not guarantee protection against cyberattacks. Therefore, additional cybersecurity measures beyond NIS2, commensurate with risk and potential harm to critical services, are in order.



Who is Covered?

NIS2 governance extends broadly across industries and companies. NIS2 defines two categories for entities that are in its scope of governance: *essential* and *important*.

"The sabotage last autumn of the Nord Stream pipelines underlined how essential sectors such as energy, digital infrastructure, transport, and space depend on resilient critical infrastructure and how interlinked the external and internal dimensions of our security are. Our new rules on critical entities resilience we are now rolling out are providing a strong framework to build up our collective protection against all threats."

Margaritis Schinas
Vice President for Promoting Our European Way of Life, July 2023

Essential Entities

Operators of Essential Services (OES) are companies that provide services considered of High Criticality and are essential to the functioning of society and the economy (as listed in the following table). OES are required to comply with the NIS2 Directive regardless of their size. (More on size later.)

Table 1: Sectors of High Criticality[3]

Sectors	Sub-Sectors and Descriptions
Energy	Electricity, Heating and Cooling, Oil, Gas, Hydrogen
Transport	Air, Rail, Water, Road
Banking	Credit institutions
Financial Market Infrastructures	Operators of trading venues, Central counterparties (CCPs)
Health	Healthcare providers, Laboratories, Research and Development of medicinal products, Manufacturers of basic pharmaceutical products and preparations, Manufacturers of medical devices considered to be critical during a public health emergency
Drinking Water	Suppliers and distributors of water intended for human consumption
Waste Water	Collectors, disposers, and treaters of urban, domestic, or industrial waste water
Digital Infrastructure	Internet exchange point providers, DNS service providers, TLD name registries, Cloud computing service providers, Data center service providers, Content delivery network providers, Trust service providers, Providers of public electronic communications networks, Providers of publicly available electronic communication services
Information and Communications Technology (ICT) Service Management (Business-to-Business)	Managed service providers (MSPs), Managed security service providers (MSSPs)
Public Administration	Public administration entities of central governments and at the regional level
Space	Operators of ground-based infrastructure owned, managed, and operated by member states or by private parties

[3] Details can be found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555, Page 64, ANNEX I SECTORS OF HIGH CRITICALITY

Important Entities

Important entities are medium-sized enterprises that operate in the sectors of High Criticality (per Table 1 above) OR large or medium-sized enterprises in the sectors listed in the following table.

Table 2: Other Critical Sectors[4]

Sectors	Sub-Sectors and Descriptions
Postal and Courier Services	Postal service providers
Waste Management	Undertakings carrying out waste management excluding those for whom waste management is not their principal economic activity
Manufacture, Production and Distribution of Chemicals	Undertakings carrying out the manufacture of substances and the distribution of substances or mixtures, and undertakings carrying out the production of articles from substances or mixtures
Production, Processing and Distribution of Food	Food businesses which are engaged in wholesale distribution and industrial production and processing
Manufacturing	Manufacture of medical devices and in vitro diagnostic medical devices, Manufacture of computer, electronic and optical products, Manufacture of electrical equipment, Manufacture of machinery and equipment, Manufacture of motor vehicles, trailers and semi-trailers, Manufacture of other transport equipment
Digital Providers	Providers of online marketplaces, Providers of online search engines, Providers of social networking services platforms
Research	Research organizations

[4] Details can be found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555, Page 69, ANNEX II OTHER CRITICAL SECTORS

Size Matters

NIS2 defines large enterprises as: headcount over 250 or more than €50 million in annual revenues. Medium enterprises have a headcount of 50-250 or €10-€50 million in annual revenues. However, this does not mean that smaller organizations are necessarily excluded. Member States may extend NIS2 requirements to small enterprises if they fulfill specific criteria that constitute a "key role for society, the economy, or for certain types of services."

Impact on OT Organizations

NIS2 will significantly impact OT organizations in terms of costs, time, processes, and management:

- Compliance Costs. Organizations undoubtedly will incur significant expenses to meet NIS2 requirements, including additional personnel, cyber solutions and/or services, and more. The Directive suggests cybersecurity training not only of management but also employees, so considerable outlay will have to go into formal, ongoing training programs.
- Accountability. The mandated high level of accountability will require that organizations ensure the security of their critical systems. This may require significant changes in operations and management structure. New functions will include risk assessments along with risk treatment plans. Management will be held responsible for such functions and adoption of requisite cybersecurity measures. NIS2 includes new measures to hold top management personally liable for gross negligence in the event of a security incident.
- Reporting. Within 24 hours of detecting an incident, an early warning must be communicated along with preliminary information regarding the kind of incident to the national CSIRT. By 72 hours, a full notification report must be communicated, detailing an assessment of the incident, its severity and impact, and indicators of compromise. By one month later, a final report must be communicated.
- Penalties. Failure to meet NIS2 requirements may result in substantial fines. Essential entities may be subject to non-compliance fines of at least €10M or 2% of the global annual revenue, whichever is higher. Important entities are subject to supervision only in cases where the authorities are in receipt of evidence of non-compliance. For these, non-compliance fines are somewhat decreased – up to €7M or 1.4% of global annual revenue, whichever is higher.

What do we get for all this bother, expense, and liability? **The goal of NIS2 is the improvement of the security posture of critical organizations.** Ideally, compliance will lead to better protection against cyber threats and reduce the risk of costly breaches.

How to Prepare

With October 2024 hanging over them like the Sword of Damocles, OT organizations should familiarize themselves with these recommendations to get ready for NIS2:

Asset Inventory

To get started, you need to know all about your assets. What are they? Who are their vendors? Where are they? What are they doing? What are their vulnerabilities? With what other assets and systems do they communicate?

Threat Detection

A cyber solution that observes and learns proper network, asset, and communication behavior can automatically spot anomalies that might indicate security threats. Every site needs such a solution. If your company operates multiple sites, then central management of the security of all the sites will make the process much easier.

Network Segmentation

A significant OT best practice, segmentation makes it easier to detect and isolate cyberattacks. It prevents unauthorized access to ICS networks from the IT side while, *within* ICS networks, it enables isolation of affected segments, limiting potential damage and downtime.

Risk Assessment

Find and measure gaps between current security posture and the requirements of accepted cybersecurity standards and best practices. That requires a risk assessment for each site as well as overall.

Risk Management Process

While vital to establishing a security baseline, the risk assessment is not a one-off matter. **To maintain compliance, companies must adopt a long-term risk management program with:**

- Periodic risk assessments that take into considering new Threats, Tactics, and Procedures (TTPs) in the ever-changing cyber threat landscape as well as new vulnerabilities due to changes in assets, networks, and business processes
- Indications of where to spend the next Euro of the security budget to minimize risk
- Measurements of progress toward security goals such as accepted standards like ISA/IEC 62443, NIST CSF, ISO 27001, and industry best practices

Incident Response and Reporting

Given NIS2's aggressive response and reporting requirements, OT operators need to know how to react BEFORE an incident occurs: How to collect information on an alert, how to triage incidents, how to report real incidents, and to whom. The threat-detection solution described above should be able to help operations and security teams comply.

Cybersecurity Training

NIS2 requires organizations to provide training to their management and employees to deepen their knowledge in cybersecurity. Measures such as awareness campaigns, training programs, and simulations are to be included in the continuous training program, with courses appropriate to the level in the organization, type of work, and exposure to security threats.

How Radiflow Helps

Cybersecurity and Risk Management Solutions

Some organizations prefer to obtain and deploy threat detection and/or risk management solutions and to train their security people to operate them. Radiflow provides such solutions to OT organizations large and small, across numerous industries.

iSID Threat Detection

Radiflow offers the iSID solution for risk-driven, continuous OT cyber threat detection and monitoring. iSID unobtrusively learns the topology and operational behavior of the ICS network and all of its assets. It automatically detects anomalies and determines if they are indicators of compromise (IOCs) whereupon it generates alerts enriched with a wealth of valuable cybersecurity information.

In addition to threat detection, iSID offers capabilities pertaining to other types of network activity:

- Modeling and visibility of OT and IT devices
- Protocols and sessions
- Policy monitoring
- Validation of operational parameters
- Rules-based maintenance management
- Networked device management

iSID can be integrated with 3rd-party and enterprise business systems, sharing information for a variety of security, compliance, and business purposes.

iCEN Centralized Management

iCEN provides central control of multiple iSID instances, simplifying and streamlining security monitoring and management. It displays a status snapshot of all iSID instances across the organization including their total risk and activity status with easy drill-down and remote connection to each iSID instance.

iCEN displays aggregated data from the iSIDs including:

- Assets organized by type
- Alerts organized by severity
- Network protocols in use

iCEN also enables single-click central provisioning of software updates, threat intelligence, and user-defined rules to multiple iSIDs.

CIARA Risk Management

Radiflow CIARA is a complete, continuous, risk-management solution for OT organizations. Based on leading industry standards such as ISA/IEC 62443, the NIST Cybersecurity Framework (CSF), and ISO 27001, CIARA empowers CISOs and other security stakeholders to optimize their OT security expenditure while ensuring the effectiveness of threat-mitigation controls with regard to standards and industry best practices as promoted by NIS2.

CIARA uses data garnered from iSID and/or other 3rd–party solutions to automatically assess risk. It performs asset impact-mapping based on a hazard approach and calculates the per-zone likelihood of attacks and the impact of those attacks on business processes. It also determines the effectiveness of corresponding risk-mitigation measures (both installed and proposed).

With CIARA, OT organizations understand the key indicators for risk, threat, and control levels. They obtain a comprehensive hardening plan (fully ISA/IEC 62443-compliant), prioritized by each mitigation control's contribution to achieving risk management goals.

Cybersecurity and Compliance Services

Not all OT organizations are ready or able to take on the full gamut of threat detection, reporting, and risk management. For these, Radiflow offers a complete menu of cybersecurity and NIS2 compliance services backed by extensive global OT experience and our own solutions as described above.

Managed Detection and Response

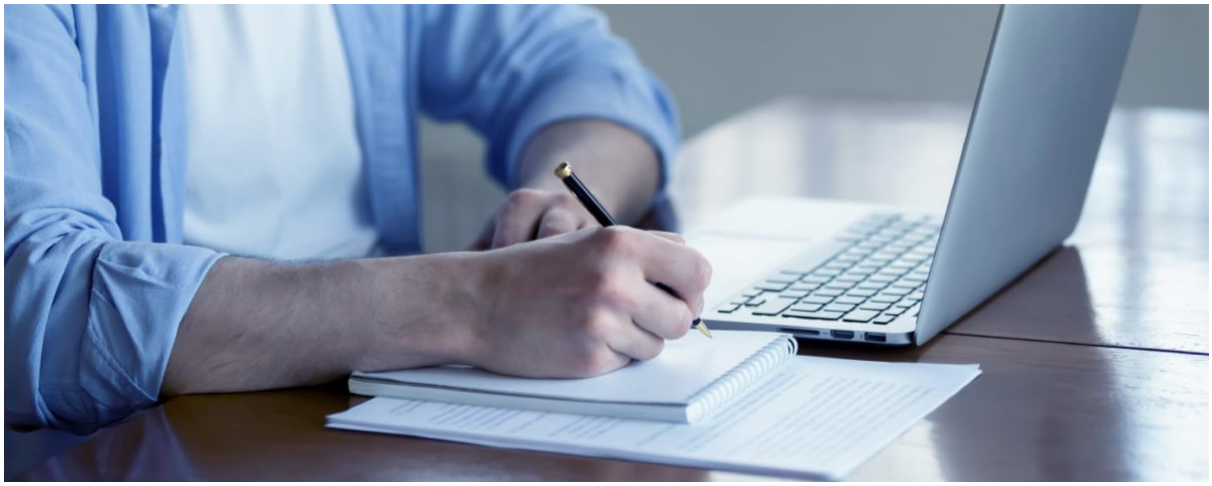
Radiflow MDR Services offload the cybersecurity burden while enabling OT organizations to establish and maintain compliance with NIS2. Customers may choose from the menu of MDR NIS2 activities to supplement their in-house capabilities. **Using iSID as a source, Radiflow MDR Services perform:**

- Comprehensive monitoring of network traffic, identification of potential threats
- Asset Inventory Management with regular reports on all assets, communications, and operations
- OT vulnerability discovery and prioritization
- Threat Intelligence
- Logs and security reports of network activity and incidents
- Detection and alerting on suspicious activity such as unauthorized access attempts and data exfiltration
- Incident response planning
- Rapid incident response procedures through effective playbooks
- Reporting of incidents to CSIRTs per NIS2 requirements

Risk Management as a Service

Managing cyber risk and executing effective risk assessments requires a high level of security, industry, and engineering expertise. Many companies, especially considering the impending requirements of NIS2, prefer to outsource this function to experts.

Radiflow combines its highly scalable OT security technologies with global expertise to deliver Risk Management Services (RMS) to Critical National Infrastructure (CNI) and Industrial Control System (ICS) operators in accordance with NIS2 requirements. Employing industry-leading CIARA, Radiflow Risk Management Services help operators comply with the risk assessment and continuous risk management requirements of NIS2.



Cyber Awareness Training

Radiflow offers an assortment of general and technical cyber training designed for senior management, CISOs, technical staff, and employees who need to be aware of the rudiments of cyber. Creation of a custom training program with flexible on-site and/or remote meetings, supplemented with hands-on exercises and simulations will boost cyber knowledge across business and industrial operations, and assure compliance with the training requirements of NIS2.

About Radiflow

Radiflow is a leading, global provider of OT security solutions and services for critical infrastructure and industrial automation. With broad and deep industrial cyber experience, we enable operators to continuously safeguard their operations while they manage risk, optimize their security budget, and comply with regulations and industry best practices.

Radiflow OT security solutions and services are deployed at more than 8000 sites worldwide, supported from offices and partners in Europe, APAC, and North America.

Radiflow is part of the Sabanci Group, an international conglomerate involved in financial services, energy, cement, retail, and other critical infrastructure and industrial sectors.

Visit us at www.radiflow.com