Radiflow

eBook

Your Guide to NIS2 Compliance

for Operators of Critical Infrastructure
and Industrial Automation and Control Systems

Radiflow

A New Age in OT Security

Ready or not, NIS2 is coming in 2024.
Thousands of OT companies will be compelled to comply.
If your company is one of them, there is no time to lose – **get started now!**

2016

August 2016
First NIS Directive enters into force

2022

December 2022
NIS2 agreed upon and published in the Official Journal

2023

January 2023
NIS2 comes into effect

2024

October 2024
Deadline for Member States to transpose NIS2 into applicable, national law

Network & Information Security Directive 2

Radiflow

What you need to know about NIS2

Radiflow

About the Network Information Security Directive 2 (NIS2)

NIS2 is EU-wide legislation that institutes obligatory measures to boost levels of cybersecurity and resilience.

By October 2024, National Computer Security Incident Response Teams (CSIRTs) in all member countries must be established to oversee compliance.

ARTICLE 11:

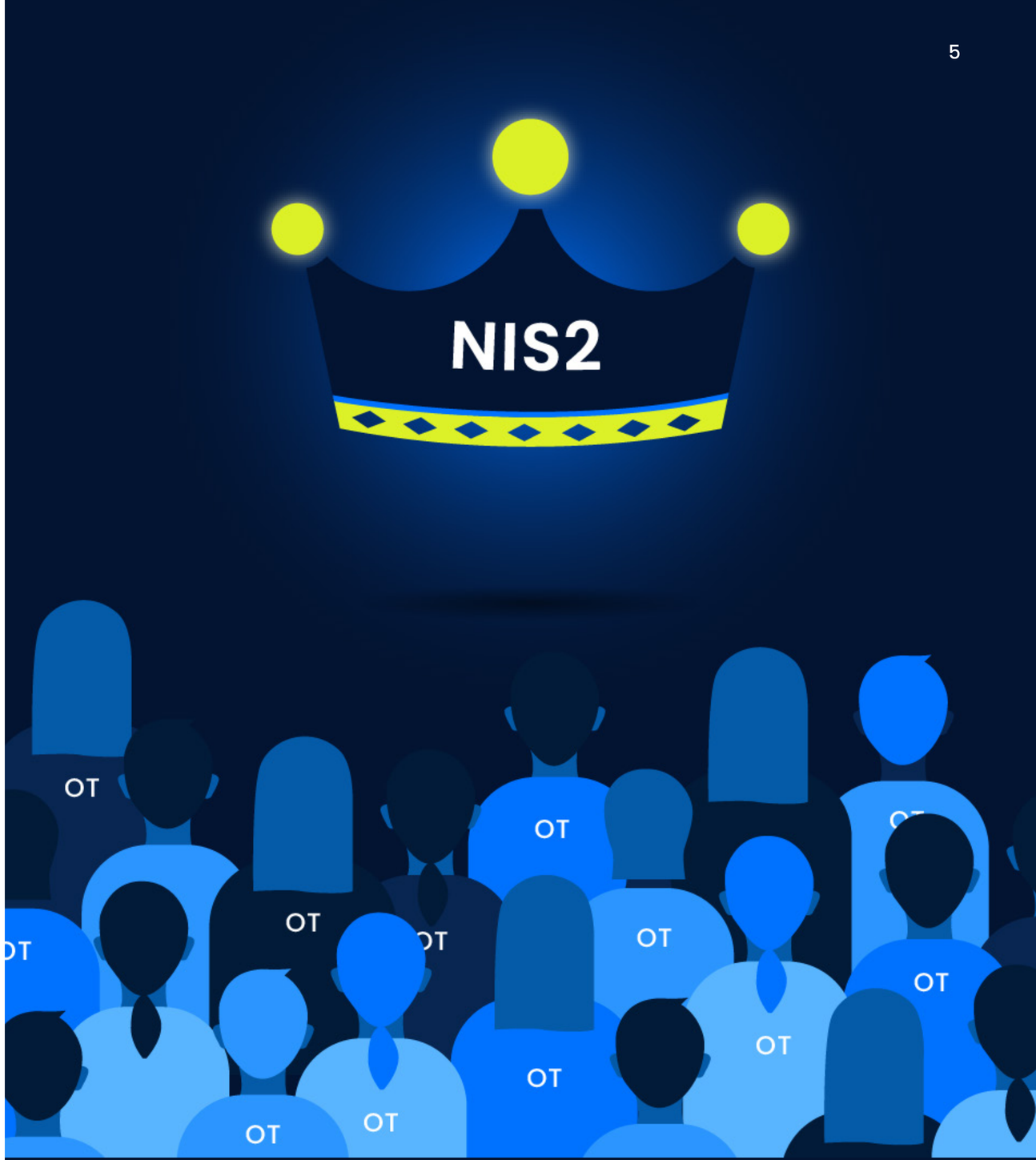
> CSIRTs may carry out proactive, non-intrusive scanning of publicly accessible network and information systems of essential and important entities… to detect vulnerable or insecurely configured network and information systems and inform the entities concerned

Radiflow

Who is Subject to NIS2?

Any organization operating or carrying out activities within the EU that provides an essential service to consumers:

“must take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems, and to prevent or minimise the impact of incidents on recipients of their services and on other services.”



Radiflow

Sectors Subject to NIS2

"HIGH CRITICALITY" SECTORS

- ASSET INVENTORY
- ENERGY
- TRANSPORT
- DRINKING WATER
- DIGITAL INFRASTRUCTURES
- WASTE WATER
- SPACE
- PUBLIC ADMIN
- ICT SERVICE MANAGEMENT(B2B)
- BANKING
- FINANCIAL MARKET INFRASTRUCTURE

"OTHER CRITICAL" SECTORS

- DIGITAL PROVIDERS
- RESEARCH
- FOOD PRODUCTION & DISTRIBUTION
- POSTAL & COURIER SERVICE
- WASTE MANAGEMENT
- MANUFACTURING
- MANUFACTURE
- DOMAIN REG SERVICES

Radiflow

Essential or Important?

Subject entities may be designated as “Essential” or ‘Important” depending on criticality, sector, and size.

LARGE ENTITIES

>= 250 employees or more than $50M in annual revenues

MEDIUM ENTITIES

50-249 employees or more than $10M in annual revenues

SECTOR	SIZE OF ENTITY	DESIGNATION
High Criticality	Large	Essential
High Criticality	Medium	Important
Other Critical	Large	Important
Other Critical	Medium	Important

There are a few exceptions that designate Medium-size entities in certain Sectors as “**Essential**”. Small entities are exempt except in a few cases.

Radiflow

Escalating Penalties for Non-Compliance

- Those responsible for discharging managerial responsibilities at CEO or legal representative level can be temporarily prohibited from exercising managerial functions (applicable to essential entities only, not important entities)
- Essential entities certification or authorization concerning the service can be suspended if deadline for taking action is not met
- Imposition of potentially stiff administrative fines
- Order to make public aspects of non-compliance
- Designation of a monitoring officer over a determined period of time to oversee the compliance
- Order to implement the recommendations provided as a result of a security audit within a reasonable deadline
- Order to inform the natural or legal persons for whom services or activities are provided which are potentially affected by a significant cyber threat
- Order to bring risk management measures or reporting obligations in compliance within a specified period
- Order to cease conduct that is non-compliant
- Binding instructions
- Warnings for non-compliance

Radiflow

Supervision

ESSENTIAL ENTITIES

Must comply with supervision requirements from the introduction of NIS2

IMPORTANT ENTITIES

Action will be taken only if authorities receive evidence of non-compliance

Radiflow

Administrative Fines for Non-Compliance

ESSENTIAL ENTITIES

A maximum of **€10M or up to 2%** of total worldwide annual turnover, whichever is higher

IMPORTANT ENTITIES

A maximum of **€7M or up to 1.4%** of total worldwide annual turnover, whichever is higher

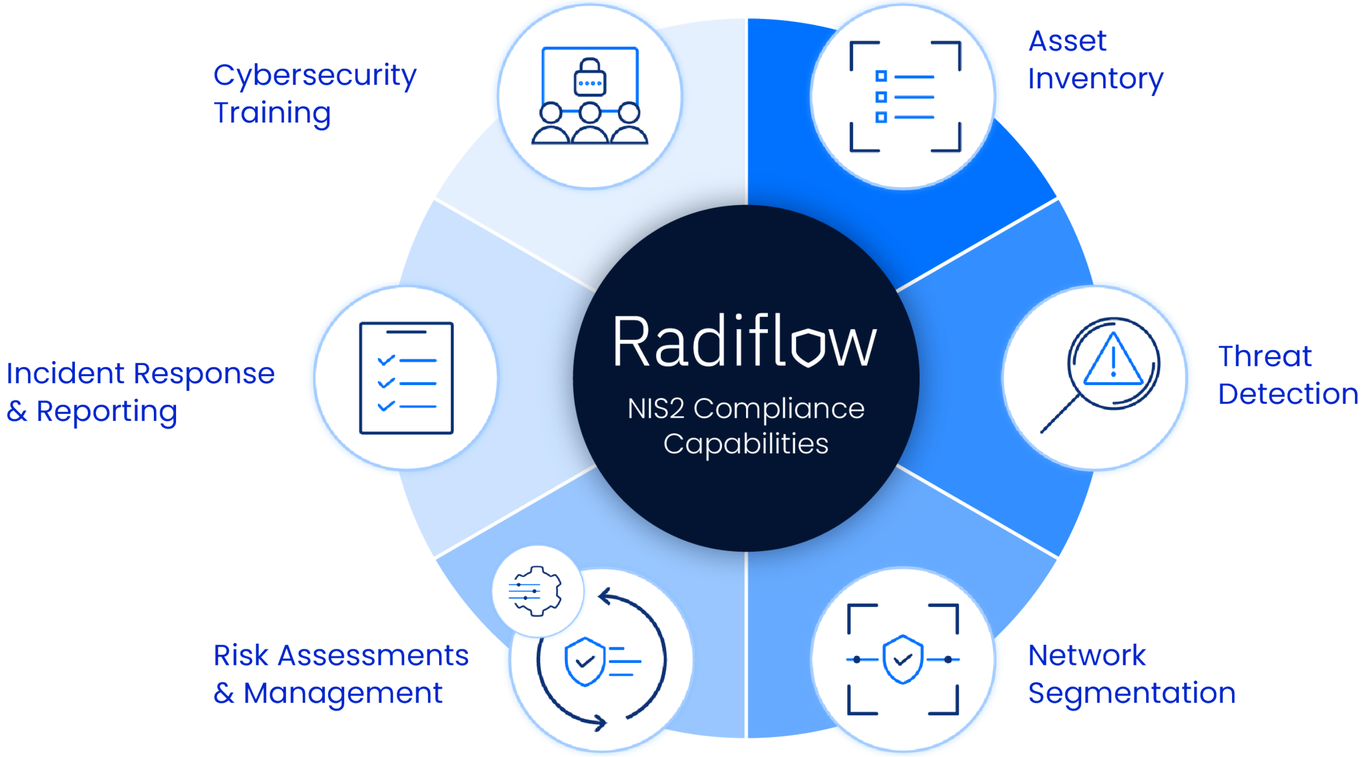
Radiflow

How Radiflow helps OT organizations comply with NIS2

Radiflow

How Radiflow Helps You Comply with NIS2

The relevant NIS2 requirements can be found in Chapter IV, Article 21, “Cybersecurity risk-management measures” and Article 23, “Reporting obligations”. Radiflow helps you comply with all of these.



Radiflow

How Radiflow Helps – Cybersecurity

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? Radiflow automatically finds all assets and constructs a complete asset inventory, including zones and conduits and communications.

NETWORK SEGMENTATION

Segmentation makes it easier to detect and isolate cyberattacks. It prevents unauthorized access to ICS networks from the IT side or from the Internet while, within ICS networks, it enables isolation of affected segments, limiting potential damage and downtime. Radiflow advises on best segmentation practices and can implement an effective solution.

THREAT DETECTION

The Radiflow threat detection solution learns proper network, asset, and communication behavior and spots anomalies that might indicate security threats. Our central management solution simplifies security management across multiple sites.

INCIDENT RESPONSE AND REPORTING

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 Radiflow threat-detection solution helps operations and security teams comply by supplying forensics and effective playbooks.

CYBERSECURITY TRAINING

Organizations must provide appropriate cybersecurity training to management and employees, including awareness campaigns and simulations. Radiflow helps set up and conduct compliant training plans.

Radiflow

How Radiflow Helps – Risk Management

RISK ASSESSMENT

To get started, the Radiflow risk management solution promptly measures the gaps between current security posture and accepted cybersecurity standards and best practices. It conducts a risk assessment for each site and across the entire organization.

RISK MANAGEMENT PROCESS

An annual risk assessment is not sufficient for NIS2 compliance. Companies must adopt a long-term risk management program with:

- Periodic risk assessments that take into consideration 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 related to accepted standards like ISA/IEC 62443, NIST CSF, ISO 27001, and industry best practices

Radiflow's data-driven risk management solution delivers long-term compliance with NIS2.

Radiflow

Radiflow for NIS2 Compliance

1. Continuous OT threat monitoring
2. Asset visibility correlated with vulnerability
3. Incident handling
4. Prompt cyber-incident reporting
5. Regular, data-driven risk assessments
6. Evaluation of the effectiveness of security measures – proposed and actual
7. Integration with 3rd party secure remote access, CMDB, SOC, other solutions
8. Advice on segmentation
9. Managed services
10. Cyber-awareness training

Radiflow

Contact Us for NIS2 Preparation and Ongoing Compliance Solutions and Services

- Radiflow solutions and services currently safeguard more than 8000 sites globally including many in Europe
- Our solutions deliver the cybersecurity and risk management capabilities that help you comply with NIS2 and are the basis for our services
- Our highly experienced experts discover the gaps in your NIS2 compliance and advise you on how to get ready

www.radiflow.com