DRAGOS®
SAFEGUARDING CIVILIZATION

European Union Directive on Security of Network and Information Systems (NIS2)

Dragos Can Help European Union Organisations Prepare to Meet and Exceed New Requirements

The mission of Dragos is to safeguard civilization by providing the platform, services, and intelligence to protect operational technology and critical infrastructure. Our technology supports numerous standards and regulations, empowering our customers to adopt best practices and exceed compliance requirements.

The NIS2 Directive is a modernised framework based on the EU Network and Information Security Directive, the first piece of EU-wide legislation on cybersecurity. The Directive provides legal measures to boost the overall level of cybersecurity in the EU by focusing on preparedness and cooperation within critical sectors.

Under the Directive, operators of essential services must take appropriate security measures, notify relevant national authorities of serious incidents, and mitigate security risks in their supply chains by assessing the product quality and cybersecurity practices of suppliers and service providers. Management bodies are required to take an active role in supervision and implementation, bolstering the importance of the CISO as an educator and best practices guide for senior executives. Organisations that do not comply risk fines; management liability; temporary bans against managers; and more.

Dragos offers monitoring technology, threat intelligence, incident response, and professional services to help your organisation prepare to meet and exceed the requirements of the NIS2 Directive. We partner directly with CISOs and other leaders in your company to help you develop a vision, create a detailed action plan, and achieve consistent and documented results.

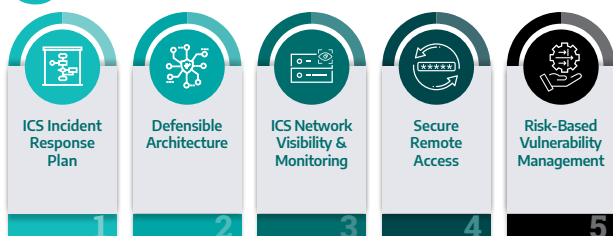# Which industrial sectors are covered by the NIS2 Directive?

Healthcare

Transport

Manufacturing of Critical Products
(such as Pharmaceuticals, Medical Devices, Chemicals)

Digital Infrastructure, including Data Centers

Space

Food

Postal and Courier Services

Public Administration

Water Supply

Wastewater and Waste Management

Energy

Digital Service Providers

When will the NIS2 Directive come into force?

The NIS2 Directive was published in the Official Journal of the EU on 27 December 2022 and entered into force on 16 January 2023. Member States have until 17 October 2024 to transpose the Directive into national law. Each Member State will adopt its own specific national legislation to meet the requirements of the NIS2 Directive.

NIS2 aims for a more aligned cybersecurity management approach to mitigate inconsistencies in cybersecurity resilience across sectors, outlining several key measures to manage risks posed to networks and information systems.

NIS2 and the Five Critical Controls for ICS/OT Cybersecurity

5 CRITICAL CONTROLS
FOR WORLD-CLASS OT CYBERSECURITY

ICS Incident Response Plan	Defensible Architecture	ICS Network Visibility & Monitoring	Secure Remote Access	Risk-Based Vulnerability Management
1	2	3	4	5

Dragos co-founder and CEO Robert M. Lee worked with SANS Institute ICS Curriculum Director Tim Conway to identify **5 Critical Controls for ICS/OT Cybersecurity**. These controls can be applied globally to enable organizations to meet and exceed several regulations, including the NIS2 Directive. The five critical controls put a strong emphasis on practices that facilitate an active defense as opposed to a traditional prevention-focused approach, aligning well with the risk-based thought process behind the NIS2 Directive.

DRAG⊘S

CRITICAL CONTROL	SUMMARY OF CONTROL	NIS2 Directive Applicability
ICS Incident Response Plan	Create a dedicated plan that includes the right points of contact, such as which employees have which skills inside which plant, as well as thought-out next steps for specific scenarios at specific locations. Identify responsible parties, notifications, and escalation policies. Leverage tabletop simulation exercises to test and improve response plans.	Incident handling (prevention, detection, and response to incidents) Business continuity and crisis management
Defensible Architecture	OT security strategies often start with hardening the environment - removing extraneous OT network access points, maintaining strong policy control at IT/OT interface points, and mitigating high risk vulnerabilities. Perhaps even more important than a secure architecture are the people and processes to maintain it. The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.	Policies and procedures to assess the effectiveness of cybersecurity risk management measures Supply chain security – including security-related aspects of relationships between each entity and (i) its suppliers or (ii) service providers (such as data storage providers and processing services or managed security services providers)
ICS Network Visibility and Monitoring	You can't protect what you can't see. A successful OT security posture maintains an inventory of assets, maps vulnerabilities against those assets (and mitigation plans), and actively monitors traffic for potential threats. Visibility gained from monitoring your industrial assets validates the security controls implemented in a defensible architecture. Threat detection from monitoring allows for scaling and automation for large and complex networks. Additionally, monitoring can also identify vulnerabilities easily for action.	Risk analysis and information system security policies Supply chain security – including security-related aspects of relationships between each entity and (i) its suppliers or (ii) service providers (such as data storage providers and processing services or managed security services providers) Policies and procedures to assess the effectiveness of cybersecurity risk management measures

DRAGOS

CRITICAL CONTROL	SUMMARY OF CONTROL	NIS2 Directive Applicability
Secure Remote Access	Secure remote access is critical to OT environments. A key method, multi-factor authentication (MFA) is a rare case of a classic IT control that can be appropriately applied to OT. Implement MFA across your systems of systems to add an extra layer of security for a relatively small investment. Where MFA is not possible, consider alternate controls such as jump hosts with focused monitoring. The focus should be placed on connections in and out of the OT network and not on connections inside the network.	The use of cryptography and encryption
Risk-Based Vulnerability Management	Knowing your vulnerabilities – and having a plan to manage them – is a critical component to a defensible architecture. Over 1200 OT-specific vulnerabilities were released last year, most of them with incomplete or erroneous information. While patching an IT system like a worker's laptop is relatively easy, shutting down a plant has huge costs. An effective OT vulnerability management program requires timely awareness of key vulnerabilities that apply to the environment, with correct information and risk ratings, as well as alternative mitigation strategies to minimise exposure while continuing to operate.	Risk analysis and information system security policies Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosures Supply chain security – including security-related aspects of relationships between each entity and (i) its suppliers or (ii) service providers (such as data storage providers and processing services or managed security services providers)

Mapping Dragos Solutions to NIS2 Directive

The table below shows how Dragos offerings map to specific NIS2 requirements.

NIS2 DIRECTIVE, CHAPTER IV, ARTICLE 21	DESCRIPTION	DRAGOS OFFERING
a	risk analysis and information system security policies	• Dragos Industrial Cyber Risk Management (ICRM) • Tabletop Exercises • OT Cybersecurity Assessment
b	incident handling (prevention, detection, and response to incidents)	• Dragos Platform • OT Watch • Dragos WorldView Threat Intelligence • Incident Response/Rapid Response Retainer
c	business continuity and crisis management	• Incident Response/Rapid Response Retainer • OT Cybersecurity Assessment • Dragos ICS-OT Cybersecurity Training
d	supply chain security including security-related aspects concerning the relationships between each entity and its suppliers or service providers such as providers of data storage and processing services or managed security services	• Dragos Platform • Dragos Industrial Cyber Risk Management (ICRM) • Dragos WorldView Threat Intelligence • ICS Network Vulnerability Assessment
e	security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure	• Dragos Platform • OT Watch • OT Cybersecurity Assessment • Dragos WorldView Threat Intelligence • Dragos Neighborhood Keeper • ICS Penetration Testing

NIS2 DIRECTIVE, CHAPTER IV, ARTICLE 21	DESCRIPTION	DRAGOS OFFERING
f	policies and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures	• Dragos Industrial Cyber Risk Management (ICRM) • OT Cybersecurity Assessment • ICS Penetration Testing • Maturity Assessment
g	basic cyber hygiene practices and cybersecurity training	• Dragos Platform • OT Cybersecurity Assessment, including Architecture Review and Penetration Testing

Descriptions of Dragos Offerings

Dragos Industrial Cyber Risk Management (ICRM)

Dragos guidelines for industrial cyber risk management distill industry best practices, frameworks, and standards into an approachable process for both novices and veterans of enterprise risk.

Tabletop Exercises

The Dragos Tabletop Exercise (TTX) Service is a step-by-step method that demonstrates how a realistic attack may occur within your unique ICS environment based on your organization's most concerning risks. Dragos TTXs include collaboration between all stakeholders, including information technology (IT) and industrial control systems (ICS) security teams, to strengthen internal communication strategies and develop relationships.

OT Cybersecurity Assessment

The OT Cybersecurity Assessment includes a full program review, creation of a collection management framework, crown jewel analysis, topology review, standards and regulations review, indicators of compromise sweep, threat discovery, asset inventory, network vulnerability assessment, and asset vulnerability assessment.

DRAGOS

Dragos Platform

The Dragos Platform is industrial control system (ICS) cybersecurity technology that delivers unmatched visibility of your ICS/OT assets and communications. It rapidly pinpoints threats through intelligence-driven analytics, identifies and prioritizes vulnerabilities, and provides best-practice playbooks to guide teams as they investigate and respond to threats before they cause significant operational impact.

OT Watch

With Dragos OT Watch, our ICS cybersecurity experts become part of your team, performing high severity notification triage and proactive threat hunting with the Dragos Platform to ensure threats don't get overlooked. Our elite team of analysts proactively hunt for and report on threat activity in your ICS environment using the latest threat intelligence exclusive to Dragos customers. We work alongside your team to triage and investigate high severity notifications to reduce the burden on internal resources.

Dragos WorldView Threat Intelligence

Dragos WorldView industrial threat intelligence provides actionable information and recommendations on threats to operations technology (OT) environments. It provides security teams with in-depth visibility of the tactics, techniques, and procedures (TTPs) of sophisticated adversaries targeting industrial networks globally, so your organization can better prepare for, detect, and respond to potential attacks.

Incident Response/Rapid Response Retainer

OT-specific response plans are essential for industrial environments. Since the potential impact of a cyber attack can vary based on visibility, the ability to respond, and your organizational security posture, a dedicated ICS/OT incident response plan accounting for your needs is crucial to quickly scope, investigate, and respond to incidents. As the cornerstone of your ICS/OT cyber program, an ICS-specific incident response retainer ensures you can respond quickly and recover confidently.

Dragos ICS-OT Cybersecurity Training

Training builds a better shared understanding of the terminologies, purpose, security goals, and technologies deployed in OT environments and security programs. Training operations staff in cybersecurity fundamentals is an important part of business continuity – cybersecurity is everyone's job, and the operations team are the front lines for identifying and mitigating issues.

ICS Network Vulnerability Assessment

An ICS Network Vulnerability Assessment helps your company close gaps in network defense by evaluating protection, detection, and response capabilities that currently exist in your environment. The assessment identifies exploitable vulnerabilities and provides action items to strengthen OT cybersecurity posture.

Dragos Neighborhood Keeper

Neighborhood Keeper is a collective defense and community-wide visibility solution that provides a more effective industrial cyber defense by sharing aggregated and anonymized asset, threat, and vulnerability intelligence at machine-speed across industries and geographic regions. By participating, each organization's defensive capability is made stronger than what they can achieve on their own.

ICS Penetration Testing

ICS Penetration Testing prevents severe breaches by leveraging real-world attacker tactics, techniques, and procedures (TTPs) gained from intelligence. Penetration testing identifies devices that could allow unauthorized access to critical ICS assets and demonstrates how attackers can move through ICS environments.

Maturity Assessment

Our industry-leading Professional Services team can help you evaluate and mature your OT cybersecurity program with a Cybersecurity Capability Maturity Model (C2M2) assessment. C2M2 was established by the U.S. Department of Energy, and provides a structured way to evaluate cybersecurity capabilities based on a graduated scale of maturity, helping organizations better understand their current cybersecurity capabilities and enhance their security posture.

Next Steps: Align Your OT Cybersecurity Journey with the NIS2 Requirements

Dragos recommends working with your executive leadership and management teams to get all stakeholders involved in discussions about NIS2 compliance. Taking these steps now will ensure that your organisation is ready to deploy programs and procedures that are compliant with the regulation when it becomes law in your country.

STEP 1	**Raise awareness among top management about cybersecurity risk management, the NIS2 requirements, and the potential impacts of maintaining the status quo.**
STEP 2	**Work with internal teams to review the cybersecurity risk management measures mandated by the NIS2 Directive. Identify how mature your organisation is currently within each of the mandates.**
STEP 3	**Consider incident response and reporting first. Do you have a response retainer in place? Do you have a fully developed, agreed upon, and practiced incident response plan? Do you know what triggers the incident response process to begin? Does your organisation have a business continuity and crisis management plan that integrates all areas of your business? If you say no to any of those questions, consider working with Dragos to get your incident response program fully developed and integrated into your processes.**

STEP 4	**Assess the security of your supply chain. You'll need a list of every asset that's part of your environment (made much easier by using technology like the Dragos Platform) – each of those asset vendors would be part of your supply chain. What software is being utilised throughout your process? Those vendors are part of your supply chain, too. Same goes for the hardware and software at the enterprise level because it's connected to your plant- and facility-level networks. All these vendors will need to be assessed. Dragos can identify remote access connections used by third parties, evaluate the policies and controls used to manage that connectivity, and recommend changes to technologies, policies, and procedures to make that access more secure.**
STEP 5	**Create a full OT cybersecurity roadmap, complete with your current level of maturity in key areas and time-bound plans for improving and optimising. From technology adoption to workforce development, you'll want to create a long-term view of your cyber readiness so that you can consistently measure progress.**

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo   Contact Us