



Business



Solution brief

**Simplifying the NIS2 directive
with Orange Belgium, powered
by Aeris IoT Watchtower™**

POWERED BY  **aeris**

In today's hyper-connected world, European utility providers are on the cusp of a significant transformation with the introduction of the NIS2 Directive. This regulation is not just another compliance checkbox—it represents a fundamental shift in how utilities and other essential service providers approach cybersecurity. The stakes are higher than ever, with the directive focusing on enhancing the resilience and security of network and information systems.

The pressure to ensure compliance while maintaining operational efficiency can feel daunting. Aeris IoT Watchtower™ is your strategic ally in navigating the NIS2 requirements for cellular IoT, enabling organizations to build robust defenses, streamline incident management, and maintain continuous monitoring—all essential for cellular IoT systems to remain secure and compliant.

Navigating the NIS2 directive for cellular IoT deployments with Aeris IoT watchtower

The digital landscape is changing rapidly, and with it comes new regulations that impact how enterprises approach cybersecurity. The NIS2 Directive is a pivotal regulatory framework set to enhance the security of systems across the EU. For organizations deploying cellular IoT solutions, the path to compliance can feel complex and overwhelming.

That's where Aeris IoT Watchtower helps. Designed with cellular IoT in mind, Aeris IoT Watchtower is here to support your enterprise with a powerful platform for robust monitoring, reporting, and proactive security—making NIS2 compliance achievable and sustainable.

Understanding the NIS2 directive

NIS2 sets comprehensive cybersecurity obligations for Essential and Important Entities, focusing on strengthening the resilience of critical infrastructure. The directive requires organizations to build solid security foundations.



How Aeris IoT Watchtower™ supports your NIS2 compliance journey

Article 3 Continuous monitoring for Essential and Important Entities	Ensures that critical infrastructure is proactively protected and compliant, reducing operational and reputational risks.
Article 3, Paragraph 5 Swift Activation	Can be activated swiftly on IoT devices, allowing entities added to these lists to rapidly meet their new obligations.
Article 21, Paragraph 1 "Always-on" risk management	Enables continuous protection against security risks and safeguards against potential disruptions that could impact services, revenue, or customer trust.
Article 21, Paragraph 2 All-hazards approach	Supports automated risk assessments and zero trust policies ensuring robust security resilience across all your IoT devices.
Article 21, Paragraph 2.a Policies on risk analysis and security	Creates regular risk assessment reports with actionable recommendations prevent vulnerabilities from being overlooked, ensuring a proactive approach to cybersecurity.
Article 21, Paragraph 2.b Incident handling with AI analysis	Provides fast, automated behavioral-based detection for blocking malicious activity significantly reduces downtime and damage from cyberattacks, providing historical data for incident forensics while improving operational reliability.
Article 21, Paragraph 2.d Supply chain security measures	Mitigates the impact of supply chain attacks and offers a compensating control through Zero Trust network access, protecting interconnected systems, limiting the potential damage from supply chain attacks.
Article 21, Paragraph 2.e Security during system acquisition, development, and maintenance	Monitors for vulnerabilities to ensure that new and existing devices, systems, and traffic are continuously detected, monitored, and logged for risk assessment reports which prove security, reducing long-term risks and compliance headaches.
Article 21, Paragraph 2.h Data encryption policies	Monitors for unencrypted data transmission protects sensitive information and your infrastructure from lateral movement, maintaining data integrity and trust in service operations.

How Aeris IoT Watchtower™ supports your NIS2 compliance journey

Article 21, Paragraph 2.j Multi-factor authentication (MFA)	Adds a critical layer of security, reducing unauthorized access risks to Aeris IoT Watchtower enhancing overall system protection.
Article 23, Paragraph 3a Incident reporting requirements	Identifies anomalies in data transmission that signal potential operational disruptions or breaches, helping to mitigate any impact, ensuring regulatory compliance proof, while supporting quicker recovery and transparency during cybersecurity incidents.
Article 23, Paragraph 4.a Reporting incidents within 24 hours	Ensures rapid detection of security incidents for early intervention and minimization of potential fallout enabling timely reporting helping you comply with regulatory timelines and demonstrate due diligence.
Article 21, Paragraph 4.b Incident report updates within 72 hours	Assists in ongoing incident updates and real-time risk management with detailed metrics and behavioral analysis helps maintain transparency and ensures that key stakeholders, including regulatory bodies, are informed of the evolving situation.
Article 23, Paragraph 4.c Intermediate incident status reports	Stores 90 days of behavioral data, aiding in comprehensive incident reporting providing thorough, intermediate status reports to regulators, showing accountability and continuous monitoring.
Article 23, Paragraph 4.and 4.e Final reports and monthly updates for ongoing incidents	Facilitates detailed final and continuous reporting for long-term incident management keeping all parties informed of ongoing efforts.

Why Aeris IoT Watchtower?

Aeris IoT Watchtower gives you full visibility to the security posture of your IoT devices as well as all the traffic that is going to and coming from your IoT devices. Our monitoring is very granular – at the device level. We monitor and log every session. That is what you need to detect threats and abnormalities. We also provide you with periodic reports outlining what risks we see and providing recommendations on how to improve your security.

Aeris IoT Watchtower also gives you complete control over the traffic that goes through your network. You can set up security policies to control which devices can communicate with which applications. The security policies are adaptive. They learn and alert about traffic or behavior outside of these policies. If a device is compromised, Aeris IoT Watchtower will contain it, no device recalls necessary. We automatically block malicious traffic occurring between your IoT devices and the Internet. Our enforcement enables you to set granular policies and groups to limit device communication to a list of explicitly allowed destination servers.

- Proactive Risk Management: Automated, in-depth monthly assessments across 19 risk dimensions, so you're never caught off guard.
- Intelligent Threat Monitoring: AI-driven analysis for early detection and response to potential security issues.
- Zero Trust Access: Ensure only authenticated, policy-compliant devices have access to critical applications.
- Enhanced Reporting: Timely, comprehensive data for all NIS2-mandated reporting requirements, easing the burden on your IT teams.

Meeting NIS2 requirements doesn't have to be a burden. With Orange Belgium and Aeris as your partner, you gain not only a tool but a reliable ally in your compliance journey. By leveraging advanced monitoring, threat intelligence, and proactive security features, you can focus on what matters most – keeping your cellular IoT operations secure and compliant. Let Aeris IoT Watchtower make your path to NIS2 compliance straightforward and effective.

POWERED BY  aeris

Copyright © 2026 Orange Business. All rights reserved. Orange, the Orange logo, Orange Business and product and service names are trademarks of Orange Brand Services Limited. All other trademarks are the property of their respective owners. More information on the use and terms of use of your plan is provided in our General Terms and Conditions. Responsible publisher: N. Rahbani – Orange Belgium SA/NV – Avenue du Bourget/Bourgetlaan 3 - B-1140 Brussels



Business