Navigating the NIS2 Directive with Aeris IoT Watchtower™

In collaboration with orange

In today's hyper-connected world, European businesses 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 be daunting. **Aeris IoT Watchtower™** is your strategic partner 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.

Understanding the NIS2 Directive and Its Importance

The Network and Information Security Directive (NIS2) is the European Union's enhanced cybersecurity framework, expanding on the original NIS Directive to strengthen resilience against cyber threats.
It establishes comprehensive cybersecurity obligations for Essential and Important Entities, focusing on reinforcing the resilience of critical infrastructure and requiring organizations to build strong security foundations.

WHAT IS NIS2?

NIS2 is a regulatory framework designed to enhance the overall cybersecurity posture of critical and important entities operating within the EU. It introduces stricter security requirements, incident reporting obligations, and higher penalties for non-compliance.

It was officially adopted in January 2023, with EU member states required to transpose it into national law by October 17, 2024. Organizations must ensure compliance by this deadline.

WHO MUST COMPLY?

If your organization operates in a critical sector such as energy, healthcare, financial services, or digital infrastructure, NIS2 compliance is not optional—it's mandatory. The directive categorizes organizations into Essential Entities (EE) and Important Entities (IE) based on their sector and size. Essential Entities operate in highly critical industries and face stricter security mandates, while Important Entities still have significant cybersecurity responsibilities but with slightly lower regulatory pressures. Compliance requires robust cybersecurity measures, incident reporting, supply chain security, and ongoing risk assessments. Failure to meet these standards can result in hefty fines and legal consequences for company leadership.

ENTITY TYPE	DEFINITION	COMPANY SIZE	KEY REQUIREMENTS	ENFORCEMENT & FINES
Essential Entities (EE)	Organizations in highly critical sectors (e.g., energy, healthcare, financial services, digital infrastructure).	Large enterprises (250+ employees and/or €50M+ turnover)	Comprehensive risk management, rapid incident reporting (within 24 hours), robust business continuity and crisis management plans, strict supply chain security measures, strong governance and accountability frameworks, regular security audits, robust encryption and access controls, and ongoing cybersecurity training.	Fines up to €10 million or 2% of global annual turnover. Legal liability for management in cases of negligence.
Important Entities (IE)	Organizations in sectors with substantial economic impact (e.g., manufacturing, postal services, food production).	Medium to large enterprises (50+ employees and/or €10M+ turnover)	Effective risk management, timely incident reporting, business continuity planning, supply chain risk management, clear governance structures, periodic security audits, appropriate encryption and access controls, and cybersecurity awareness training.	Fines up to €7 million or 1.4% of global annual turnover. Legal liability for management in cases of negligence.

Simplifying 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.

It was officially adopted in January 2023, with EU member states required to transpose it into national law by October 17, 2024. Organizations must ensure compliance by this deadline.

HOW AERIS IOT WATCHTOWER SUPPORTS YOUR NIS2 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 of 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.
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.

HOW AERIS IOT WATCHTOWER SUPPORTS YOUR NIS2 JOURNEY

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 23, 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, Paragraphs 4.d 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?

Navigating the complexities of the NIS2 Directive can be daunting, but Aeris IoT Watchtower simplifies compliance while providing robust security for your cellular IoT deployments. Aeris IoT Watchtower is the optimal choice for ensuring your organization meets and exceeds NIS2 requirements for cellular IoT, delivering significant business value through enhanced security, streamlined operations, and proactive risk management.

FULL VISIBILITY AND GRANULAR MONITORING

Aeris IoT Watchtower offers unparalleled visibility into the security posture of your IoT devices and the traffic they generate. Our monitoring is granular, down to the device level, ensuring that every session is logged and analyzed. This level of detail is crucial for detecting threats and abnormalities in real-time, providing you with the insights needed to maintain a secure and resilient cellular IoT environment.

- **Device-Level Monitoring:** Track and log every session to detect threats and abnormalities, ensuring comprehensive oversight and quick identification of potential issues.
- **Comprehensive Traffic Analysis:** Monitor all incoming and outgoing traffic to and from your cellular IoT devices, enabling you to identify and mitigate risks effectively.

Business Value: Full visibility and granular monitoring help prevent security breaches, reduce downtime, and protect sensitive data, ultimately safeguarding your business operations and reputation.

PROACTIVE RISK MANAGEMENT

Stay ahead of potential threats with automated, in-depth monthly and continuous assessments across 25 risk categories. Aeris IoT Watchtower ensures you're never caught off guard, providing you with the insights needed to manage risks proactively and maintain a robust security posture.

- **Automated Risk Assessments:** Daily, detailed evaluations of your security posture ensure that vulnerabilities are identified and addressed promptly.
- **Actionable Insights:** Periodic reports outlining identified risks and recommendations for improvement, enabling informed decision-making.

Business Value: Proactive risk management minimizes the likelihood of costly security incidents, enhances operational efficiency, and ensures compliance with regulatory requirements.

INTELLIGENT THREAT PROTECTION

Leverage advanced threat intelligence to detect potential issues early, enabling swift responses that minimize impact. Aeris IoT Watchtower's intelligent threat protection ensures that your IoT devices remain secure against evolving threats, protecting your business from potential disruptions.

- **Threat Intelligence Integration:** Utilize up-to-date threat intelligence feeds to stay informed about the latest threats and vulnerabilities, allowing for early detection and proactive defense.
- **AI-Driven Analysis:** Employ sophisticated algorithms to analyze threat data and identify potential issues before they can impact your business.

Business Value: Early detection and swift response to threats reduce the risk of operational disruptions, protect sensitive data, and maintain customer trust.

MALWARE DETECTION AND PREVENTION

Ensure robust protection for your IoT devices with Aeris IoT Watchtower's advanced malware detection and prevention capabilities. Our solution safeguards your network by identifying and blocking malicious activities in real-time, ensuring continuous protection

- **Sophisticated Malware Detection:** Use cutting-edge detection techniques to identify and block malware, ensuring comprehensive protection for your IoT devices.
- **Swift Response:** Minimize the impact of threats with rapid threat mitigation, containing and neutralizing malware before it can compromise your network.

Business Value: Effective malware protection prevents costly data breaches, reduces downtime, and maintains the integrity of your IoT ecosystem.

ZERO TRUST ACCESS

Implement a Zero Trust security model with Aeris IoT Watchtower, ensuring that only authenticated, policy-compliant devices are granted access to the applications they need. This approach significantly bolsters your security posture by preventing unauthorized access and ensuring that only trusted devices can interact with your network.

- **Authenticated Access:** Only verified devices can connect to your network, reducing the risk of unauthorized access.
- **Policy Compliance:** Enforce strict access controls based on security policies, ensuring that all devices adhere to your security standards.

Business Value: Zero Trust Access enhances overall security, reduces the risk of insider threats, and ensures compliance with regulatory requirements.

STREAMLINE AUDITS

Simplify the audit process and meet NIS2-mandated reporting requirements with detailed, timely data from Aeris IoT Watchtower. Our platform eases the burden on your IT teams by providing comprehensive reports that ensure transparency and accountability, making audits more efficient and less time-consuming.

- **Detailed Compliance Reports:** Generate comprehensive data that meets regulatory requirements, providing clear evidence of your security measures and practices.
- **Timely and Regular Updates:** Receive regular updates to keep you informed and compliant, ensuring that your audit documentation is always current and accurate.

Business Value: Streamlined audits save time and resources, reduce the risk of non-compliance penalties, and enhance transparency and accountability within your organization.

VULNERABILITY MITIGATION AND CONTAINMENT

Effectively manage and respond to Common Vulnerabilities and Exposures (CVEs) within your cellular IoT network with Aeris IoT Watchtower. Our platform enables you to implement robust protection policies that contain vulnerabilities, allowing for systematic patching and updates without the need for emergency, disruptive actions.

- **Proactive CVE Response:** Set specific policies to manage and mitigate vulnerabilities, ensuring that identified CVEs are addressed in a timely manner. This approach allows for regular patching schedules rather than urgent, reactive measures.
- **Controlled Containment:** Quickly contain compromised devices to prevent the spread of threats, maintaining network security while you address vulnerabilities at a normal, manageable pace. This ensures that your operations continue smoothly without the need for fire-drill responses.

Business Value: Effective vulnerability management reduces the risk of security breaches, minimizes operational disruptions, and allows for systematic, planned updates, thereby maintaining business continuity and protecting your reputation.

Conclusion

Meeting NIS2 requirements doesn't have to be a burden. With Aeris IoT Watchtower as your trusted partner, you gain not only a powerful solution, but a reliable partner dedicated to simplifying your compliance journey. Focus on what matters most—securing your cellular IoT operations—while Aeris IoT Watchtower handles the heavy lifting of continuous monitoring, threat intelligence, and proactive risk management.

Choose Aeris IoT Watchtower to ensure your organization remains secure, compliant, and resilient in the face of evolving cybersecurity challenges.

aeris

For more than three decades, Aeris has been a trusted cellular IoT leader enabling the biggest IoT programs and opportunities across Automotive, Utilities and Energy, Fleet Management and Logistics, Medical Devices, and Manufacturing. Our IoT technology expertise serves a global ecosystem of 7,000 enterprise customers and 30 mobile network operator partners, and 80 million IoT devices across the world. Aeris powers today's connected smart world with innovative technologies and borderless connectivity that simplify management, enhance security, optimize performance, and drive growth. To learn how Aeris IoT Accelerator Platform, Aeris IoT Watchtower and Aeris Mobility Suite can secure and supercharge your critical IoT programs, visit aeris.com and follow us on LinkedIn.

AERIS.COM

UNITED STATES CONTACT
info@aeris.net

EUROPE CONTACT
EU_info@aeris.net

INDIA CONTACT
india_info@aeris.net

In collaboration with orange™