ENTHEC

WHITEPAPER

OBJECTIVE CYBER RESILIENCE:

Good practices, keys and compliance with NIS 2 Directive

TABLE OF CONTENT

INTRODUCTION

More than a decade ago, the European Union became aware of the need to develop a common legal framework on cybersecurity that would lay the basis for a strategy shared by the Member States to fight cybercrime together.

The result of this need was the European Directive NIS 1 (Directive on Network and Information Security), which was adopted in 2016 by the European Union (EU) with the aim of improving cybersecurity in Europe and establishing a framework for cooperation between Member States to protect critical infrastructures and digital services. This directive marked a milestone in cybersecurity legislation by setting minimum cybersecurity standards in Europe and promoting greater resilience against cyber-attacks.

NIS 1 sought to ensure the protection of essential services such as energy, transport, health, telecommunications, and financial services, as well as digital service providers, search engines, online trading platforms, and cloud services. Member States should identify operators of essential services and digital service providers and ensure they implement appropriate measures to manage cybersecurity risks and report significant incidents.

INTRODUCTION

However, as technology and cyber threats evolve rapidly, the NIS 1 Directive became obsolete and insufficient to cover the growing complexity of cybercrime:

- Limited scope: NIS 1 only covered specific sectors and digital service providers, leaving out other essential services and types of companies that are increasingly vulnerable to cyber-attacks.

- Lack of harmonization: NIS 1 failed to unify cybersecurity approaches across Member States, leaving most security measures to the will of each national legislator, leading to differences in how cybersecurity measures were implemented across the EU.

- Emerging threats: Over time, new and more sophisticated cyber threats have emerged, such as ransomware, distributed denial of service (DDoS) attacks, and large-scale data theft, which NIS 1 did not effectively address.

To address these shortcomings and update the legal framework, the EU has developed the NIS 2 Directive, a new Cybersecurity Directive that expands and enhances the key aspects of its predecessor.

In this document, we will analyze the new European legal framework in Cybersecurity and what key aspects it reveals as the axes of updating the common cybersecurity strategy of all Member States. A guide to inspire the renewal of any organization’s strategy and to address security challenges caused by emerging threats.

NIS 2 DIRECTIVE: THE NEW EUROPEAN LEGAL FRAMEWORK FOR CYBERSECURITY

With the drafting of the NIS 2 Directive, the European Union seeks to overcome the shortcomings of NIS 1 by offering a more comprehensive and harmonized approach to protect networks and information across the European Union in a unified manner against the growing and changing threats.

The NIS 2 Directive entered into force on 27 December 2022 after its publication in the Official Journal of the European Union. Until 17 October 2024, Member States have the deadline for transposition to adopt and publish the measures necessary to comply with the Directive. As of that date, this new legal framework on Cybersecurity will be operational and binding throughout the European Union.

The main objective of NIS 2, which inspires all its provisions, is to unify the Cybersecurity strategy between Member States by defining standard minimum requirements and establishing mechanisms to ensure practical cooperation between authorities of the Member States.

In the spirit of the law, we can guess the key aspect of the new framework: Cybersecurity depends equally on the own measures adopted and the measures adopted by all those with whom some relationship is maintained.

NIS 2 DIRECTIVE: THE NEW EUROPEAN LEGAL FRAMEWORK FOR CYBERSECURITY

To remedy the deficiencies and obsolescence presented by its predecessor, the NIS 2 Directive incorporates as main axes of the regulation:

- **Wide scope:** NIS 2 extends its scope to include more digital sectors and services, covering a wider range of companies and services considered essential for the functioning of society.
- **Greater harmonization:** NIS 2 promotes greater harmonization of cybersecurity measures across the EU to ensure a more consistent and uniform approach to protecting critical infrastructures and digital services.
- **Focus on resilience:** NIS 2 stresses that Member States and businesses must develop capacities to resist and recover rapidly from cyber-attacks, thus strengthening cyber resilience across the EU.
- **Boosting proactivity:** NIS 2 focuses cybersecurity on the control and prevention of threats and risks, prompting to pre-empt cyberattacks as the main measure to avoid their consequences.
- **New threats and technologies:** NIS 2 considers emerging threats and evolving technologies, such as artificial intelligence and the Internet of Things (IoT) and seeks to address the challenges they pose for cybersecurity.
- **Addressing third-party risks:** NIS 2 integrates the obligation to control supply chain risks as one of the axes of the effectiveness of any cybersecurity strategy. The key approach that fuels policy development is the idea that cybersecurity is no longer a matter for one, both at the level of States and at the level of organizations. This implies that NIS 2 will have influence on a more significant number of organizations due to the cascade effect than stipulated in its articles.
- **Responsibilities and sanctions:** It is essential that, as soon as NIS 2 enters into force in the Member States, senior officials and management teams may be held personally responsible for their organization's non-compliance with NIS 2. In addition, the NIS 2 establishes a fine for essential entities for non-compliance that may reach up to 10 million Eur. or 2% of the company's annual worldwide turnover. For significant entities, the fine may amount to 7 million Eur. or 1.4% of the world's annual turnover.

SCOPE OF THE NIS 2

The scope of the NIS 2 Directive is broader than its predecessor's.

NIS 2 covers various digital services and sectors to ensure comprehensive and coordinated protection against cyber threats in the European Union.

The main objective of extending the scope of the NIS 2 Directive is to ensure a more coherent and comprehensive approach to protecting networks and information across the Union. By including new sectors, services, and technologies, the directive seeks to address current and future challenges more effectively and strengthen cyber resilience across Europe.

The new legal framework ends the voluntary implementation of the measures, obliging Member States to include it in their national legislation and businesses to monitor, manage and monitor risks and improve resilience and responsiveness.

In practice and because of the cascade effect, it is estimated that this scope will be much broader than the strict provisions of the directive because of the obligation to control the supply chain risk imposed on the companies and sectors to which it is addressed.

SCOPE OF THE NIS 2

COVERED SECTORS

HIGH CRITICALITY

11 sectors considered essential for the functioning of society, to which the NIS 2 Directive applies

CRITICAL

7 sectors considered critical for which the NIS 2 provisions will also be mandatory

- Energy
- Banking
- Financial Markets
- Health Sector
- Transport
- Digital Infraestructure
- Drinking Water
- Waste Water
- ICT Service Management B2B
- Space
- Public Administration

- Research
- Chemical Industry
- Food Sector
- Post and Courier
- Digital Providers
- Manufacturing
- Waste Management

OBLIGED ORGANIZATIONS

COMPANIES

Medium and large companies

(more than 250 employees and with an annual turnover of 50 million euros from now on)

ADMINISTRATION

All Public Administrations

(except National Defense or security, public security, the police, the judiciary and parliaments and central banks).

SCOPE OF THE NIS 2

ENTITIES CLASSIFICATION

ESSENTIAL

Those belonging to the highly critical sectors exceeding the ceilings, as well as qualified providers of trust services and top-level domain name registrations and DNS service providers, regardless of their size. Also, providers of public electronic communications networks or publicly available electronic communication services which are considered to be medium-sized enterprises, public administration entities, any other entity belonging to other critical sectors identified by the Member State as an essential entity, the critical entities identified by the CER Directive, and, if the Member State so provides, entities identified as operators of essential services in the previous NIS Directive 1.

Will be required to meet supervisory requirements as of the introduction of NIS 2.

IMPORTANT

Those entities that belong to highly critical sectors or other critical sectors that cannot be considered essential entities, such as online platforms, search engines and cloud services, among others.

Will be subject to ex-post supervision, meaning that in case authorities receive evidence of non-compliance, action is taken.

THE FIVE GOOD CYBERSECURITY PRACTICES IN NIS 2

The NIS 2 Directive is based on principles articulated through establishing **five good practices in cybersecurity**: continuous assessment, proactive mitigation, management and continuity, coordination and transparent communication, and cyber-hygiene and training.

Continuous risk and vulnerability assessment.

The **continuous assessment of risks and vulnerabilities** underpins the proactive and preventive approach to strengthen cybersecurity in the EU and is the cornerstone of constructing the Cybersecurity strategy. It involves identifying and monitoring potential threats to evaluate their impact and likelihood of occurrence and analyze weaknesses in the cybersecurity strategy.

Included in this principle, the Directive determines the importance of including the **supply chain and third-party risk** in this continuous assessment and makes it mandatory.

Proactive mitigation of identified risks and vulnerabilities.

Proactive risk and vulnerability mitigation is a central element of NIS Directive 2, as it focuses on preventing and reducing the impact of potential cyber-attacks rather than simply responding to them after they occur.

Once risks and vulnerabilities have been identified through continuous assessment, security measures should be taken in accordance with the identified risk levels. This may include enforcing stricter access controls, regularly updating software and systems, using data encryption, active network monitoring, the demand for cybersecurity remediation and scorings to the supply chain, or implementing robust security protocols, among others.

That is, we must act before the attack materializes to prevent it or, at least, prevent it from having consequences.

GOOD CYBERSECURITY PRACTICES IN NIS 2

The NIS 2 Directive is based on principles articulated through establishing **five good practices in cybersecurity:** continuous assessment, proactive mitigation, management and continuity, coordination and transparent communication, and cyber-hygiene and training.

Crisis management and business continuity

The idea is to prevent the cyber-attack from occurring. Still, if unavoidable, the NIS Directive 2 establishes the need to develop effective crisis management procedures to ensure maximum operational continuity during an incident.

Organizations must develop well-defined incident response plans and procedures and have them tested and updated. This ensures that, in the event of a cyberattack or security incident, there is a rapid and coordinated response to mitigate the impact and restore normal business operations as soon as possible.

- Development of a detailed Crisis Management Plan with roles and responsibilities, the sequence of actions to be followed, and communication protocols with the competent authority and stakeholders.
- Development of a detailed Business Recovery and Continuity Plan focused on actions to maintain or restore operational time within the allowable time frame and ensure the continuity of essential services.
- Conducting tests and simulations to test plans, verifying their effectiveness, familiarizing workers with the procedure, and detecting improvement points.
- Collaboration with the competent authorities to prevent the spread and improve the response to the incident.
- Post-incident evaluation to analyze failures and identify points to improve or change.

GOOD CYBERSECURITY PRACTICES IN NIS 2

The NIS 2 Directive is based on principles articulated through establishing **five good practices in cybersecurity**: continuous assessment, proactive mitigation, management and continuity, coordination and transparent communication, and cyber-hygiene and training.

Rapid and transparent coordination and communication of risks, vulnerabilities, and incidents.

The NIS Directive 2 stipulates that entities must notify the relevant authorities of any significant incident. The institutions concerned shall follow a particular procedure:

- **Initial notification - Early warning**: Within 24 hours of the incident, the entity shall notify the CSIRT or, failing that, the designated Competent Authority.
- **Interim Notification - Update**: 72 hours after incident detection, the entity shall update the incident status by presenting an initial assessment.
- **Final notification - Reporting**: Within one month of notification of the incident, the entity shall submit a final report containing a detailed description of the incident (including severity, impact, type of threat caused by the incident, mitigation measures in place, and ongoing and, if applicable, cross-border impacts).

In addition, **continuous, rapid, and transparent communication** on cybersecurity is promoted both between Member States, between competent authorities and organizations, or between stakeholders potentially affected either directly or indirectly. This exchange of information on vulnerabilities and incidents should be rapid, open, and transparent.

GOOD CYBERSECURITY PRACTICES IN NIS 2

The NIS 2 Directive is based on principles articulated through establishing **five good practices in cybersecurity:** continuous assessment, proactive mitigation, management and continuity, coordination and transparent communication, and cyber-hygiene and training.

Cyber-hygiene and training.

The NIS 2 Directive focuses on increasing the awareness and capabilities of Union citizens and organizations to protect themselves against cyber threats and contribute to a safer and more resilient digital environment.

- **Cyber-hygiene**: Cybersecurity practices and habits that users must follow to protect their devices and data. This includes using strong and unique passwords, regularly updating software and applications, activation of two-factor authentication, caution when clicking links or downloading files, and using secure Wi-Fi networks.
- **Training and awareness in cybersecurity for users and staff of organizations.** Companies must train employees to identify and report potential security incidents and follow established security procedures.
- **Education**: NIS 2 advocates the inclusion of e-hygiene in educational curricula. Teaching basic cybersecurity skills from an early age is essential to form a generation of more conscious and safe users in the digital environment.
- **Public awareness** of the importance of cybersecurity through awareness and communication campaigns on cybersecurity issues.

KEY ELEMENTS OF NIS 2

The good cybersecurity practices established by the NIS 2 Directive pivot on key elements for its implementation, execution, and effectiveness.

Innovation, AI, and automation.

NIS 2 establishes an obligation for Member States to encourage using innovative technology, including artificial intelligence, to improve the detection and prevention of cyber-attacks, allowing resources to be diverted more effectively toward fighting them. To this end, research and development activities aimed at facilitating the use of such technologies, in particular those related to automated or semi-automated tools in the field of cybersecurity, and, where appropriate, the exchange of data necessary to train users of these technologies and improve them, will be promoted within the National Cybersecurity Strategies.

Emerging threats and advanced technologies.

NIS Directive 2 considers new cyber threats and evolving technologies, such as artificial intelligence, the Internet of Things (IoT), and 5G networks. This ensures that legislation is up-to-date and relevant to current and future challenges in Cybersecurity.

Data protection.

NIS 2 Directive encourages the full use of data protection principles by design and default, as well as the most advanced security and privacy measures, such as pseudonymization and encryption, to protect personal data. In addition, it establishes that the use of any cybersecurity technology, including artificial intelligence, must comply with Union data protection law, including the data protection principles of accuracy, data minimization, fairness and transparency, and data security, such as advanced encryption.

KEY ELEMENTS OF NIS 2

Supply chain.

NIS Directive 2 states that addressing cybersecurity risks arising from an entity's supply chain and its relationship with its suppliers is particularly important due to the prevalence of incidents in which entities have been victims of cyberattacks and in which malicious actors have been able to compromise the security of an entity's network and information systems by taking advantage of vulnerabilities affecting third-party products and services. Small and medium-sized enterprises are increasingly suffering from attacks against supply chains due to the weaker stringency of their cybersecurity risk management and attack management measures and their limited security resources. Such supply chain attacks not only affect small and medium-sized enterprises and their operations in isolation but can also have a cascading effect in the context of larger attacks against the entities to which they have supplied. The Directive therefore calls on Member States to help small and medium-sized enterprises address the challenges they face in their supply chains through their National Cybersecurity Strategies.

Figure of the CISO.

NIS 2 Directive establishes the obligation of the companies to which it is addressed to have the Security Manager (CISO) figure, a duly qualified and full-time person who manages the company's cybersecurity and is part of the management team. It represents an excellent opportunity for CISOs to strengthen their position within the company, as NIS 2 introduces the notion of management responsibility in managing cybersecurity risks, as well as substantial penalties for violators. The NIS 2 Directive obliges critical entities and important entities to establish a proactive approach in risk management and the protection of critical data and systems, an approach for which the CISO is required to adopt the role of guide and leader in the decisions that must be made, both in technical and business matters, as well as disseminator within the organization, including senior managers, of Cybersecurity policies and best practices.

KEY ELEMENTS OF NIS 2

Related Organizations.

- **Competent Authorities:** Designated by each Member State, they will supervise the entities through inspections, security analyses, or audits.

- **Single point of contact:** Designated by each Member State, it will ensure cross-border cooperation between all designated Competent Authorities in that State.

- **CSIRT:** Computer Security Incident Response Teams that will assist essential entities affected by any incident and disseminate alerts, warnings, and information about cyber threats, vulnerabilities, and incidents among the entities involved in the NIS 2 Directive.

- **CSIRT Network:** Formed by representatives of the CSIRTs and the Computer Emergency Response Team of the institutions, bodies, offices, and agencies of the Union (CERT-EU) to exchange information on incidents, cyber threats...

- **Cooperation Group:** Composed of representatives of the Member States, the Commission, and ENISA, it will provide competent authorities with guidance with the transposition and application of the Directive, develop and implement policies on coordinated disclosure of vulnerabilities, and serve for the exchange of good practices and information related to the implementation of the Directive, cyber threats, vulnerabilities, etc.

- **European Network of Cybersecurity Crisis Liaison Organizations (EU-CyCLONe):** Formed by the Cybersecurity Crisis Management Authorities of the Member States and the Commission, it will have an observer role in case of cyber incidents likely to have a significant impact on the services and activities included in the NIS Directive 2, serving as a support in the coordinated management of large-scale cybersecurity incidents and crises.

NIS 2 COMPLIANCE: ADVANTAGES OF EXTERNAL ATTACK SURFACE MONITORING

The ability to prevent and nullify cyberattacks is today the fuel for the sustainable growth of any business and any State. This is recognized in the spirit that guides the drafting of the NIS 2 Directive.

> Therefore, much of the innovation of the NIS 2 Directive is based on the concept of Cyber Threat Intelligence: discover, analyze, and control both own and third-party risks to implement a proactive Cybersecurity strategy in the organization.

The **continuous and automated monitoring of leaked information and other threats from the corporate external attack surface** (Internet, Dark Web, and Deep Web) using Artificial Intelligence (AI) can play an essential role in the compliance of the European Directive NIS 2 by organizations. This Directive seeks to strengthen Cybersecurity in the European Union (EU), and AI applied to external surface surveillance helps to proactively identify and address Cybersecurity risks in a constantly evolving digital environment.

The concept of **corporate external attack surface** refers to the set of digital assets and data that are exposed and accessible from outside the organization, that is, those that can be detected and reached by anyone who knows how to search for them. This includes public websites, repositories, servers, databases, network-connected devices, and other digital resources accessible from the public web.

NIS 2 COMPLIANCE: ADVANTAGES OF EXTERNAL ATTACK SURFACE MONITORING

Identification of own threats and vulnerabilities:

Continuous and automated monitoring of the corporate external surface allows organizations to identify threats and vulnerabilities in real-time and continuously. Using advanced AI techniques, online sources, including social media, hacking forums, and Dark Web marketplaces, can be scanned and analyzed for mentions of the organization, its assets, or sensitive data. If leaked information, exposed access credentials, or details of vulnerabilities are detected, the monitoring system alerts the security team to take immediate action and nullify the risk.

Compliance with incident reporting:

NIS Directive 2 obligates critical institutions and major entities to report significant incidents to competent authorities. Continuous and automated monitoring with AI facilitates the early detection of vulnerabilities and incidents and the collection of relevant information to meet the notification deadlines established in the Directive.

Proactive response to incidents:

Continuous and real-time monitoring, together with the use of AI technologies, allows for automating identifying and categorizing risks and vulnerabilities on the corporate external surface and detecting the gap that has caused them. This makes prioritizing responses easier and allocating appropriate resources to address real-time critical incidents. By proactively detecting vulnerabilities and incidents, organizations can act before significant damage occurs, reducing the impact of attacks and improving their resilience.

NIS 2 COMPLIANCE: ADVANTAGES OF EXTERNAL ATTACK SURFACE MONITORING

Analysis of trends and attack patterns:

Continuous and automated monitoring of the corporate external surface provides objective data for analyzing trends and attack patterns over time. Identifying suspicious activity and anomalous behavior indicates developing threats or infiltration attempts. With this information, organizations can strengthen their defenses and improve their security posture.

Proactive supplier security assessment:

AI-powered continuous monitoring of the external attack surface also enables proactive and non-intrusive cyber security assessment of suppliers and third parties before they become a weak link in the supply chain. By analyzing public data and accessing relevant information in real-time, vulnerabilities are detected, and the security level of providers is evaluated to determine if they comply with the requirements of NIS 2. This enables a rapid and coordinated response to negate third-party risk, mitigate the impact of the potential incident, and prevent it from spreading throughout the supply chain.

Adaptation to new threats:

AI is especially effective at detecting emerging threats and unknown malware variants. Through machine learning and anomaly detection algorithms, AI can identify changing attack patterns and new tactics used by cybercriminals. This allows organizations to adapt their security strategies and be prepared to face ever-evolving cyber threats.

NIS 2 COMPLIANCE: ADVANTAGES OF EXTERNAL ATTACK SURFACE MONITORING

Compliance with regulations and security standards of the Directive:

Continuous and automated monitoring of the external attack surface helps organizations comply with regulations and security standards, including the NIS 2 Directive. By staying on top of threats and vulnerabilities, organizations can demonstrate that they are taking proactive measures to protect their systems and data and protect their supply chain and ensure that suppliers meet the required security standards, which is essential to meet the security requirements of the Directive and avoid penalties, which may involve a personal responsibility of the Management.

kartos©

XTI watchbots

Kartos XTI Watchbots: EASM + DRPS + SRS on a single platform

Kartos XTI Watchbots is the Cyber-surveillance platform developed by Enthec Solutions to extend the security perimeter controlled by organizations and institutions. Conceived from a hacker strategy approach, Kartos is in an ongoing R&D process to incorporate categories and capabilities ahead of the evolution of cyberattacks.

External Attack Surface Management

Detection of corporate assets and information about systems, cloud services, and applications that are available and visible in the public domain to any cybercriminal.

Digital Risk Protection Services

Detection of contextual information about possible attack agents, their tactics and processes to carry out malicious activities, and removal of malicious activities on behalf of the organization.

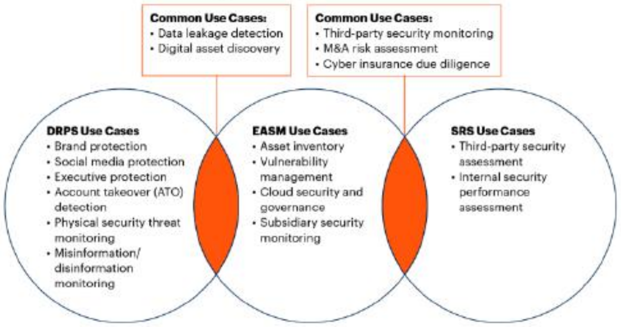
Security Rating Services

Independent risk assessment of own and third parties for a broad visualization of the maturity in cybersecurity of any organization using an external approach. Extension and weighting of information provided by third-party risk assessment traditional methods.

Analysis of 9 threat categories

- Network
- DNS Health / Phishing
- Patch Management
- IP Reputation
- Web Security
- Email Security
- Document Filtering
- Credential Filtering
- Social Networking

The Common Use Cases Supported by DRPS, EASM and SRS



Common Use Cases:
- Data leakage detection
- Digital asset discovery

Common Use Cases:
- Third-party security monitoring
- M&A risk assessment
- Cyber insurance due diligence

DRPS Use Cases
- Brand protection
- Social media protection
- Executive protection
- Account takeover (ATO) detection
- Physical security threat monitoring
- Misinformation/ disinformation monitoring

EASM Use Cases
- Asset inventory
- Vulnerability management
- Cloud security and governance
- Subsidiary security monitoring

SRS Use Cases
- Third-party security assessment
- Internal security performance assessment

Source: Gartner
758248_C

Gartner

kartos©

XTI watchbots

AI layer that allows operation 100% automated without intervention in any part of the process.

Strictly non-intrusive tool. The research is conducted on the Internet, the Deep Web and DarkWeb, and does not attack the IT perimeter of companies, so their operation and the information obtained strictly comply with the limits imposed by the legislation.

The only platform that analyzes **conversations on social networks from the perspective of detecting threats and attacks** beyond that relating to reputation and branding.

Continuous operation 365x24x7, allowing you to detect new information leaks practically in real time.

Maximum ease of use. No complex configuration is required. Simply enter the domain in the platform and it works autonomously without configuring search parameters or other criteria for locating information.

Automated, objective, and continuous monitoring of risks caused by third-parties belonging to the Company´s External Attack Surface.

Learn more about our licenses
Try the XTI Cyber-Intelligence for free
Start using Kartos

→ hello@enthec.com

Enthec is a Deep Tech that develops and manufactures cybersecurity software with a hacker approach to extend the reach of cyber-protection strategies of organizations.

Founded as a startup in 2019 by María Rojo, Enthec has grown through funding rounds and the success of its Kartos platform to consolidate itself as one of the Deep Tech with more innovative and effective solutions in the field of Cybersecurity.

To learn more about us, you can visit our website:

www.enthec.com