

ENTHEC

kartos[®]

Corporate Threat Watchbots

Resilience Objective

Best practices, key points and compliance with NIS 2

PAG.

Index

3	INTRODUCTION	
5	THE NEW EUROPEAN LEGAL FRAMEWORK ON CYBERSECURITY	
8	SCOPE OF THE DIRECTIVE	
12	THE 5 GOOD PRACTICES OF CYBERSECURITY NIS 2	
16	KEY ELEMENTS OF NIS 2	
19	COMPLIANCE WITH NIS 2:	
	• ADVANTAGES OF EXTERNAL SURFACE MONITORING	

INTRODUCTION

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

This need gave rise to 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 establishing minimum cybersecurity standards at European level and promoting greater resilience against cyberattacks.

NIS 1 aimed 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 were required to identify operators of essential services and digital service providers and ensure that they implemented appropriate measures to manage cybersecurity risks and reported significant incidents.

INTRODUCTION

However, as technology and cyber threats rapidly evolved, NIS Directive 1 became outdated and insufficient to address the growing complexity of cybercrime.

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

In this document we analyse the new European legal framework on Cybersecurity and what key aspects it reveals as axes for updating the common Cybersecurity strategy of all Member States. A guide to inspire the renewal of any organisation's strategy and to address the security challenges caused by emerging threats.

Limited range

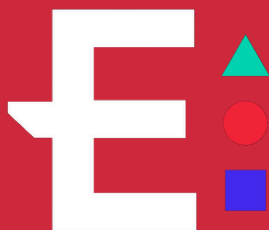
NIS 1 only covered certain sectors and digital service providers, leaving out other essential services and types of businesses that are increasingly vulnerable to cyberattacks.

Lack of harmonization

NIS 1 failed to unify cybersecurity approaches across Member States because it left the implementation of most security measures to the discretion of each national legislator, leading to differences in the way they were implemented across the EU.

Emerging threats

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



NIS DIRECTIVE 2:

THE NEW EUROPEAN LEGAL FRAMEWORK ON CYBERSECURITY

The key aspect of the new framework can be seen in the spirit of the law:
Cybersecurity depends equally on both the measures adopted and on
the measures taken by all those with whom any relationship is maintained.

DIRECTIVE NIS 2

THE NEW EUROPEAN LEGAL FRAMEWORK ON CYBERSECURITY

With the development of the NIS 2 Directive, the European Union seeks to overcome the shortcomings of NIS 1, offering a broader and more harmonized approach to unified protection of networks and information throughout the European Union against growing and changing threats.

The NIS 2 Directive entered into force on 27 December 2022, following its publication in the Official Journal of the European Union. Member States have until 17 October 2024 to transpose and adopt and publish the measures necessary to comply with the provisions of the Directive.

From that date, this new legal framework on Cybersecurity will be operational and mandatory throughout the European Union. The main objective of NIS 2, which inspires all its provisions, is the unification of the Cybersecurity strategy between Member States by defining common minimum requirements and establishing mechanisms that guarantee effective cooperation between the authorities of the Member States.

DIRECTIVE NIS 2

In order to remedy the deficiencies and obsolescence presented by its predecessor, the NIS 2 Directive incorporates the following as main axes of the regulations:



WIDE RANGE

NIS 2 expands its scope to include more digital sectors and services, covering a broader range of businesses and services considered essential to the functioning of society.



GREATER HARMONIZATION

NIS 2 promotes further harmonisation of cybersecurity measures across the EU to ensure a more consistent and uniform approach to protecting critical infrastructure and digital services.



FOCUS ON RESILIENCE

NIS 2 emphasises the need for Member States and businesses to develop capabilities to resist and quickly recover from cyber-attacks, thereby strengthening cyber resilience across the EU.



BOOSTING PROACTIVITY

NIS 2 focuses cybersecurity on the control and prevention of threats and risks, urging people to anticipate cyberattacks as the primary measure to avoid their consequences.



NEW THREATS AND TECHNOLOGIES

NIS 2 takes into account emerging threats and evolving technologies, such as artificial intelligence and the Internet of Things (IoT), and seeks to address the challenges they present to cybersecurity.



THIRD PARTY RISKS

NIS 2 integrates the obligation to control supply chain risks as one of the pillars of the effectiveness of any cybersecurity strategy. The idea that cybersecurity is no longer a matter for one person, both at the state and organisational level, is the key approach that fuels regulatory development. This implies that NIS 2 will have, due to the cascading effect, influence on a wider number of organisations than stipulated in its articles.



RESPONSIBILITIES AND PENALTIES

A very important new development is that, as soon as NIS 2 comes into force in the Member States, senior management and management teams may be held personally liable for their organisation's failure to comply with NIS 2. In addition, NIS 2 establishes a fine for non-compliance for essential entities of up to €10 million or 2% of the company's annual worldwide turnover. For important entities, the fine may be up to €7 million or 1.4% of the company's annual worldwide turnover.

NIS Directive 2

THE NEW EUROPEAN LEGAL
FRAMEWORK ON CYBERSECURITY



NIS DIRECTIVE 2:

SCOPE OF THE DIRECTIVE

It is estimated that this scope of application will be, in practice and as a consequence of the cascade effect, much broader than the strict stipulation in the Directive due to the obligation to control the risk of the supply chain that it imposes on the companies and sectors to which it is directed.

DIRECTIVE NIS 2

SCOPE OF THE DIRECTIVE

The scope of the NIS 2 Directive is broader and more comprehensive than that of its predecessor.

NIS 2 covers a range of digital sectors and services 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 eliminates the voluntary nature of the implementation of measures, requiring Member States to include them in their national regulations and companies to control, manage and monitor the risks and continue to improve resilience and response capacity.

DIRECTIVE NIS 2

SCOPE OF THE DIRECTIVE

REQUIRED ORGANIZATIONS

- **COMPANIES:**

Medium and large companies (more than 250 employees and an annual turnover of 50 million euros or more)

- **ADMINISTRATION:**

All Public Administrations (except Defence or national security, public security, police, judiciary and parliaments and central banks).

SECTORS COVERED

HIGH CRITICALITY

Eleven sectors considered essential for the functioning of society, of high criticality, to which the NIS 2 regulations are applied in a mandatory manner: Energy,

Banking, Financial Markets, Healthcare, Transport, Digital Infrastructure, Drinking Water, Wastewater, B2B ICT Services Management, Space, Public Administration.

CRITICS

Seven sectors considered critical for which the provisions of the NIS 2 Directive will also be mandatory:

Research, Chemistry, Food, Postal Services, Digital Suppliers, Manufacturing, Waste Management.

DIRECTIVE NIS 2

SCOPE OF THE DIRECTIVE

Classification of Entities

ESSENTIAL ENTITIES

Those belonging to highly critical sectors that exceed the maximum limits provided, as well as qualified providers of trust services and top-level domain name registries and DNS service providers, regardless of their size.

Providers of public electronic communications networks or publicly available electronic communications services that are considered medium-sized enterprises, public administration entities, any other entity belonging to other critical sectors that the Member State identifies as an essential entity, critical entities identified by the CER Directive, and, if so provided by the Member State, entities identified as operators of essential services in the previous NIS 1 Directive.

They will be required to comply with the monitoring requirements from the introduction of NIS 2.

IMPORTANT ENTITIES

Entities belonging 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.

They will be subject to ex-post supervision, meaning that measures will be taken when the authorities have received the evidence of breach.

NIS DIRECTIVE 2:

THE 5 GOOD PRACTICES OF CYBERSECURITY NIS 2

The NIS 2 Directive is based on a series of principles articulated through the establishment of good Cybersecurity practices: continuous evaluation, proactive mitigation, management and continuity, coordination and communication, transparent, and cyber hygiene and training.

DIRECTIVE NIS 2

THE 5 GOOD PRACTICES OF CYBERSECURITY NIS 2

All of this, in order to assess its impact and probability of occurrence and to analyse the 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 establishes its obligation.

Proactive mitigation of detected risks and vulnerabilities.

Proactive mitigation of risks and vulnerabilities is a core element of the NIS 2 Directive, as it focuses on preventing and reducing the impact of potential cyberattacks rather than simply responding to them after they occur. Once risks and vulnerabilities have been detected through continuous assessment, security measures must be adopted in accordance with the identified risk levels. This may include applying stricter access controls, regularly updating software and systems, using data encryption, active network monitoring, requiring remediation and cybersecurity scoring for the supply chain, or implementing robust security protocols, among others. In other words, action must be taken before the attack materializes in order to prevent it or, at least, prevent it from having consequences.

Continuous assessment of risks and vulnerabilities.

The continuous assessment of risks and vulnerabilities underpins the proactive and preventive approach to strengthening Cybersecurity in the EU and is the first stone in building the Cybersecurity strategy. It involves developing a corporate Cyberintelligence strategy that allows potential threats to be identified and monitored.

NIS Directive 2

THE 5 GOOD PRACTICES OF
CYBERSECURITY NIS 2

Resilience Objective

Best practices, key points and compliance with NIS 2

Crisis management and business continuity.

The first objective is to prevent the cyber attack from happening, but in the event that it is unavoidable, the NIS 2 Directive establishes the need to develop effective crisis management procedures to ensure maximum operational continuity in the event of an incident. Organizations are required to develop well-defined incident response plans and procedures and to have them tested and updated. This ensures that, in the event of a cyber attack or security incident, there is a rapid and coordinated response to mitigate the impact and restore normal business operations as quickly as possible.

- Development of a detailed Crisis Management Plan with designation of roles and responsibilities, the sequence of actions to be followed and communication protocols with the competent authority and stakeholders.
- Development of a detailed Business Continuity and Recovery Plan focused in actions to maintain or restore operability within the acceptable time frame and ensure the continuity of essential services.
- Conducting tests and simulations to test the plans, verify their effectiveness,

familiarize workers with the procedure and identify areas for improvement.

- Collaboration with the 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.

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

NIS 2 stipulates that entities are required to notify the relevant authorities of any significant incident that occurs. Affected entities must follow a specific procedure:

- **Initial Notification – Early Warning:**
Within 24 hours of becoming aware of the incident, the entity must report it to the CSIRT or, failing that, to the designated Competent Authority.

NIS Directive 2

THE 5 GOOD PRACTICES OF
CYBERSECURITY NIS 2

- Interim Notification – Update:
After 72 hours from the detection of the accident, the entity shall update the state of the accident exposing one initial assessment.
- Final notification – Report presentation:
Within a maximum period of one month after notification of the incident, the entity must submit a final report containing a detailed description of the incident (including severity, impact, type of threat that caused the incident, mitigating measures applied and in progress and, if applicable, cross-border repercussions).

Furthermore, continuous, rapid and transparent communication on cybersecurity is promoted, both between Member States and between competent authorities and organisations or between interested or potentially affected parties, whether directly or indirectly. This exchange of information on vulnerabilities and incidents must be rapid, open and transparent.

Cyber hygiene and training.

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

- **Cyber-hygiene:**
Cybersecurity practices and habits that users should follow to protect their devices and data. This includes using strong and unique passwords, regularly updating software and applications, enabling two-factor authentication, being cautious when clicking on links or downloading files, and using secure Wi-Fi networks.
- **Training and awareness**
in cybersecurity to users and staff of organizations. Companies are responsible for training their employees to identify and report potential security incidents, as well as to follow established security procedures.
- **Education:**
NIS 2 advocates for the inclusion of cyber hygiene in educational curricula. Teaching basic cybersecurity skills from an early age is essential to raising a generation of more aware and confident users in the digital environment.
- **Raising public awareness on the importance**
of cybersecurity through awareness and communication campaigns on cybersecurity issues.

NIS Directive 2

THE 5 GOOD PRACTICES OF
CYBERSECURITY NIS 2

NIS DIRECTIVE 2:

KEY ELEMENTS OF NIS 2

- INNOVATION, AI AND AUTOMATION
- EMERGING THREATS AND ADVANCED TECHNOLOGIES
- DATA PROTECTION
- SUPPLY CHAIN
- FIGURE OF THE CISO
- LINKED ORGANISATIONS

Resilience Objective

Best practices, key points and compliance with NIS 2

INNOVATION, AI AND AUTOMATION

NIS 2 establishes an obligation for Member States to encourage the use of all innovative technologies, including artificial intelligence, that can improve the detection and prevention of cyberattacks, allowing resources to be more effectively diverted towards combating them.

To this end, research and development activities aimed at facilitating the use of these technologies, particularly those relating to automated or semi-automated tools in the field of Cybersecurity, will be promoted within the National Cybersecurity Strategies, and, where appropriate, the exchange of data necessary to train users of these technologies and improve them.

EMERGING THREATS AND ADVANCED TECHNOLOGIES

The NIS 2 Directive takes into account cyber threats and evolving technologies such as AI, the Internet of Things (IoT) and 5G networks.

This ensures that legislation is up-to-date and relevant to current and future challenges in the field of Cybersecurity.



DATA PROTECTION

The NIS 2 Directive encourages the full use of the principles of data protection by design and by default, as well as more advanced security and privacy protection measures, such as pseudonymisation and encryption, to protect personal data.

It also provides 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 minimisation, fairness and transparency, and data security, such as advanced encryption.

RELATED ORGANISATIONS

Competent Authorities:

Appointed 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 administrations.



NIS Directive 2

KEY ELEMENTS OF NIS 2

Resilience Objective

Best practices, key points and compliance with NIS 2

SUPPLY CHAIN

NIS 2 establishes an obligation to address cybersecurity risks arising from an entity's supply chain. The relationship with suppliers is particularly important due to the prevalence of incidents where entities have been victims of cyberattacks and where malicious actors have been able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Small and medium-sized enterprises are increasingly experiencing supply chain attacks due to their less stringent cybersecurity risk management and attack handling measures and 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 within larger attacks against the entities they have supplied. The Directive therefore also calls on Member States to assist small and medium-sized enterprises in meeting the challenges they face in their supply chains through their National Cybersecurity Strategies.

FIGURE OF THE CISO

The NIS 2 Directive establishes the obligation for companies to which it is addressed to have a Security Manager, a duly qualified and exclusively dedicated person who manages corporate Cybersecurity and forms part of the management.

It represents a great opportunity for CISOs to strengthen their position, as NIS 2 introduces the notion of management responsibility for managing cybersecurity risks, as well as strong penalties for violators.

NIS 2 requires essential and important entities to establish a proactive approach to risk management and the protection of critical data and systems, which implies that the CISO adopts the role of guide and leader in the technical and business decisions that must be made, as well as disseminator of Cybersecurity policies.

kartos[®]

CSIRT: Crisis Response Teams

Computer Security Incident Response Teams that will provide assistance to critical and important entities affected by any incident and disseminate alerts, warnings and information about cyber threats, vulnerabilities and incidents among 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) for the exchange of information on incidents, threats...

Cooperation Group: Formed by

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

European Cybersecurity Crisis Liaison Organisation Network (EU-CyCLONe):

Formed by the Cybersecurity Crisis Management Authorities of the Member States and the Commission, it will have an observer role in the event of cyber incidents likely to have a significant impact on the services and activities included in the NIS 2 Directive, supporting the coordinated management of large-scale cybersecurity incidents and crises.

NIS Directive 2

KEY ELEMENTS OF NIS 2

NIS DIRECTIVE 2:

NIS 2 COMPLIANCE: BENEFITS OF EXTERNAL SURFACE MONITORING

Much of the innovation of the NIS 2 Directive is based on the concept of Cyber Threat Intelligence: monitoring, discovering, analyzing and controlling both internal and third-party risks to implement a Cybersecurity strategy, proactive in the organization.

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

Continuous, automated monitoring of leaked information and other surface threats

(Internet, Dark Web and Deep Web) using Artificial Intelligence (AI), can play an important role in organizations' compliance with the European NIS 2 Directive. 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 an ever-evolving digital environment.

The concept of a 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 look for them. This includes public websites, repositories, forums, marketplaces, servers, databases, network-connected devices, and any other digital resource accessible from the public web.

NIS Directive 2

NIS 2 COMPLIANCE: BENEFITS OF EXTERNAL SURFACE MONITORING

DIRECTIVE NIS 2

NIS 2 COMPLIANCE: BENEFITS OF EXTERNAL SURFACE MONITORING



IDENTIFICATION OF OWN THREATS AND VULNERABILITIES

Continuous and automated monitoring of the corporate external surface allows companies 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 login credentials, or vulnerability details are detected, the monitoring system alerts the security team to take immediate action to negate the risk.



COMPLIANCE WITH INCIDENT REPORTING

The NIS 2 Directive establishes an obligation for essential entities and important entities to report significant incidents to the competent authorities. Continuous and automated monitoring of the external attack surface facilitates the early detection of vulnerabilities and incidents and the collection of relevant information to meet the reporting deadlines set out in the Directive.



PROACTIVE INCIDENT RESPONSE

Continuous, real-time monitoring, coupled with the use of AI technologies, enables the automation of the identification and categorization of risks and vulnerabilities on the corporate external surface and the detection of the breach that caused them. This facilitates the prioritization of responses and the allocation of appropriate resources to address the most critical vulnerabilities in real time. By proactively detecting security breaches, organizations can act before significant damage is done, reducing the success and impact of attacks and improving their ability to recover.

NIS Directive 2

NIS 2 COMPLIANCE: BENEFITS OF EXTERNAL
SURFACE MONITORING

DIRECTIVE NIS 2

NIS 2 COMPLIANCE: BENEFITS OF EXTERNAL SURFACE MONITORING



ANALYSIS OF TRENDS AND ATTACK PATTERNS

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



PROACTIVE EVOLUTION OF SUPPLIER SECURITY

Continuous AI monitoring of the external attack surface also enables a proactive, non-intrusive assessment of the cybersecurity status 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 suppliers is assessed to determine if they comply with the requirements of the NIS 2 Directive. 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 particularly effective at detecting emerging threats and sophisticated attack 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 cyberthreats.

NIS Directive 2

NIS 2 COMPLIANCE: BENEFITS OF EXTERNAL
SURFACE MONITORING



AI layer that enables 100% automated operation without human intervention anywhere in the process.

Continuous operation 365x24x7, which allows for the detection of leaks of new information practically in real time.

Strictly non-intrusive tool. The Research is carried out on the Internet, the Deep Web and the DarkWeb and does not attack the IT perimeter of organizations, so its operation and the information obtained strictly comply with the limits imposed by legislation.

Maximum ease of use. Does not require No complex configuration. Simply enter the domain into the platform and it works autonomously, without the need to configure search parameters or any other information location criteria.

The only platform that analyzes the **conversations on social networks from the perspective of threat detection and attacks**, beyond those related to reputation and branding.

Automated, objective and continuous monitoring of the risks caused by third parties, that belong to the external surface of the organization

5 FEATURES on a single platform

Kartos Corporate Watchbots is the Continuous Threat Exposure Management (CTEM) platform developed by Enthec to extend the security perimeter controlled by organizations. Kartos provides companies with all the information that cybercriminals have about them so that they can improve their defense against various types of attacks.

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

Detecting contextual information about potential attackers, their tactics and processes for carrying out malicious activities. Eliminating malicious activities on behalf of the organization.

THIRD PARTIES

Management, assessment and control of the risk in the value chain throughout the duration of the business relationship, through objective data obtained in real time in an automated, continuous and non-intrusive manner.

COMPLIANCE:

Control and management of corporate and third-party legal compliance based on objective data obtained in real time in an automated and continuous manner.

SECURITY RATING SERVICES

Independent assessment of own and third-party risks, for a broad view of the cybersecurity maturity of any organization. Extension and weighting of the information provided by traditional third-party risk assessment methods.

Analysis of 9 Threat Categories

- DNS
- Health/Phishing
- Patch Management
- IP Reputation
- Web Security
- Email Security
- Document Leaks
- Credential Leaks
- Social Networks


Learn more about our licenses.
Try our tool for free.
Start using Kartos and become NIS 2 compliant


hello@enthec.com

#WeAlreadyKnow

ENTHEC[®] 

 @enthec

 @enthecsolutions

 @enthecsolutions

 kartos[®]