TEHTRIS NIS2 GUIDELINES

DECODING NIS2:
IS YOUR COMPANY TRULY IMPACTED?

www.tehtris.com

TEHTRIS
FACE THE UNPREDICTABLE

WHY?

Boosting the level of cybersecurity in the European Union, across companies and the entire supply chain, is the objective of the latest NIS2 directive.

Modernizing the existing legal framework to keep up with an increased digitization and an evolving cybersecurity threat landscape, this regulation expands the scope of cybersecurity rules to new sectors and entities, further improving the resilience and incident response capacities of public and private sectors, competent authorities, and the EU as a whole.

TEHTRIS decodes for you NIS2 directive:

Simpler than you think! Your company could be already ahead of the game.

Table of Contents

NIS2 IN A NUTSHELL

NIS2 aims to enforce a higher level of security for EU networks and information systems through various measures.

It has expanded its list of sectors covered by NIS2 from 8 to 18. These measures includes:

ENHANCED NATIONAL CYBERSECURITY FRAMEWORKS:

Requires EU member states to **strengthen their current national cybersecurity infrastructures** and **establish dedicated authorities and response teams.**

STRINGENT SECURITY MEASURES:

Imposes on companies in critical sectors **stronger security measures (23 new security rules)** and the **obligation to report incidents**.

CROSS-BORDER COLLABORATION:

Stresses better cooperation and **sharing info among EU countries** for dealing with cyber threats.

INCREASED ENFORCEMENT AND PENALTIES:

Introduces stricter supervisory measures, including the power for national authorities to **impose fines** and **conduct audits** to ensure compliance.

TEHTRIS GUIDELINES

This guideline aims to:

1. Identify if your company is impacted by NIS2 regulations

2. Explain the easy way to be compliant

3. Share solutions and use cases to ensure compliance and operational continuity for every industries

Understanding NIS2: Are You Affected?

While not universal, the NIS2 directive targets specific entities. It focuses on organizations with **sales exceeding €10 million** or those employing **more than 50 employees in selected sectors**.

Essential Entities** (EE)

+250 +50M€

- Energy*
- Transport
- Water*
- Financial Market
- Public Administration
- DNS Provider
- Managed services
- Digital Infrastructure
- Health
- Space

Important Entities** (IE)

+50 +10M€

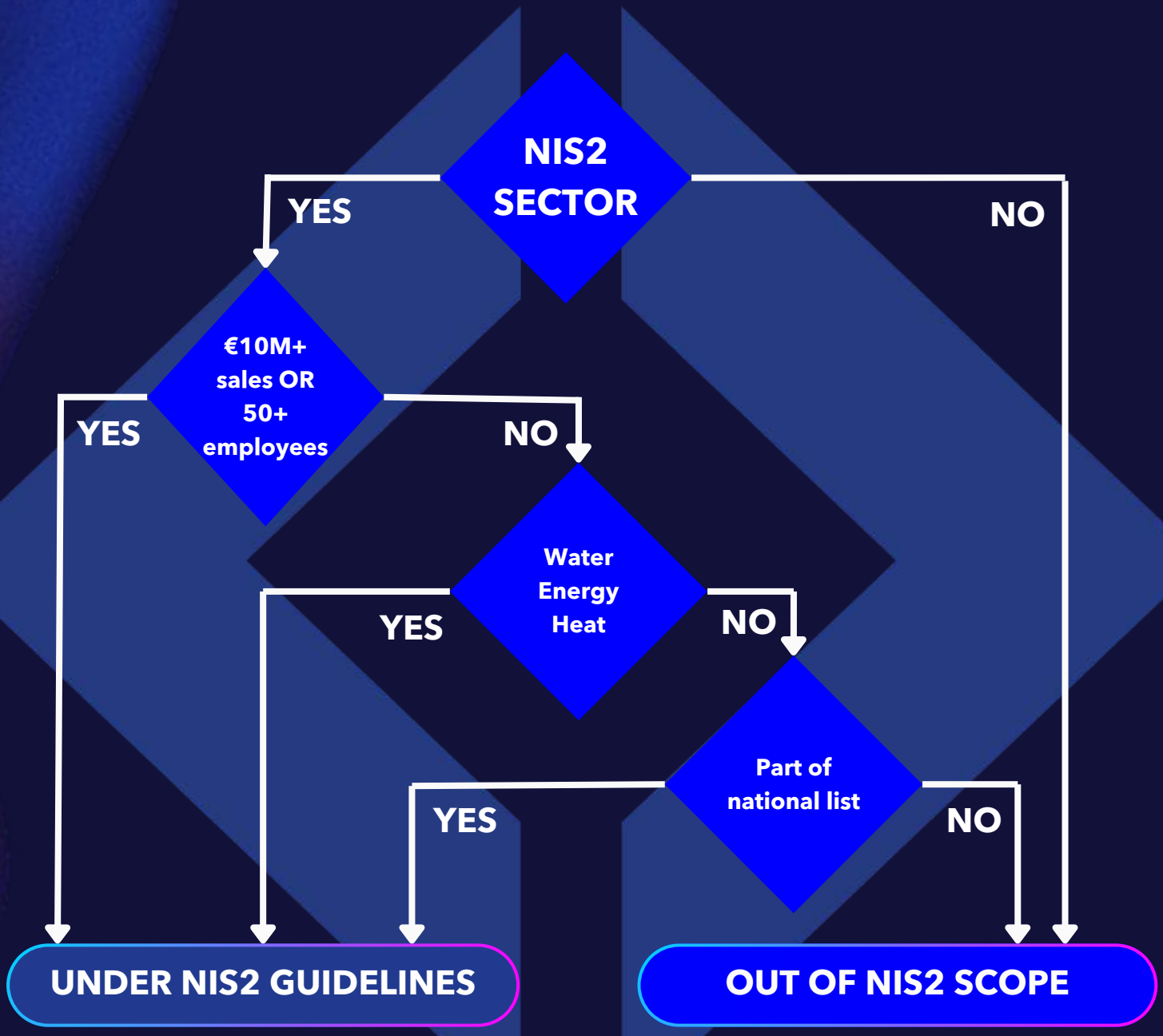
- Postal
- Waste
- Pharmaceuticals
- Chemicals
- Manufacturing
- Food Production
- Digital Providers
- Research

*Energy, water and heating companies under 50 employees are still subject to the NIS2 guidelines.

**Any entity from the above sectors with 50 to 250 employees and/or between €10M and €50M in annual sales is considered critical and subject to heavier penalties.

Understanding NIS2: Are you affected?

Who's on the National lists? Follow the diagram to check if NIS2 impacts your structure:



Understanding NIS2: Are you affected?

Each EU member compiles a list of crucial entities for NIS2, regardless of whether they fully meet criteria.

Some entities are afforded additional time to adapt as these lists are finalised after NIS2 starts.

See timeline below for detail:

Dec 14th, 2023

NIS2 adoption

Oct 18th, 2024

NIS2 enters into force in all EU countries

Apr 17th, 2025

Every EU member releases its national list of IEs and EEs

Be Compliant with Ease

If you opt for a European-based cybersecurity vendor offering NIS2 compliant products, the vendor assumes the following responsibilities, ensuring peace of mind for you:

EU-based cybersecurity vendors

- **Transparency on solution and product offerings**
- **Company compliance with NIS2 and GDPR**
- **Conformance to ISO, PSSI, PQS, PAS standards, along with regulatory contract monitoring**
- **Providing documentary audits and audit reports**
- **Historical compromise tracking PSSI compliance questionnaire**
- **No use of Meta data**

Non-EU based cybersecurity vendors

- **Vendor solutions and products MUST adhere to NIS2 requirements**
- **The vendor MUST appoint an EU-based representative office responsible within the EU**
- **Historical compromise tracking MUST be provided.**
- **Meta data CAN be used**

When a European business or public organization under NIS2 guidelines uses solutions from an EU cybersecurity vendor, **it shifts responsibility to the vendor,** ensuring compliance and implementation of all requirements, saving time for the customer.

However, opting for a non-EU-based vendor means **your Meta data can be used**, implying that your **data may be at risk** of exposure or misuse.

NIS2 Non-Compliance: Consequences & Sanctions

CEOs Accountability:

- Temporary or permanent **ban from business leadership**
- **Jail time** of up to 6 months in certain countries
- **Suspension** of certifications and authorizations for organizational activities

Monetary Penalties:

- Essential Entities (EE): up to **€10M** or 2% of worldwide annual sales
- Important Entities (EE): up to **€7M** or 1.4% of worldwide annual sales

Double sanctions:

- NIS2 and GDPR: **sanctions do cumulate**

Be Compliant with Ease

Simplifying NIS2 Compliance with TEHTRIS Solutions

As organizations adhere to NIS2 guidelines, the choice of cybersecurity vendor holds significant weight. **Opting for an EU-based vendor transfers responsibility** to ensure compliance and implementation, **saving time for the customer.**

However, **opting for a non-EU-based vendor** means **your metadata can be used,** implying that your data may be at risk of exposure or misuse.

TEHTRIS has meticulously decrypted NIS2 requirements, providing tailored solutions for each NIS2 measure, across various themes like:

- **Governance**
- **Third party management**
- **Incident management**
- **Data security**
- **Identity, Access and Asset Management**
- **Artificial Intelligence use-case**

Additionally, while NIS2 does not explicitly address AI, **TEHTRIS addresses ethical and privacy concerns with its Artificial Intelligence use-case solutions.**

In the following pages, we'll delve into each NIS2 requirement, provide you TEHTRIS solution for each measure, to guide your organization towards seamless compliance and enhanced cybersecurity posture.

Prepare for NIS2 with TEHTRIS:

A TEHTRIS solution for every NIS2 measure:

Governance

Key facts and requirements:

- **Define ambition and vision**
- **Define a Risk Management Policy**
- **Define an Information System Security Policy:**
  - Business continuity
  - Third Parties Management
  - Incident Management
  - Vulnerability Disclosure
  - Secured Architecture
  - Identity Access and Asset Management
  - Data security
  - Secured communication
  - AI usages

TEHTRIS solutions:

- **TEHTRIS Information Security Policy**
- **TEHTRIS Insurance Security Plan**
- **TEHTRIS ISO27001 Certification**
- **TEHTRIS GAFAM free hosting**

Prepare for NIS2 with TEHTRIS:

A TEHTRIS solution for every NIS2 measure:

Third Party Management

Key facts and requirements:

- **Manage Risk through ISP applications by the Third Parties:**
  - Request Third Party ISP
  - Request Audit
  - Request Incident Disclosure
- **Software Security Design**

TEHTRIS solutions:

- **TEHTRIS Information Security Policy**
- **TEHTRIS Incident Management Policy**
- **TEHTRIS Data Protection Policy / DPO + GDPR**
- **TEHTRIS Vulnerability Management Policy**
- **TEHTRIS Insurance Security Plan**
- **TEHTRIS ISO27001 Certification**
- **TEHTRIS Application Security Testing plan (pentest...)**
- **TEHTRIS Certified Hosting provider (ISO, Secnumcloud, PCI-DSS, ...)**
- **TEHTRIS OT integration plan readiness & retex**

Prepare for NIS2 with TEHTRIS:

A TEHTRIS solution for every NIS2 measure:

⚠ Incident management

Key facts and requirements:

- **Define an Incident and Crisis Management Policy**
- **Implement tools to detect attacks and raise alerts**
- **Secured Communication Crisis**

TEHTRIS solutions:

- **Reduced MTTD: TEHTRIS XDR AI PLATFORM with 3 pillars to detect / qualify**
  - Endpoints: XDR/EDR / XDR/EPP / XDR/MTD
  - Data: Investigation Toolkit / XDR/SIEM / XDR/Threat Intel / Sandboxes
  - Network: XDR/NTA / DR
  - Alerts Handling: eGuardian Artificial Intelligence sort out, ticketing
- **Reduced MTTR: TEHTRIS XDR AI PLATFORM to react**
  - TEHTRIS XDR/EDR / XDR/EPP automated / manual actions: Kill, Quarantine, Isolate, Remote script executions
  - TEHTRIS XDR/SOAR based response with any third-party tools
- **TEHTRIS XDR/MTD secured & encrypted push notification for emergency communications without adherence with traditional IT solutions**

Prepare for NIS2 with TEHTRIS:

A TEHTRIS solution for every NIS2 measure:

Data security

Key facts and requirements:

- Define a Data Security Policy
- Define an Encryption Security Policy

TEHTRIS solutions:

- TEHTRIS GAFAM free hosting
- TEHTRIS SECNUMCLOUD / C5 hosting
- Data encryption by default: TEHTRIS XDR Storage and Transport
- TEHTRIS Customers enable or not the access to their business data to their SOC, TEHTRIS...
- TEHTRIS Identity Management Module with RBAC
- TEHTRIS actions traceability module

Prepare for NIS2 with TEHTRIS:

A TEHTRIS solution for every NIS2 measure:

Identity, Access and Asset Management

Key facts and requirements:

- **Define a IAM Policy**

TEHTRIS solutions:

- **TEHTRIS Identity Management Module with RBAC**
- **TEHTRIS Information Security Policy – regular access review**
- **TEHTRIS actions traceability module**
- **TEHTRIS Asset Discovery (EDR)**
- **TEHTRIS Asset Inventory (XDR)**
- **TEHTRIS Software Inventory**

Prepare for NIS2 with TEHTRIS:

A TEHTRIS solution for every NIS2 measure:

Artificial Intelligence use-case

Key facts and requirements:

- **Promote a fair use of AI based on:**
  - **Equity**
  - **Management of potential Biases**
  - **Model Transparency**
  - **Model Explicability**
- **3 Keys criteria**
  - **Ethics**
  - **Confidence / Trust ability**
  - **Reliability**

TEHTRIS solution:

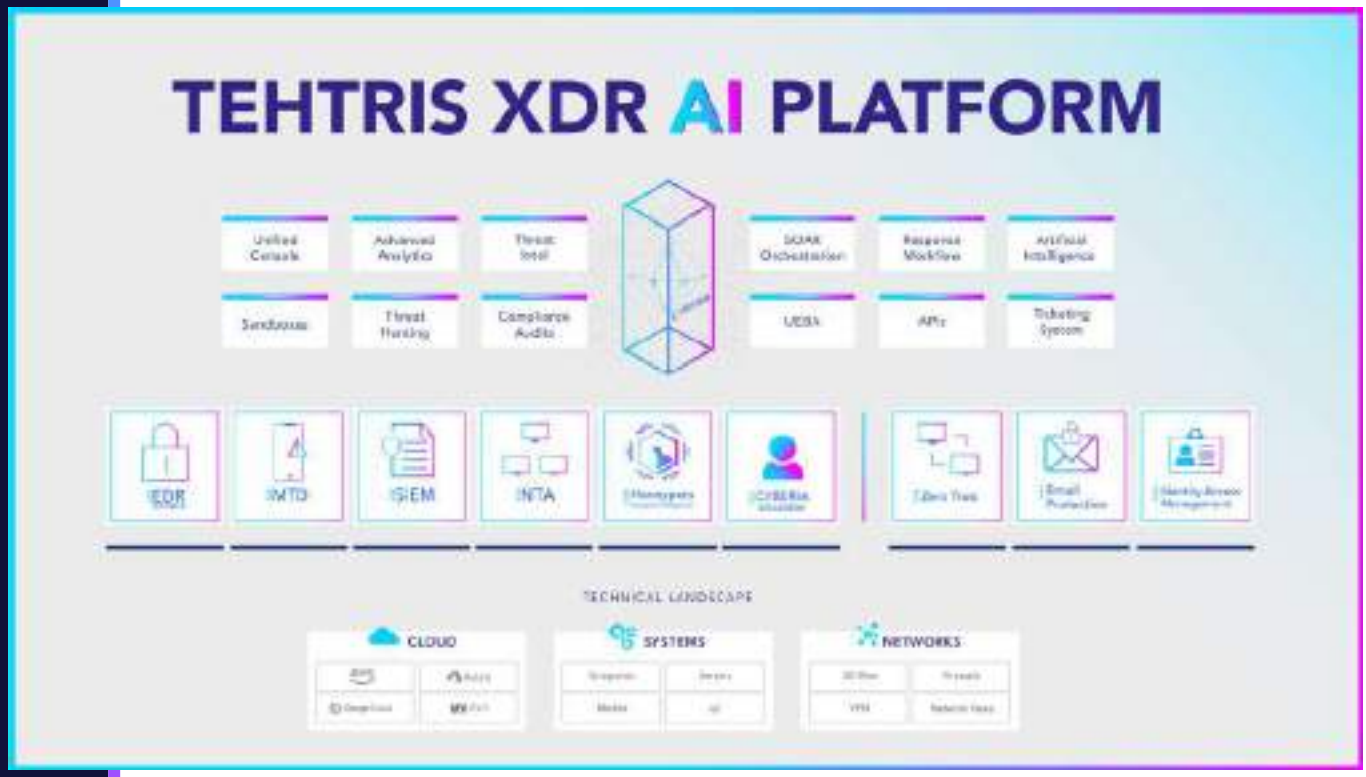
- **Ethical and Privacy by design and by defaults TEHTRIS AI Cyberia**
- **TEHTRIS AI training done under human supervision / validation**
- **TEHTRIS AI model explicability for human understanding**
- **TEHTRIS is not a data broker**

TEHTRIS SOLUTIONS

TEHTRIS XDR AI PLATFORM

A single console for global orchestration and security

Unify your cybersecurity by bringing together all your solutions in a single console for high-speed detections and responses. Within the TEHTRIS XDR AI PLATFORM, you will find an XDR/EDR, XDR/MTD, XDR/SIEM, XDR/Honeypots, XDR/NTA, XDR/CYBERIA, XDR/Threat Intel, XDR/Zéro Trust Response, XDR/Email Protection and XDR/Identity Access Management.



Orchestrate all your cybersecurity tools simultaneously, including your existing solutions such as Zscaler and Proofpoint, with the TEHTRIS XDR AI PLATFORM. Our platform is available in our secured cloud or on-prem. Easily deploy it in your ecosystem with in & out APIs. With its customizable playbooks and its hyperautomation capabilities you will get immediate response to cyberattacks.

TEHTRIS SOLUTIONS

TEHTRIS XDR / SOAR

Orchestrate all your solutions and enable Hyperautomation at the service of your teams

Saving time is essential when remediating attacks. In order to achieve this objective, TEHTRIS has designed its own SOAR. Perfectly integrated into the TEHTRIS XDR AI PLATFORM, our XDR/SOAR orchestrates the actions of your cybersecurity tools and automates them. Combined with TEHTRIS CYBERIA (TEHTRIS proprietary artificial intelligence), the detection, contextualization and response to incidents are hyperautomated.
Supported in its decision making and freed from repetitive tasks, your SOC gains decisive seconds during cyberattacks.
Interoperate your cybersecurity for augmented and hyperautomated remediation.

TEHTRIS XDR / THREAT INTELLIGENCE

Our Threat Intelligence for real-time neutralization

Our Threat Intelligence is directly integrated into the TEHTRIS XDR AI PLATFORM, giving you full visibility on all available threats. Our cybersecurity solutions are systematically linked to the TEHTRIS XDR/Threat Intelligence. As soon as a cyberattack is attempted, the TEHTRIS XDR/Threat Intelligence analyses, (also using our TEHTRIS AI Cyberia), to hyperautomate your responses to attacks for real-time neutralization without human action. You can subscribe to our TEHTRIS XDR/Threat Intel service on its own, or benefit from it automatically if you are a customer of a related TEHTRIS product. The knowledge base consultation is also available via API.

TEHTRIS SOLUTIONS

TEHTRIS XDR / CYBERIA

Enhance your cybersecurity with our artificial intelligence.

With Cyberia, you are protected from threats undetectable by humans.
Addressing the pressing challenges faced by cybersecurity experts, TEHTRIS has invested and developed its proprietary Artificial Intelligence: TEHTRIS Cyberia, a multi-modular AI and a cornerstone component of TEHTRIS XDR AI PLATFORM.
Overcoming cyber security workforce shortage and fatigue, TEHTRIS Cyberia is embedded through TEHTRIS XDR AI PLATFORM, offering hyperautomation of real-time detection, triage of every single alert, without compromise, remediation, without human intervention VS traditional approaches based on use-cases and filters creating blind spots: a safer alternative to cyber solutions currently offered on the market.

Meet NIS requirements with TEHTRIS solutions

TEHTRIS offers tailored cyber solutions for NIS2 readiness, fortifying defenses with advanced technologies. From endpoint detection to threat response, **TEHTRIS equips companies to proactively mitigate risks.**

Collaborating closely with the cyber community and boasting GDPR compliance and ISO 27001 certification, TEHTRIS ensures comprehensive NIS2 compliance, **empowering companies to navigate evolving cyber landscapes with confidence.**

ABOUT US

TEHTRIS, a mission-driven company, has been engaged since 2012 in the fight against cyber espionage and cyber sabotage as a provider of cybersecurity software.

With its «Zero Trust» approach and a unique «Security & Ethics by design» concept, TEHTRIS supports organizations of all sizes and sectors, guiding them to anticipate and confront the unpredictable and become exemplary guardians of their cyber space.

Deployed in over 120 countries, the TEHTRIS XDR AI PLATFORM stands out as the ultimate hyper-automated cybersecurity solution. By ensuring real-time detection and neutralization of cyber attacks, ransomware, and malicious behaviors without requiring human intervention, it also guarantees interoperability with market security solutions via its APIs.

Combining active protection from installation with deployment simplicity and continuous support from our experts, it provides users with a holistic view of their infrastructure while preserving the confidentiality of their data 24/7.
By continually enriching its Threat Intel database through globally deployed sensors, TEHTRIS ensures high-level contextual detection and prediction of security alerts, through behavioral analysis and its Cyberia Artificial Intelligence.

Compliant with all current regulations including GDPR and NIS2, TEHTRIS provides organizations with the confidence needed to address cybersecurity challenges, thus strengthening their defense posture against active and emerging threats.

Follow us on:

LinkedIn Twitter YouTube

<TEHTRIS>

FACE THE UNPREDICTABLE