Trellix

EU Network and Security directive NIS 2

An overview

Chris Hutchins
MD Public Policy EMEA
October 25th 2023

Why propose a NIS 2?

1. Digital transformation of society post COVID-19
2. the number of incidents in critical infrastructure growing
3. The evolving cybersecurity threat

- NIS I evaluation showed
  - Low level of cyber resilience of businesses operating in the EU
  - Inconsistent resilience across Member States and sectorse.g. differing designation of whether entities were in scope NIS (e.g., hospitals).
  - Low level of joint situational awareness and lack of joint crisis response

Changes brought by NIS 2

Expanded scope: NIS2, imposes security, incident notification, and governance obligations on entities in a range of critical sectors, including energy, transport, finance, health, and digital infrastructure

Merging of essential and important entities: Compliance requirements essentially the same, the supervision regime lighter for important entities and fines are set at a lower level.

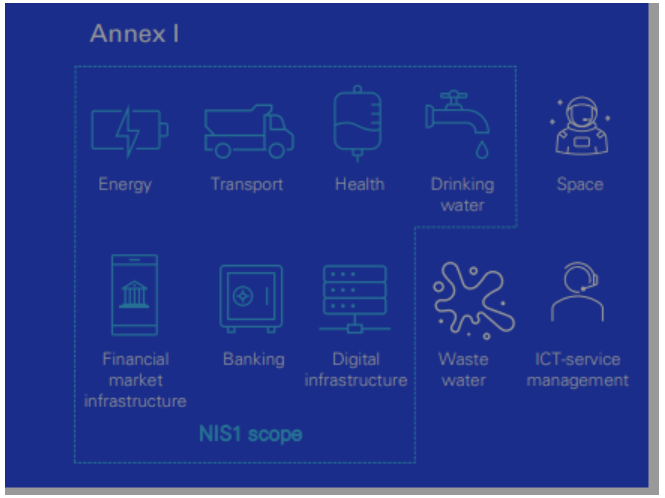
Stronger security governance measures: Senior management team is now accountable for the deployment of the security standards and risk management measures.

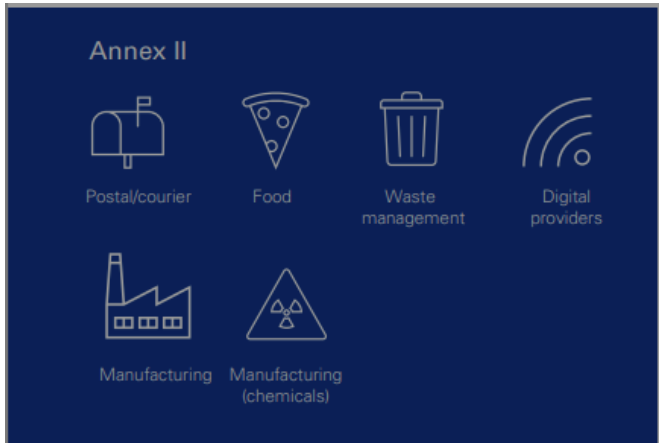
Expanded security measures: Covering risk management and governance obligations organization must implement, rather than the non-specific approach of NIS 1

Expanded incident reporting obligations: NIS 2 establishes a timeline and gives CSIRTs some additional powers, e.g., requesting follow-up reports.

What organisations are in scope?

- Both public and private entities
- Annex I lists the sectors of high criticality, which can be either an **Essential** or an **Important**
- If you are a large (>€50m annual revenue; 250+ Employees) or medium enterprise (>€10m annual revenue; 50+ Employees) in an annex I sector, you are deemed essential.
- But a national government can make *any organisation* essential based on its risk profile
- Annex II lists the other critical sectors, which will only fall into the Important Entity category





Trellix

Do the rules differ between important and essential organisations?

.

Critical organisations in annex I must up-level their governance, risk management and evaluate their incident reporting obligations

Essential operators are under **proactive supervision**, whereas important entities will only be monitored after an incident of non-compliance

But both organisations must now self-assess whether their services fall within scope of NIS2 and update their security controls and policies against NIS2 obligations.

In September the EU issued a template for companies to self-assess and declare their status to national authorities

NIS2 does not apply directly - Member States must transpose it into their national law by 18 October 2024.

Essential | Proactive supervision

- Annex I – Large enterprises[a]
- Qualified trust service providers, TLD name registries, DNS service providers
- Public administration entities
- Operators of essential services
- Operators of essential services (Directive 2016/1148)
- Member State selected entity

Important | Reactive supervision

- Annex I – Medium enterprises[b]
- Annex II – Medium & large enterprises
- Member State selected entity[c]

Trellix

Main requirements

Compliance obligations

- **Governance:** management body to approve cyber risk management plans; supervise implementation; be accountable and be properly trained.
- **Risk management:** Technical, operational and organizational measures to manage ICT risk and to prevent or minimize the impact of incidents on service recipients.
- **Reporting obligations:** notification without undue delay about incidents that have a significant impact on the provision of services – see next slide

Supervision and enforcement

- **Supervisory authorities can undertake a number of actions:** on-site inspection and checks; regular and targeted security audits; ad hoc audits; security scans; requests of information; data access requests; request to designate a monitoring officer;
- **They can impose remedies:** non-compliance warnings, binding instructions; order entities to be brought into compliance, to implement recommendations, to publish aspects of non-compliance; levy fines.
- **National authorities can impose fines** would be set at **EUR 10M or 2% of total worldwide annual turnover for essential** and **EUR 7M or 1.4% for important entities**

Trellix

Incident reporting and management responsibilities

4

Incident Notification

NIS2 imposes notification obligations in phases, for incidents which have a 'significant impact' on the provision of their services. These notifications must be made to the relevant competent authority or CSIRT (Computer Security Incident Response Team).

24h — EARLY WARNING
Is it a suspected malicious act with potential cross-border impacts?

72h — OFFICIAL INCIDENT NOTIFICATION
Assessment of the incident, severity and impact, plus indicators of compromise.

as requested — INTERMEDIATE STATUS REPORT
At the request of CSIRT or relevant competent authority.

1 month — FINAL REPORT
Or if incident ongoing at time of final report a progress report and final report 1 month after end

Where appropriate, entities shall notify the recipients of their services of significant incidents.

When in the public interest, the CSIRT or relevant competent authority may inform the public about the significant incident or may require the entity to do so.

8

Management Responsibilities

Senior management have ultimate responsibility for cybersecurity risk management in essential and important entities. Failure by management to comply with NIS2 requirements could result in serious consequences, including liability, temporary bans and administrative fines as provided for in the implementing national legislation.

Management bodies of essential and important entities must:

- **Approve the adequacy** of the cybersecurity risk management measures taken by the entity;
- **Supervise the implementation** of the risk management measures;
- **Follow training** in order to gain sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact on the services provided by the entity
- **Offer similar training to their employees** on a regular basis;
- **Be accountable** for the non-compliance

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications
NCSC National Cyber Security Centre

Trellix

Next steps

NIS 2 does not apply directly so Member states will now begin to transpose NIS2 into their national - October 18, 2024 is the deadline for transposition.

Before NIS2 comes into force, companies will need to:

1. assess whether they provide any services or conduct any activities that are captured by the Directive
2. begin assessing their security controls and preparing amendments to their security, risk management and incident response policies to achieve compliance with NIS2;
3. "flow through" new security controls and incident response obligations to their suppliers given the explicit requirement in NIS2 to address supply chain risk and the new incident reporting obligations.

Trellix

NIS 2 Solution Mapping

Oliver Stuck
Senior Solution Engineer
October 25, 2023

NIS II critical requirements

Recap

Article 20 Governance:

- Management body to approve cyber risk management plans; supervise implementation; be accountable and be properly trained.

Article 21 Risk management:

- Technical, operational and organizational measures to manage ICT risk and to prevent or minimize the impact of incidents on service recipients.

Article 23 Reporting obligations:

- Notification without undue delay about incidents that have a significant impact on the provision of services, including information for national CSIRTs to assess cross-border impact of an incident.

Trellix

Base Security

All you need for your basic security

Endpoint Security, Endpoint Firewall, Endpoint Web Control

- Windows, Linux and MAC OS

Integrity Control – Integrity Monitoring, Change Control & Application Whitelisting

- Supporting legacy OS´s & OT & PCI DSS and SWIFT and more

Data Loss Prevention

- DLP Endpoint incl. Device Control, DLP Network – Discover, Prevent & Monitor
- Last line of defense

NIS II requirements on governance and risk management

- Visibility to end-point, firewall and web control establishes a first assessment of your organisations risks.
- Assist in driving governance and risk management, conversations and ensuring disaster recovery and business continuity
- Also supports patch and vulnerability management and remote access security
- Also, a “must have” for GDPR, DORA, etc.

Trellix

Advanced Security

SIEM Functionalities, EDR Functionality, and above

ePO ePolicy Orchestrator

- Centralized Management of Products, Policies, Reporting & Infrastructure available on Prem or as SaaS

Trellix EDR

- OnPrem or SaaS - Endpoint Detection, Forensics, Hunting, Remediation

Trellix XDR

- Next Gen XDR for all Security Information's incl. SIEM Functionalities & EDR Functionalities
- Over 200 different Log Information's & Integration capabilities

Threat Intelligence

- Insights, Atlas, INT as a Service Threat Intelligence Sharing, ThreatQ, Insights

NIS II requirements – Incident reporting obligations

- Real time visibility into risks and incident across your estate's threat perimeter
- Advanced threat hunting
- Incidence & Response
- Manual & automated Remediation
- Latest threat intelligence feeds delivered
- Special Services

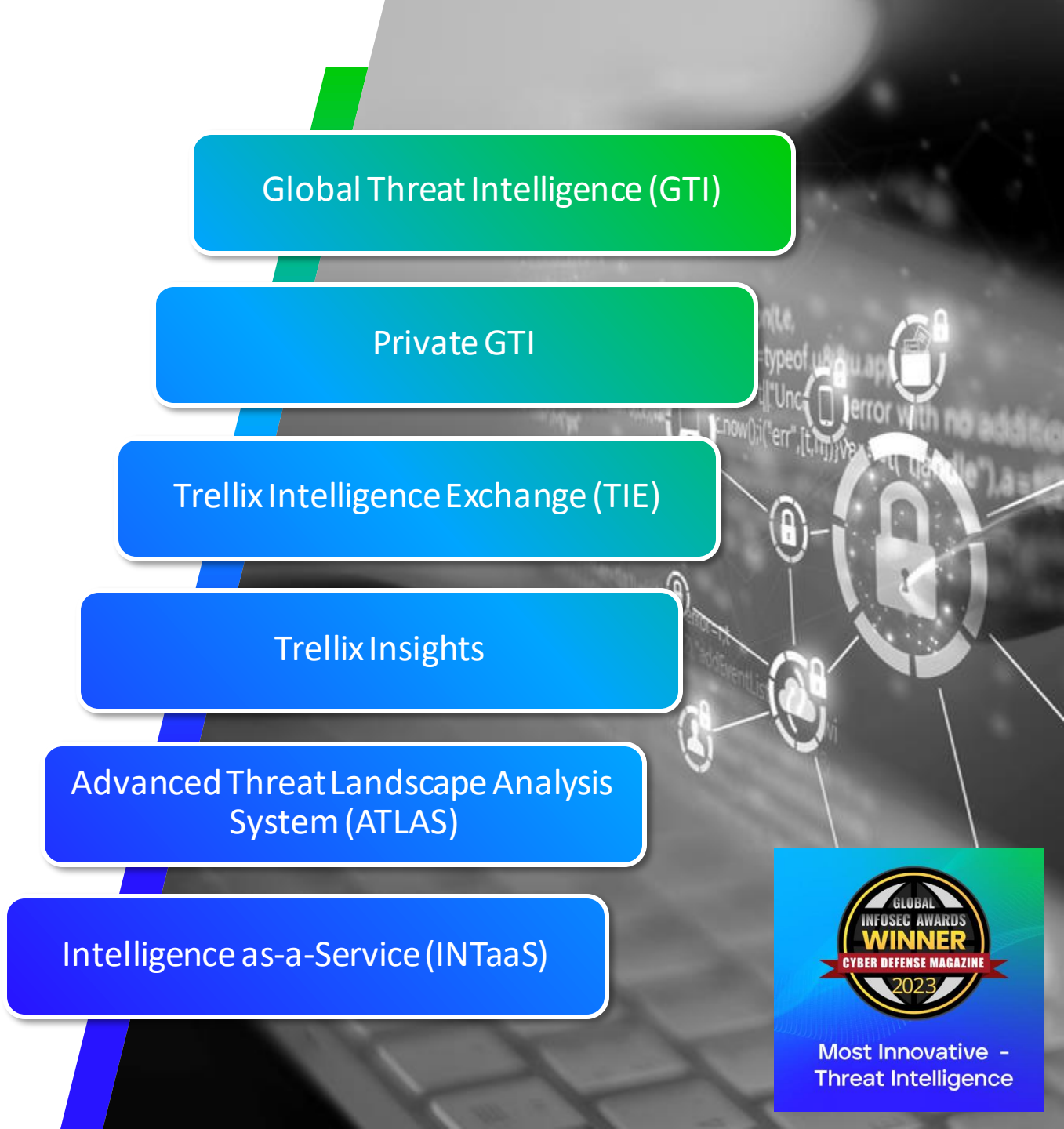
Trellix

Trellix Threat Intelligence Portfolio

Build a Strong Defense with Global Intelligence and Local Visibility

- Mission-critical insights 24/7
- Millions of sensors distinctly across key vectors (endpoint, email, web, & network)
- One of the broadest and deepest intelligence offerings on the market
- Critical context to prioritize and drive better comprehensive protection

https://www.trellix.com/en-us/platform/threat-intelligence.html



Trellix

Thank You!