eye.

NIS2 Incident Response Starter Kit.

A practical guide to 24h / 72h incident reporting readiness

Under NIS2, organisations must be able to detect, manage, and report significant cybersecurity incidents quickly and accurately. In practice, most organisations are missing only a few critical building blocks: clear ownership, a tested response process, and the ability to gather the right facts under pressure. This starter kit outlines a practical, minimum-viable approach to incident response readiness, helping you protect operations, meet NIS2 reporting timelines, and reduce business impact.

What NIS2 expects from you

NIS2 requires organisations to demonstrate that they can:

- ✓ Detect and respond to cybersecurity incidents
- ✓ Manage incidents as a business risk, not only a technical issue
- ✓ Provide early warning within 24 hours of becoming aware of a significant incident
- ✓ Submit a follow-up notification within 72 hours, with clearer facts and impact
- ✓ Coordinate technical, legal, and executive decision-making during incidents

Your 3-step action plan

Step 1

Assign clear ownership

Clear ownership prevents delays and confusion in the first critical hours. Before an incident happens, define who is responsible for:

- Incident leadership and coordination
- Technical investigation and containment
- Business and risk decisions
- Internal and external communications
- Regulatory reporting and documentation

Step 2

Create a minimum-viable incident response plan

An effective IR plan does not need to be long. The goal is clarity under pressure. We recommend that you keep a small, printed incident response plan that covers the basics:

- How incidents are detected and escalated
- Who decides whether an incident is significant
- Determine roles and responsibilities in case of an incident
- How containment and investigation are initiated
- How evidence and logs are preserved
- How information is gathered for 24h and 72h reporting

Step 3

Run one tabletop exercise

One tabletop exercise often reveals more than months of planning. Choose one realistic scenario, ransomware is the most effective starting point, and test:

- Who gets notified, and how fast
- Who makes decisions in the first hours
- What actions are taken in the first 4 hours
- What information would be available after 24 hours
- What gaps exist for the 72-hour notification

If you do only 5 things...

These five steps alone significantly reduce reporting risk and response chaos.

1. Assign an Incident Lead and a backup
2. Agree internally what qualifies as a "significant incident"
3. Prepare a 24-hour reporting facts checklist (what you need to know, not how to phrase it)
4. Ensure logs and identity activity are centralised and accessible
5. Test one scenario this month

Common gaps we see in practice

- No clear incident owner during the first hours
- Incident response plans that have never been tested
- Technical teams focus on recovery, while reporting data is missing
- Evidence is overwritten or unavailable when regulators ask questions
- Executives are unsure what decisions they need to make and when

How Eye Security supports NIS2 incident readiness

Eye Security supports organisations across Europe with real-world incident response and continuous detection, including:

- ✓ 24/7 detection and response via our European Security Operations Centre (SOC)
- ✓ Practical incident response planning aligned to NIS2 expectations
- ✓ Preparation for 24h and 72h reporting (what to collect, when, and from where)
- ✓ Hands-on investigation and containment during real incidents
- ✓ Strengthening foundational controls that reduce impact, downtime, and reporting stress

Let's talk about incident response planning and 24/7 monitoring.

About Eye Security

Eye Security helps small and medium-sized businesses identify cyber risks proactively and strengthen operational resilience. As one of Europe's leading MDR providers, the company blends advanced AI technology, expert guidance, and integrated cyber insurance into one cohesive solution. More than 800 organisations across Europe rely on this unified approach to safeguard their digital operations.

eye.security

Incident response hotline

Experiencing a cyber incident? Call the Eye Security Incident Response hotline at **+31 88 644 4898** (24/7 availability) or contact the IR team via email at **cert@eye.security** for non-urgent cases.

The information contained in this publication is provided for general informational purposes only and does not constitute any contractual or other form of commitment. While every effort has been made to ensure the accuracy and completeness of the content, Eye Security makes no guarantees regarding its correctness, completeness, or timeliness. Any liability, particularly for direct or indirect damages resulting from the use or non-use of this information, is excluded to the extent permitted by law. All service descriptions are subject to the applicable terms, exclusions, and conditions of the relevant contracts. This publication does not replace individual advice or contractual agreements.