CISO CHEAT SHEET:

# NIS2 Compliance Blueprint

## What NIS2 Means for CISOs

NIS2 is not a documentation exercise. It is a resilience and accountability mandate. For CISOs, it introduces three non-negotiable expectations:

- **Executives and boards are directly accountable** for cybersecurity risk management *(Article 20)*
- **Organizations must demonstrate operational cyber resilience**, not just prevention *(Article 21)*
- **Incident impact must be contained and provably minimized**, with formal reporting obligations *(Article 23)*

**In other words, the questions directed at CISOs are moving from:** *Do you have security controls?* **to** *Can you demonstrate that your controls actively limit damage when something fails?*

## Where Most Organizations Struggle Under NIS2

Across mid and large enterprises, NIS2 gaps consistently appear in the same operational areas:

**Uncontrolled lateral movement** inside internal networks

**Overreliance on perimeter defenses and endpoint detection** without internal enforcement

**Privileged access pathways** that exist but are not controlled at the network layer

**Legacy systems that cannot support** modern identity or MFA technologies

**Overscoped vendor and third-party access** into critical environments

**Incident response strategies** focused on detection, not containment

These gaps directly undermine NIS2 objectives around limiting propagation, preserving service continuity, and reducing systemic impact.

# NIS2 Operational Readiness Checklist for CISOs

Use this checklist to assess whether your organization can meet NIS2's expectations for containment, resilience, and accountability.

1

### Lateral movement is prevented

- We can block unauthorized east–west communication between systems.
- Attackers cannot move laterally after an initial compromise.

2

### Privileged access is enforced on the network

- Credentials can only be used on explicitly approved network paths, with MFA enforced.
- Service accounts and legacy systems are protected by enforced network controls.

3

### Containment is built into the environment

- Breaches are automatically contained without manual isolation or shutdown.
- Incidents do not disrupt large portions of the business; critical services remain operational.

4

### Third-party access is restricted

- Vendor and supplier access is segmented at the network level.
- External accounts cannot pivot into unrelated internal systems

5

### Controls are provable

- We can demonstrate, with evidence, how segmentation and access controls are enforced.
- We can clearly define the full scope of a breach for regulators and leadership.

# How Zero Networks Enables NIS2 Compliance

Zero Networks directly supports NIS2 priorities by addressing the areas where most organizations struggle:

**Prevents lateral movement at scale** through automated, identity-aligned microsegmentation

**Enforces privileged access for all systems,** including legacy environments, using network-layer MFA.

**Minimizes breach impact and blocks lateral movement** by containing threats to their initial point of compromise.

**Reduces supply chain and third-party risk exposure** by restricting external access pathways to only the systems and services explicitly required.

**Provides defensible visibility into access paths, segmentation boundaries, and containment zones,** supporting incident scoping, regulatory reporting, and executive accountability.

Rather than adding another monitoring layer, Zero Networks operates as a dynamic containment and enforcement layer inside the network, helping organizations demonstrate that they can actively limit propagation and operational impact – which is central to NIS2 compliance.