SOLUTIONS_

Simplifying NIS2 Compliance with Eclypsium

NIS2 is an EU cybersecurity directive that covers an incredibly broad set of services including but not limited to Energy, Transportation, Finance, Healthcare, and Digital Infrastructure. The legislation is designed to ensure that these critical services maintain a consistent set of minimum responsibilities when it comes to managing their risk and responding to security incidents.

As an EU *directive*, NIS2 requirements are translated into each member state's national law, with each country having a requirement to enact their respective laws by 17 October 2024. Unlike some standards, NIS2 comes with considerable teeth, with non-complying organizations facing potential fines of between 1.4% and 2% of their global annual revenue.

ADDRESSING NIS2 REQUIREMENTS WITH ECLYPSIUM_

Complying with any regulatory standard requires a multi-disciplinary approach that goes well beyond the scope of any one security tool. However, Eclypsium offers a variety of unique capabilities that can help organizations address NIS2 requirements that would be missed by traditional tools or would require extensive effort from security and technical teams.

Specifically, Chapter 4, Article 21 of NIS2 defines 10 minimum requirements of cybersecurity risk management. Eclypsium directly applies to each of the first six requirements and provides an assortment of unique capabilities.

Supply Chain Security and System Acquisition

Like most modern security standards, NIS2 puts a strong focus on the security of the technology supply chain. Of the 10 minimum security measures, 2 are dedicated to the topic as follows:

- *(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;*
- *(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;*

Eclypsium is specifically designed to meet these challenges that are largely invisible to most security tools. Eclypsium knows precisely what should be in each asset down to the lowest levels of firmware code and actively audits the integrity and posture of every critical component and ensures that all available protections are enabled and properly configured. With a simple scan, teams can see exactly what components and suppliers are used in their assets, and verify that all code from the vendor and their many suppliers is intact and has not been tampered with in the supply chain. Similarly, Eclypsium proactively identifies any out-of-date code or low-level vulnerabilities, or misconfigurations that could put an asset at

risk. The simple automated nature of scans means organizations can easily evaluate prospective solutions before they are acquired and then also confirm that all delivered products conform to the vendor's SBOMs.

Risk Management and Incident Response

NIS2's minimum requirements also address several more common cybersecurity requirements such as detecting vulnerabilities and responding to security incidents. Eclypsium provides unique value in these areas as well with visibility into low-level firmware and components, enabling security teams to find risks and threats that would be missed by traditional scanners and EDR products.

Requirements	How Eclypsium Helps
(a) Policies on risk analysis and information system security	Automated scanning to proactively verify the integrity of all critical code and components, and to identify vulnerabilities, misconfigurations, or threats down to the firmware level of laptops, servers, and networking gear.
(b) Incident handling	Ability to alert or trigger automated responses based on any changes in system integrity. Allow analysts to assess systems for secondary exploitation or threat persistence using implants and similar methods.
(c) Business continuity	Reduce the risk of permanent damage to systems due to corruption of system firmware. Enable faster recovery by quickly verifying that affected systems are free of threats before being returned to service.
(f) policies and procedures to assess the effectiveness of cybersecurity measures	Assess and support threat detection tools by analyzing for threats and changes below the level of the operating system,

NEXT STEPS_

Like most cybersecurity regulations, NIS2 forces organizations to balance a variety of competing demands. Naturally, the quality of security is paramount, but teams must also ensure that they can meet their demands efficiently without overwhelming their staff. Eclypsium ensures teams can succeed on both fronts by simplifying some of the technical and time-consuming tasks of NIS2 into automated scans that find hidden problems and guide staff through the appropriate responses. To learn more about the Eclypsium solution and how it applies to NIS2 as well as other regulatory standards such as NIS2, please reach out to the Eclypsium team at info@eclypsium.com.