Contact us

Muninn & NIS 2

More Than Standard Cybersecurity

Recognizing shortcomings in NIS1, NIS2 focuses on improving cyberresilience and risk management across essential service providers, streamline cyberresilience through stricter security requirements and penalties for violations.

With the aim to increase efficiency to managing large-scale cybersecurity crises across the EU, member states are mandated to designate national authorities for cybercrisismanagement and companies are obliged to address a core set of minimum requirements in their cybersecurity policies.

Efficient Reporting

NIS2 will enhance and simplify cybersecurity and mandate organizations to incorporate multi-stage incident reporting approach, ensuring a balance between swift reporting for containment and comprehensive reporting for valuable insights. Affected companies must submit an early warning within 24 hours, an incident notification within 72 hours, and a final report within one month.

Muninn captures the packet data of your network activity, which allows you to efficiently report incidents on a high detail level. Create reports with all relevant information in no time using Muninn's Chain of Events and Muninn Report.

Risk Management

NIS2 states that organizations should use an all-hazards approach to address cyberrisks and introduces measures such as incident management, stronger supply chain security, enhanced network security, better access control, and encryption.

Muninn provides ongoing visibility into the use of potentially insecure encryption keys, such as insufficient use or low levels of SSL/TLS encryption. Muninn also generates notifications for the use of expired certificates on both internal and external servers.

Business Continuity

With the new Directive organizations need to strategize on how to guarantee the continuation of their business operations in the event of major cyberincidents. This strategy will have to include aspects such as recovering systems, implementing emergency protocols, and establishing an incident response team.

Muninn AI Prevent is a core element of your incident response, isolating the attacker, giving your team the time to take the next steps and preventing further damage. Increase efficiency with easy reporting based on detailed network traffic data.