sonatype

Putting NIS2 into Context

User's Guide to Compliance

Network and Information Systems Directive (NIS2)

The Network and Information Security Directive 2 (NIS2) is the European Union's updated cybersecurity legislation, developed to strengthen cybersecurity across the EU with a focus on critical infrastructure and essential services. NIS2 replaces the previous NIS Directive, introduced in 2016, and modernises the legal framework to keep pace with increased digitisation and evolving cybersecurity threats. This directive represents the EU's most comprehensive cybersecurity legislation, partly through strengthening the security posture of European software development but also by introducing stronger reporting requirements and penalties for failing to comply.

In this executive summary, we examine the key features of NIS2, what this new legal framework means for software developers, and how the Sonatype platform can help organisations proactively address regulatory challenges and enhance software development processes for a more secure and compliant future.

NIS2 is expected to go into effect on **October 17th, 2024**, and EU member states are required to adopt and publish measures to comply with its intended goals by that date. It also requires that businesses deemed essential by Member States in specified sectors must implement suitable security measures and report significant incidents to national authorities.

NIS2 is expected to go into effect on October 17th, 2024, and EU member states are required to adopt and publish measures to comply with its intended goals by that date.

The directive covers all companies that provide essential services and breaks them down into **Highly Critical** and **Critical Sectors**:

Highly Critical Sectors

>49 employees and an annual turnover exceeding € 10 million or a balance sheet total exceeding € 10 million

- **Transportation**
- **Water and Sanitation**
- **Energy Digital Infrastructure**
- **Banking**
- **Financial Markets**
- **Infrastructure**
- **Space**
- **Healthcare**

Critical Sectors

>249 employees and an annual turnover exceeding € 50 million or a balance sheet total exceeding € 43 million

- **Postal and Couriers**
- **Waste Management**
- **Chemical Industries**
- **Food and Nutrition**
- **Manufacturing**
- **Digital Service Providers**
- **Research**

The Sonatype Platform and NIS2

The vulnerability of **software supply chains** is central to NIS2 guidance, and like most EU-wide legislation, NIS2 provides a minimum framework that member states must adhere to but allows for flexibility in how it's implemented at the national level. Sonatype has been at the forefront of software supply chain management, including empowering developers and organisations to protect the integrity of their software components through automated cybersecurity hygiene practices like vulnerability scanning, dependency analysis, and policy enforcement. These strengths make Sonatype ideally suited to help manage the **minimum cybersecurity risk management measures and reporting obligations** outlined in **Article 21, Section 2** of NIS2.

These strengths make Sonatype ideally suited to help manage the minimum cybersecurity risk management measures and reporting obligations outlined in Article 21, Section 2 of NIS2.

These include:

a. policies on risk analysis and information system security;

b. incident handling;

c. business continuity, such as backup management and disaster recovery, and crisis management;

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;

f. policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

g. basic cyber hygiene practices and cybersecurity training;

h. policies and procedures regarding the use of cryptography and, where appropriate, encryption;

i. human resources security, access control policies and asset management;

j. the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate

To help individual countries address these broad requirements, the **European Union Agency for Cybersecurity (ENISA)** published guidance in its **Good Practices for Supply Chain Security** documentation. We believe these practices provide an excellent path forward for NIS2 compliance, and we've outlined how the Sonatype platform complies with its guidelines.

Good practices for vulnerability handling for operators of IT networks and operational infrastructure

Measure	Objective	Sonatype Capability
An inventory of assets should be drawn up and maintained that includes patch-relevant information	Enable product users to link reported vulnerabilities to respective assets.	**Sonatype Lifecycle** analyses software components and can scan SBOMs either as part of the application analysis or scan a standalone SBOM.
Information resources shall be used to identify relevant technical vulnerabilities	Monitor vulnerabilities, e.g. by scanning for advisories or by receiving vulnerability information from suppliers.	**Sonatype Lifecycle** continuously scans applications and sends notifications if new policy violations are discovered.
Evaluate the risks of vulnerabilities for the own operational environment and have a documented and implemented maintenance policy available.	Understand the risk of vulnerabilities and have a maintenance policy that defines treatment depending on the risk level.	**Sonatype Lifecycle** and **Sonatype Firewall** let you define and automatically enforce specific policies for open-source components.
Patches should be received from legitimate sources.	Verify the authenticity of software and mitigate supply chain and mitigate supply chain risks.	**Sonatype Nexus Repository** centralises access and **Sonatype Firewall** provides identification and protection from malware.
Patches should be tested before they are installed	Test compatibility and against malware.	**Sonatype Repository Firewall** protects against known and unknown threats.
Alternative measures should be evaluated in case patches are not available or applicable	Mitigate risks with additional measures, if necessary, e.g. closing of firewall ports etc.	**Sonatype Nexus Intelligence** provides universal and timely understanding of open source security, license, and architectural risk.
The patch deployment process needs to consider rollback procedures as well, e.g. an effective back-up and restoration process.	Ensure product availability in case a patch deployment fails by applying rollback options.	**Sonatype Nexus Repository** centralises patches, facilitating their management, version control, and efficient deployment across systems.

Good Practices for Supply Chain Security, June 2023
- European Union Agency for Cybersecurity

Good practices for vulnerability handling in product and component development

Measure	Objective	Sonatype Capability
A process shall be implemented for receiving and tracking to closure of security vulnerabilities reported by internal and external sources that includes used third-party components.	Monitor all used components for vulnerabilities and track them for closure; the measure implicitly requires having an asset list of used third-party components maintained.	**Sonatype Nexus Repository** provides continuous creation and monitoring of SBOMs for new vulnerabilities.
A process shall be implemented to analyse the risks of vulnerabilities in the context of the documented intended use and operational environment (if applicable) by using a vulnerability scoring system (e.g. the common vulnerability scoring system).	Understand the risks of vulnerabilities by using recognised practices for vulnerability scoring.	Out of the box, **Sonatype Nexus Intelligence** allows organisations to create custom policies for specific situations, prioritising vulnerabilities according to policy and CVSS.
A maintenance policy shall exist that defines the treatment of identified vulnerabilities depending on the risk	Define how vulnerabilities are treated depending on the risk level.	Out of the box, **Sonatype Nexus Intelligence** allows organisations to create custom policies for specific situations, prioritising vulnerabilities according to policy and CVSS.
A process shall be implemented for informing product users about vulnerabilities	Inform product users on vulnerabilities.	The **Sonatype platform** provides continuous monitoring and can send notifications when policy alerts occur.
A process shall be implemented to verify that a patch is addressing the respective vulnerability and that the patch does not contradict other operational, safety or legal constraints	Patches shall be qualified before a release.	The **Sonatype platform** features CI/CD scanning for generating new SBOMS and policy verification of releases for verifying that risks are mitigated.

Good Practices for Supply Chain Security, June 2023
- European Union Agency for Cybersecurity

NIS2 Reporting Obligations

In **Article 23**, NIS2 details **Reporting Obligations** that all member states must adhere to, including *filing a final report not later than one month after the submission of the incident notification under point (b), including the following:*

Final Report Obligations	Sonatype Capability
a detailed description of the incident, including its severity and impact;	**Sonatype Lifecycle** can search across impacted applications to quickly identify which applications are affected, and our policy engine can help you establish severity in the context of the applications.
the type of threat or root cause that is likely to have triggered the incident;	**Sonatype Nexus Intelligence** is presented around the vulnerability and helps you establish the issue, applicability, remediation steps and potential impact of the issue
applied and ongoing mitigation measures;	Policy engine and up-to-date SBOMS can help you prove mitigation via waiver descriptions or replacement of the offending components **Recommendations for better versions in context**, including when the issue is a transitive vulnerability Waiver descriptions keep information with the application SBOM
where applicable, the cross-border impact of the incident;	

Optimise and Protect Your Software Supply Chain

NIS2 is the EU's most comprehensive cybersecurity legislation, but it will not be its last. Organizations planning for compliance can start by adopting a proactive disposition to minimise security threats. The Sonatype platform can help by directly addressing many of the management and reporting obligations in NIS2, including risk analysis, disaster recovery, supply chain security, and more. To learn more about how we can help you ensure compliance with emerging and existing regulations, schedule a demo today.

sonatype

Sonatype is the leader in software supply chain optimization. Sonatype's platform empowers enterprises to create safer software faster and to protect against the inherent risk from free open source components used to develop modern software applications. As founders of Nexus Repository and stewards of Maven Central, the largest public repository of Java, Sonatype pioneered software supply management and maintains the world's leading knowledge base of open source intelligence for software composition analysis and dependency management.

Sonatype's platform integrates this intelligence with customers' Software Development Life Cycle and delivers reliable automated identification and remediation of vulnerable and malicious open source code while also enabling customers to generate and continuously monitor SBOMs (Software Bill of Materials) to increase their security posture and be prepared for the next zero-day threat or software supply chain attack.

More than 2,000 organizations, including 70% of the Fortune 100, fifteen million software developers and hundreds of government customers rely on Sonatype to set and enforce policies for open source governance, and "shift left" to deliver software applications that are secure by design and secure by default. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com