sonatype

NIS2 Checklist:

How Sonatype helps you

The Network and Information Security Directive 2 (NIS2) is the EU's most comprehensive cybersecurity legislation, and taking steps to make sure your organisation is compliant should be a top priority. But that doesn't mean it needs to be complex.

We've outlined the key elements, **Articles 21 and 23**, that relate to protecting software components and how Sonatype can help you manage these obligations.

Cybersecurity risk-management measures Article 21

NIS2 Measures	Why it Matters	Sonatype Platform
21-2(a) policies on risk analysis and information system security;	☐ **Conduct a risk assessment:** You can't find what you can't see so building a risk assessment needs to be a priority. ☐ **Documented policies:** Organisations should have documented policies in place to analyse risk on a continual basis.	**Sonatype Lifecycle | Sonatype Intelligence** ✓ Define and automatically enforce specific policies for open source ✓ Universal and timely understanding of open source security, licence, and architectural risk. ✓ Create custom policies for specific situations
21-2(b) incident handling;	☐ **Cybersecurity incident handling:** Documentation should include detection, mitigation and reporting measures.	**Sonatype Nexus Repository** ✓ Centralise updates to a single binary repository for control and deployment.
21-2(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	☐ **Setting clear prioritisation:** Supply chain security is paramount for maintaining safe software components. ☐ **Identification and documentation of weaknesses and/or vulnerabilities:** This is a foundational step to NIS2 compliance. ☐ **Attesting to compliance:** Identify whether or not your organisation is required to attest to compliance with legal requirements.	**Sonatype SBOM Manager | Sonatype Lifecycle** ✓ Continuous application scanning and notification ✓ Creation and monitoring of SBOMs for new vulnerabilities ✓ Share SBOMs at scale with traceable and transparent VEX-based annotation
21-2(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	☐ **Regularly scheduled evaluations:** perform continuously monitored evaluations automatically. ☐ **Setting security benchmarks** is essential for the ongoing improvement of an organisation's cybersecurity posture.	**Sonatype Lifecycle and Sonatype SBOM Manager** ✓ Tailor remediation policies and assign risk profiles based on needs
21-2(g) basic cyber hygiene practices and cybersecurity training;	☐ **Establish cyber hygiene standards:** This helps create a foundation for effective risk management. ☐ **Evaluate cyber hygiene standards:** This is an opportunity to assess the integrity and reliability of a company's digital infrastructure.	**Sonatype Repository Firewall | Sonatype Nexus Repository** ✓ Sonatype's out of the box policies help you establish and enforce standards automatically ✓ Centralise your open source consumption into a single artifact repository and gain insight into your risks ✓ reporting to show effectiveness of SBOM based security (SBOM Manager)
21-2(i) human resources security, access control policies and asset management	☐ **Security-focused culture:** Human engineering is still one of the most common threats to an organisation. Fostering a culture of security can dramatically reduce human error.	**Sonatype Lifecycle | Sonatype Nexus Repository** ✓ Provides a single source of truth for every item of the software supply chain
21-2(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	☐ **Multi-Factor authentication:** Enabling this function substantially decreases the possibility of user accounts being exploited.	**Sonatype Platform** ✓ Control access to your components with single sign-on (SSO), role-based access controls, and full auditability

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:

Final Report Obligations	Sonatype Platform
A detailed description of the incident, including its severity and impact;	✓ Search across applications to quickly identify which are affected. ✓ Our policy engine helps establish severity in context of the applications.
The type of threat or root cause that is likely to have triggered the incident;	✓ Sonatype Intelligence Sonatype SBOM Manager helps establish the issue, applicability, remediation steps, and potential impact.
Applied and ongoing mitigation measures;	✓ Policy engine and up-to-date SBOMS help 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
Where applicable, the cross-border impact of the incident;	✓ Waiver descriptions keep information with application SBOM

Optimise and Protect Your Software Supply Chain

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. For a detailed look at how Sonatype can help meet NIS2 requirements, download our **User's Guide to NIS2 Compliance**.

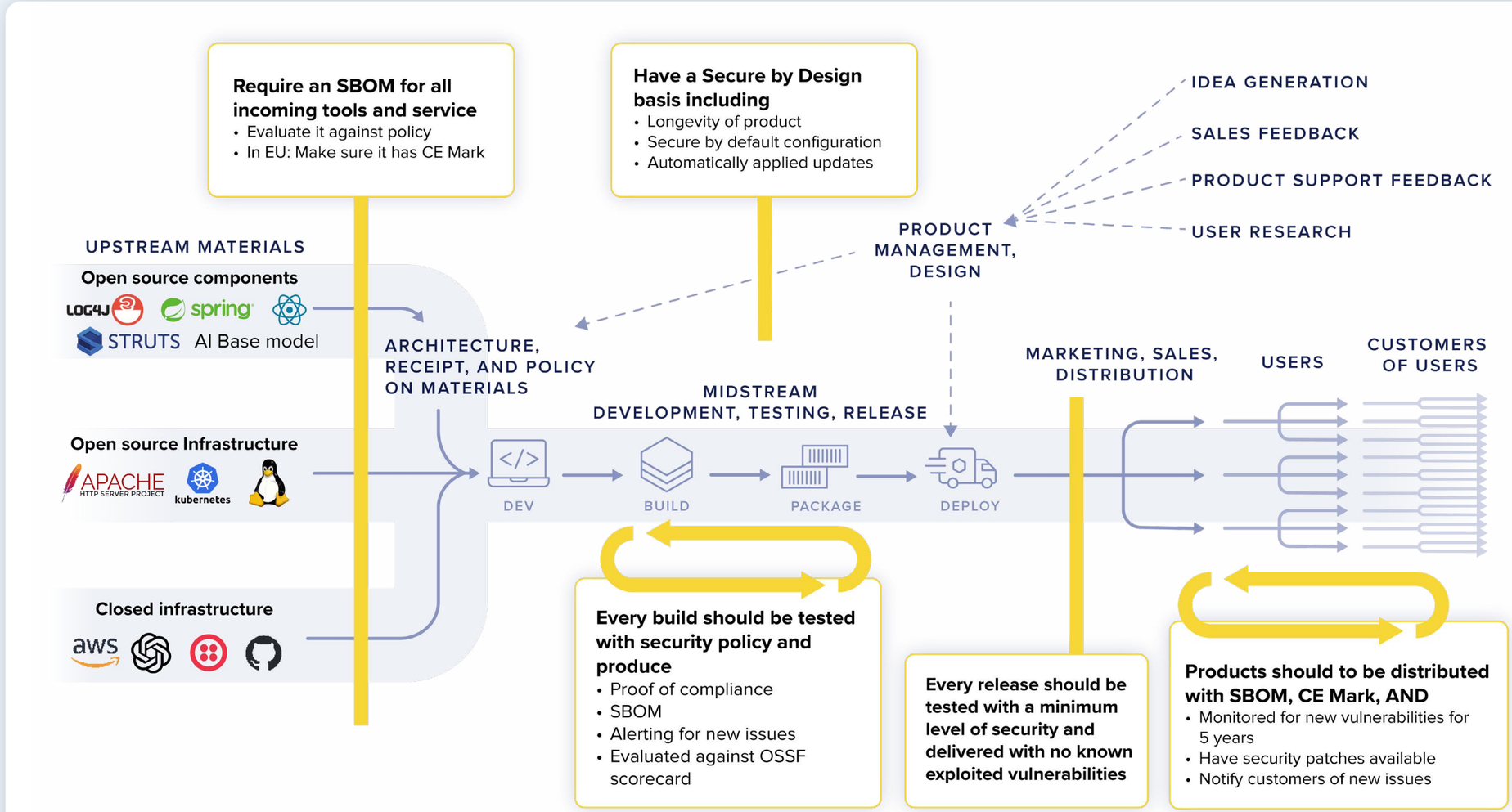
sonatype

How Sonatype's Platform helps you comply

Simplify SBOM Compliance and Security Monitoring with Sonatype SBOM Manager

More than 70 percent of Fortune 100 companies manage their software supply chains with Sonatype, and our SBOM Manager has been developed to take the uncertainty out of SBOM collection and monitoring compliance.

Request a demo today



Discover our full range of products that support your compliance journey

Maven Central Repository
World's largest Java repository, administered by Sonatype

Sonatype Lifecycle
Achieve faster release velocity withreliable SDLC security automation

Sonatype SBOM Manager
Simplify Software Bill of Materials compliance and monitoring

Sonatype Nexus Repository
Smart repository to manage and build artifacts, trusted by more than 150K organizations

Sonatype Developer
Prioritized recommendations and reliable automations for developer velocity

Advanced Legal Pack
Automate and streamline OSS comp-onent licensing and legal compliance

Sonatype Repository Firewall
Automatically spot and stop risk before entering your repository

Sonatype Container
Protection for container network, process and file system