sonatype

CHEAT SHEET

Preparing SBOMs for Audits

Internal policy requirements

- **Set expectations for OSS components:** Define risk tolerance and rules for utilizing OSS and communicate these expectations across development teams.
- **Continuously monitor for violations:** Address violations faster by continuously monitoring SBOMs for potential risks for real-time response and mitigation.
- **Provide controls:** Document and enforce policies around what components are allowed into your supply chain and which are not.

Understand applicable cybersecurity requirements

- **NIST and CISA:** If you supply software to the US government, you must comply with NIST SP 800-218 and Cybersecurity and Infrastructure Security Agency (CISA) attestation attestation mandates.
- **PCI DSS:** The PCI Software Security Framework (SSF) applies globally to any organization that handles, processes, or stores payment card data. It ensures the security of payment software, with an emphasis on security integration in the development process.
- **EU CRA:** The Cyber Resilience Act applies to any company that sells physical products containing software in the European Union.
- **EU NIS 2:** The NIS2 directive applies to any company operating a digital service or serving a critical industry in the European Union.
- **DORA:** The Digital Operational Resilience Act (DORA) is a European Union-wide act that will require EU financial entities to implement operational and resilience strategies.
- **FD&C Act:** The United States Federal Food, Drug, and Cosmetic (FD&C) Act applies to any company selling medical devices.
- **FAR:** The Federal Acquisition Regulation (FAR), applies to any US company that develops software under contract with the US federal government.

Terms and Conditions

- **Anticipate updates to Terms and Conditions:** As awareness around cybersecurity requirements grows, terms and conditions will reflect the requirement for suppliers to provide SBOMs. SBOMs are also becoming increasingly common requirements for vendor contract renewals.

Operate at Scale

- **Establish processes for regular SBOM generation:** To comply with DORA, FD&C Act, and FAR
- **Deliver secure software at scale:** Manage libraries and store components in a central repository and easily share them across the SDLC.
- **Produce a machine-readable SBOM:** An SBOM that can be automatically generated, updated, and analyzed makes identifying and mitigating potential risks faster and more comprehensive across different tools.
- **Separate build and release:** Incorporate SBOMs within your software development life cycle (SDLC) to enable monitoring. Also, ensure SBOM data is meticulously captured and securely retained for versions that are released, deployed, or shipped.

Continuous monitoring and feedback

- **Alert system:** Implement an alert mechanism for newly discovered vulnerabilities in existing SBOMs that could be affecting your first- and third-party applications.
- **Iterative improvement:** Establish feedback loops for continuous refinement of your SBOM strategy, adapting to emerging security challenges and tech advancements.
- **Internal audits:** Build an expectation with customers of proactive communication when critical vulnerabilities or license issues are discovered.

Implementation steps

1 **Create SBOMs throughout the release process:** Create SBOMs for every application to provide visibility into what components are in each version.

2 **Automate SBOM creation:** Automatic SBOM creation ensures each build has a corresponding SBOM for compliance or auditing purposes.

3 **Centralize your SBOMs:** Storing SBOMs with your repository or artifact manager provides a central location for access across your organization.

4 **Include scan results with your SBOM:** Keeping track of potential risks provides transparency and helps customers assess threat levels of specific components.

5 **Establish Governance, Risk, and Compliance [GRC] protocols:** Integrate SBOM insights into your governance, risk management, and compliance (GRC) framework to enhance decision-making and regulatory adherence.