sonatype

Implement CERT-In Software Development Guidelines with Sonatype

Introduction

The Indian Computer Emergency Response Team, or CERT-In, is responsible for cybersecurity policy in India. As with similar organizations around the world, the value of effective Software Bill of Materials (SBOM) management has become a key to threat prevention, detection, and mitigation. In October 2024, CERT-In published its **Technical Guidelines on SOFTWARE BILL OF MATERIALS** to bolster the security and transparency of software supply chains. These guidelines provide a systematic framework for creating, managing, and sharing comprehensive SBOMs, enabling more effective vulnerability management and risk mitigation.

India's approach to supporting suppliers, developers, and organizations that utilize software mirrors the trend **we're seeing around the world** as governments are taking a more active role in matters of cybersecurity. While not a legal requirement, CERT-In recommends these guidelines become mandatory standard practice for entities, especially in the Government, Public Sector, Essential Services Organizations, and organizations involved with software exports and the software services industry.

In this executive summary, we examine the key features of these guidelines and how Sonatype can help address regulatory challenges and enhance software development processes for a more secure and compliant future.

CERT-In SBOM Guideline and Sonatype Capabilities

2.3 SBOM Implementation	
SBOM should be implemented for every new software component release and updated promptly for any changes such as updates, upgrades, releases, and patches. The accuracy of SBOM is maintained by updating whenever there is new information about included components, regardless of whether the components themselves have changed. When modifying existing components, choose a consistent approach: either treat the change as a new component or update the existing one. For clarity, use standardized versioning methods throughout.	**Sonatype SBOM Manager** facilitates secure distribution and sharing of SBOM documents through a Vendor Portal, secure file-sharing, and API integrations. It can also reliably manage SBOMs at scale, which is essential for managing the large volumes of software components that make up modern applications.

3.1 Levels of SBOM

The different levels of SBOM, each offering varying degrees of granularity and complexity, indicate specific needs and the complexity of their respective software environments. Organizations should choose to implement one or more SBOM levels to achieve an efficient balance of transparency, risk management, and operational efficiency.

Sonatype supports the generation and management of various levels of SBOMs, such as Top-Level, N-Level, Delivery, Transitive, and Complete SBOMs, as well as SBOMs aligned with different stages of the Software Development Lifecycle (SDLC) like Design, Source, Build, Analyzed, Deployed, and Runtime SBOMs. It also provides detailed historical version control so users are ready to address compliance and security inquiries at any time.

3.3 Roadmap for Organizations to develop and adopt SBOM

*To establish an SBOM ecosystem within an organization, the development of an SBOM program should follow a phased approach, starting from a basic foundation (***START***), then building upon it (***PROGRESS***), and ultimately reaching a mature and scalable SBOM implementation (***ADVANCE***). The order of activities is indicative. Organization may choose to move an activity up or down depending on their overall security requirements, project timeline, and resource availability.*

START	PROGRESS	ADVANCE
• Identify Critical Assets and Develop a Project Plan • Determine the SBOM format and minimum requirements • Identify security requirements, secure storage, and tooling. • Acquire SBOM as a part of the procurement process.	• Secure Installation and Operation Guidance Development. • Assign unique identifiers to each component. • Mapping of supplier's SBOM with consumer's internal SBOM • Preparation of SBOM • Integrate SBOM in each phase of Secure Software Development Lifecycle • Establish secure configuration management.	• Enhance vulnerability tracking processes • Enhance incident response process • Analysis and review for updation of existing SBOM periodically. • Maintain awareness of emerging software components and industry advancements.

Sonatype SBOM Manager makes it possible for organizations to quickly identify and address known vulnerabilities by continuously monitoring first and third-party SBOMs for new security vulnerabilities and malware risks.

3.4 License Management

License management is an early use case for SBOM, helping organizations with large and complex software portfolios track the licenses and terms of their diverse software components, especially for open-source software. SBOM can convey data about the licenses for each component. This data can also allow the consumer to know if the software can be used as a component of another application without creating legal risk. License information for components included in software can be checked to prevent negligence in compliance, thus reducing the risk of license violations and the workloads required for license management.

Sonatype SBOM Manager helps track open-source software licenses and share package information using the SPDX (Software Package Data Exchange) format, ensuring compliance with license requirements and exceptions. Critical license details like the license type, compatibility, and any restrictions are included, making it possible to identify potential license conflicts or compliance issues.

4.3 Automation Support

Supporting automation, such as automatic generation and machine readability, enables scaling across software ecosystems and organizational boundaries. It allows for seamless integration of SBOM data into various tools and processes, facilitating collaboration and visibility across the software supply chain.

Sonatype SBOM Manager streamlines compliance with CERT-In's minimum SBOM requirements by automating the generation and maintenance of accurate and comprehensive SBOMs. It provides deep insights into open-source and third-party components, ensuring transparency and traceability throughout the software supply chain. Integrating with development workflows enables real-time monitoring for vulnerabilities, license risks, and policy violations. This ensures organizations meet regulatory mandates while maintaining secure and resilient software systems.

5.3 Secure SBOM Distribution

To implement access control, precise terms must be defined for SBOM data integration. These terms can be established through licensing, contracts, or other existing mechanisms governing software usage and rights. Suppliers, including open-source maintainers, may prefer public SBOM data, while others might opt for confidentiality, limiting access to select users. By following these steps, organizations should implement a secure and controlled distribution of SBOM, ensuring that sensitive information is accessible only to authorized parties while maintaining transparency and trust in the software supply chain.

Sonatype SBOM Manager
Sonatype SBOM Manager facilitates secure distribution and sharing of SBOM documents through a Vendor Portal, secure file-sharing, and API integrations.

6. Vulnerability Tracking and Analysis

This chapter discusses vulnerability tracking and analysis using Software Bill of Materials (SBOM) Vulnerability Exchange Document (VEX) and Common Security Advisory Framework (CSAF). VEX facilitates standardized sharing of vulnerability information, while CSAF provides a structured framework for describing security advisories. These include:

a) *Design a VEX Document*

b) *Adoption of Common Security Advisory Framework (CSAF)*

c) *Integration with diverse vulnerability databases and advisory*

d) *Implement shift-left approach and vulnerability scanning*

Sonatype SBOM Manager simplifies adherence to security regulations, guidelines, and best practices on software security by ensuring that SBOMs are generated, managed, and distributed as per compliance with regulatory standards. It supports automated Vulnerability Exchange (VEX) information and data, which is crucial for regulatory compliance.

Finally, the CERT-In guidelines include a list of practical recommendations and best practices to strengthen software supply chain security.

7. Recommendations and Best Practices	
Recommendations	
7.1.1	All the government, public sector, essential services organizations and organizations involved with software exports and software services industry should include requirements for SBOM in all their software and solutions Purchase/Procurement.
7.1.2	All software supplied to the government, public sector & essential services organizations/departments must be accompanied by a complete SBOM.
7.1.3	All government, public sector and essential services organizations/ departments must ensure to maintain SBOM of the software being used, procured and developed.
7.1.4	The SBOM of the software supplied to the government and public sector organizations/departments must include the data fields mentioned in Chapter 4, section 4.2 of this document.
7.1.5	The format to generate the SBOM of the software supplied to government and public sector organizations/departments should be Software Package Data eXchange (SPDX) or CycloneDX.
7.1.6	*The software developer/integrator organization that supplies software to government and public sector organizations/departments should design a Vulnerability Exchange Document (VEX) after a vulnerability is discovered informing customers about the exploitability status to allow consumers to prioritize their remediation efforts. The VEX document must include the following about the status of vulnerability in specific software products:* • *Not affected – No remediation is required regarding this vulnerability.* • *Affected – Actions are recommended to remediate or address this vulnerability.* • *Fixed – Represents that these product versions contain a fix for the vulnerability.* • *Under Investigation – It is not yet known whether these product versions are affected by the vulnerability. An update will be provided in a later release.* *Subsequently, after the VEX document, the supplier should provide the CSAF advisory, which includes detailed information about the vulnerability, such as a description, affected product versions, severity assessment, recommended mitigation steps, etc.*

7.1.7	Software Developer/Consumer/Integrator organizations should integrate their SBOM data with vulnerability databases, CERT-In vulnerability notes, alerts, threat intelligence platforms, and vendor-specific advisories, enabling comprehensive visibility into their software's security posture.
7.1.8	Consumer organizations should update their own SBOM to reflect applied patches or Mitigations.
7.1.9	A separate SBOM for each software version, updating it only when additional component information is provided or SBOM errors are corrected.
7.1.10	The consumer organizations (especially the government and public sector organisations) should map and develop an internal SBOM on the basis of the SBOM provided by the supplier.
7.1.11	Security teams of Software consumer organizations should include SBOM inventory in the workflow of vulnerability management.
7.1.12	Regular audits and assessments of SBOM processes should be conducted to ensure accuracy and completeness.
7.1.13	Consumer organizations should combine component data from SBOM with vulnerability status information from VEXes to provide an up-to-date view of the status of vulnerabilities to enable a targeted approach to identifying and addressing software Vulnerabilities.
7.1.14	It should be ensured the SBOM data is stored and transmitted securely, using encryption, access controls, and other security measures to protect the sensitive information.
7.1.15	Establish workflows to regularly update the SBOM as new software components are introduced or existing ones are updated.

Best Practices	
7.2.1	Ensure the SBOM captures detailed metadata, such as component names, versions, licenses, and unique identifiers.
7.2.2	Integrate SBOM generation into the secure software development lifecycle (SSDLC) & CI/CD pipelines to maintain the SBOM's accuracy and timeliness
7.2.3	Implement risk-based approaches to prioritize the remediation of vulnerabilities based on factors like severity, exploitability, and potential business impact.
7.2.4	Establish clear policies and procedures for the handling, sharing, and distribution of the SBOM data.
7.2.5	The SBOM data should be generated in such a way that it can be utilized to demonstrate compliance and fulfill regulatory reporting obligations related to software supply chain security.
7.2.6	Implement alerting systems to promptly notify relevant stakeholders about critical security events, enabling timely remediation.
7.2.7	Develop detailed playbooks for responding to security incidents and managing the remediation of vulnerabilities identified through the SBOM analysis.
7.2.8	Adopt a zero-trust security model to verify every user and device trying to connect to the network, enhancing security by eliminating implicit trust assumptions.
7.2.9	Implement Multi Factor Authentication (MFA) mechanisms to add an extra layer of security, reducing the risk of unauthorized access to systems and data.
7.2.10	Conduct periodic vulnerability assessments and measurements to identify and address security weaknesses promptly.
7.2.11	Implement continuous monitoring of software components and dependencies to detect vulnerabilities and address them promptly.

7.2.12	Obtain assurances from third-party software vendors and suppliers regarding the accuracy, completeness, and timeliness of SBOM provided, and establish contractual agreements to ensure compliance with SBOM requirements.
7.2.13	Perform thorough analysis to ensure that the licenses of all software components within an application or software are compatible with each other. Identify any conflicts or restrictions that may arise from combining different licensed components.

SBOMs are one of the key building blocks of modern software development, and full transparency into what goes into the applications you build is the only way to ensure compliance. For more information about best practices for SBOM management, visit our **Resource Center** or schedule a **Sonatype SBOM Demo** with an expert today.

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