开放原子开源基金会
OPENATOM FOUNDATION | OpenEuler OPENCHAIN

openEuler's Conformance to ISO/IEC 18974

The journey to supply chain security

ISO/IEC 18974:2023 Adoption by openEuler

开放原子开源基金会 OPENATOM FOUNDATION | openEuler OPENCHAIN

Overview

ISO/IEC 18974:2023 is an international standard maintained by the OpenChain Project, which defines the key requirements of establishing and managing a quality open-source security assurance program.

This case study analyzes the rationale behind openEuler's adoption of ISO/IEC 18974:2023 and shares best practices derived from this process. These practices have empowered the openEuler community to optimize processes, cultivate talent, construct community rules, and enhance the security of open-source software releases.

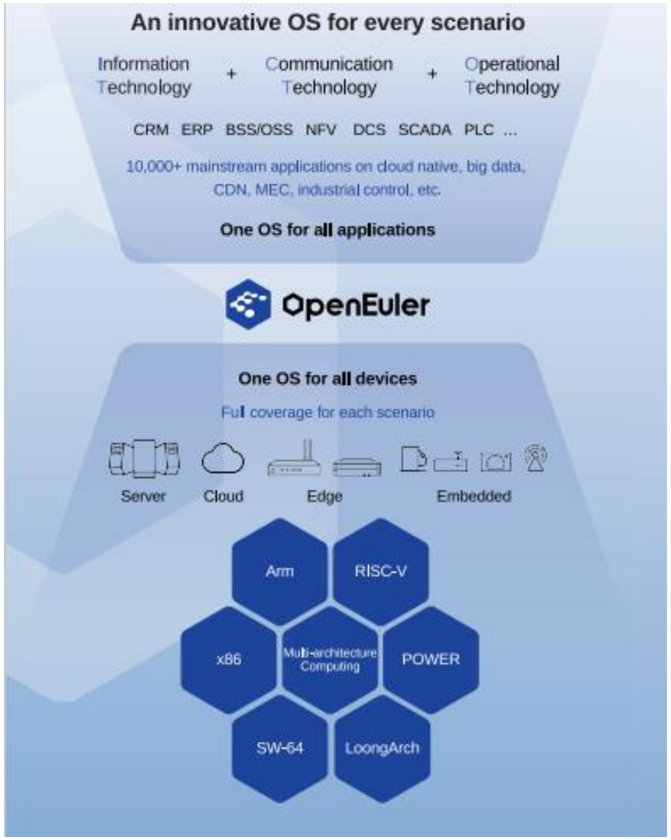
By sharing these practices, we aim to collaborate with OpenChain and other open-source communities to build a trusted open-source supply chain.

Who are we

openEuler is a digital infrastructure OS incubated and operated by the OpenAtom Foundation. It is suitable for any server, cloud computing, edge computing, and embedded deployment. This secure, stable, and easy-to-use open-source OS is compatible with multiple computing architectures. It is ideal for operational technology (OT) applications and enables the convergence of OT and information and communications technology (ICT).

The openEuler open-source community collaborates with global developers to create an inclusive and diverse software ecosystem catering to all digitalization scenarios, empowering enterprises to develop their software, hardware, and application ecosystems.

For more information, visit https://www.openeuler.org/



An innovative OS for every scenario

Information Technology + Communication Technology + Operational Technology

CRM ERP BSS/OSS NFV DCS SCADA PLC ...

10,000+ mainstream applications on cloud native, big data, CDN, MEC, industrial control, etc.

One OS for all applications

One OS for all devices

Full coverage for each scenario

Understanding ISO/IEC 18974:2023

- The ISO/IEC 18974:2023 is the standard maintained by the OpenChain Project, which defines the key requirements of a quality open-source security assurance program.

- ISO/IEC 18974 helps organizations check open source for known security vulnerability issues like CVEs, GitHub dependency alerts or package manager alerts. It is lightweight, easy to read and is supported by our global community with free reference material and conformance resources.

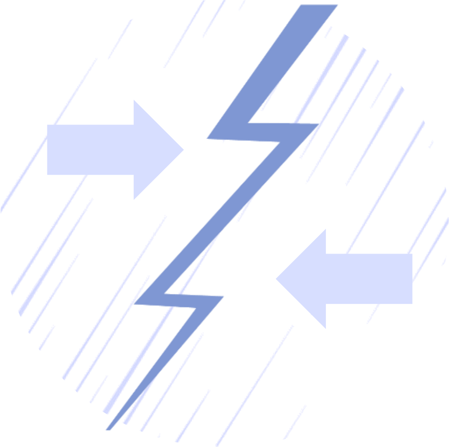
It identifies:

The key places to have security processes

How to assign roles and responsibilities

How to ensure sustainability of the processes

Challenges we face

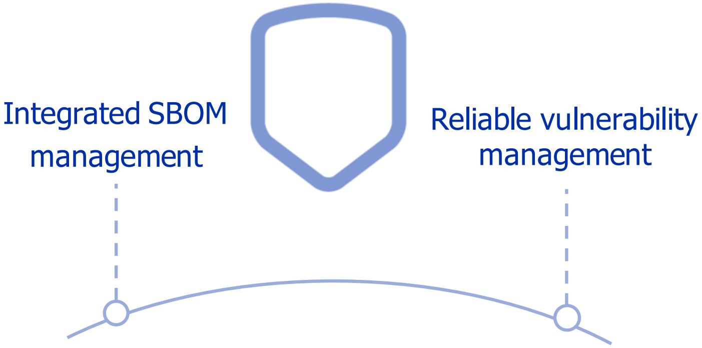


Emerging open-source supply chain attacks:

e.g., supply chain compromise on xz utils and log4j

Incompleteness in standardized security assurance processes to protect our community, specifically in

- Integrated SBOM management
- Reliable vulnerability management



Integrated SBOM management

Reliable vulnerability management

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler OPENCHAIN

Opportunity for improvement

openEuler aims to build a secure and compliant community for all. Adopting ISO/IEC 18974:2023 provides an opportunity for self-reflection, helping to identify the weaknesses in our proposed solutions.

This continuous improvement process focuses on optimizing processes, cultivating talent, constructing community rules, and enhancing the security of open-source software releases.

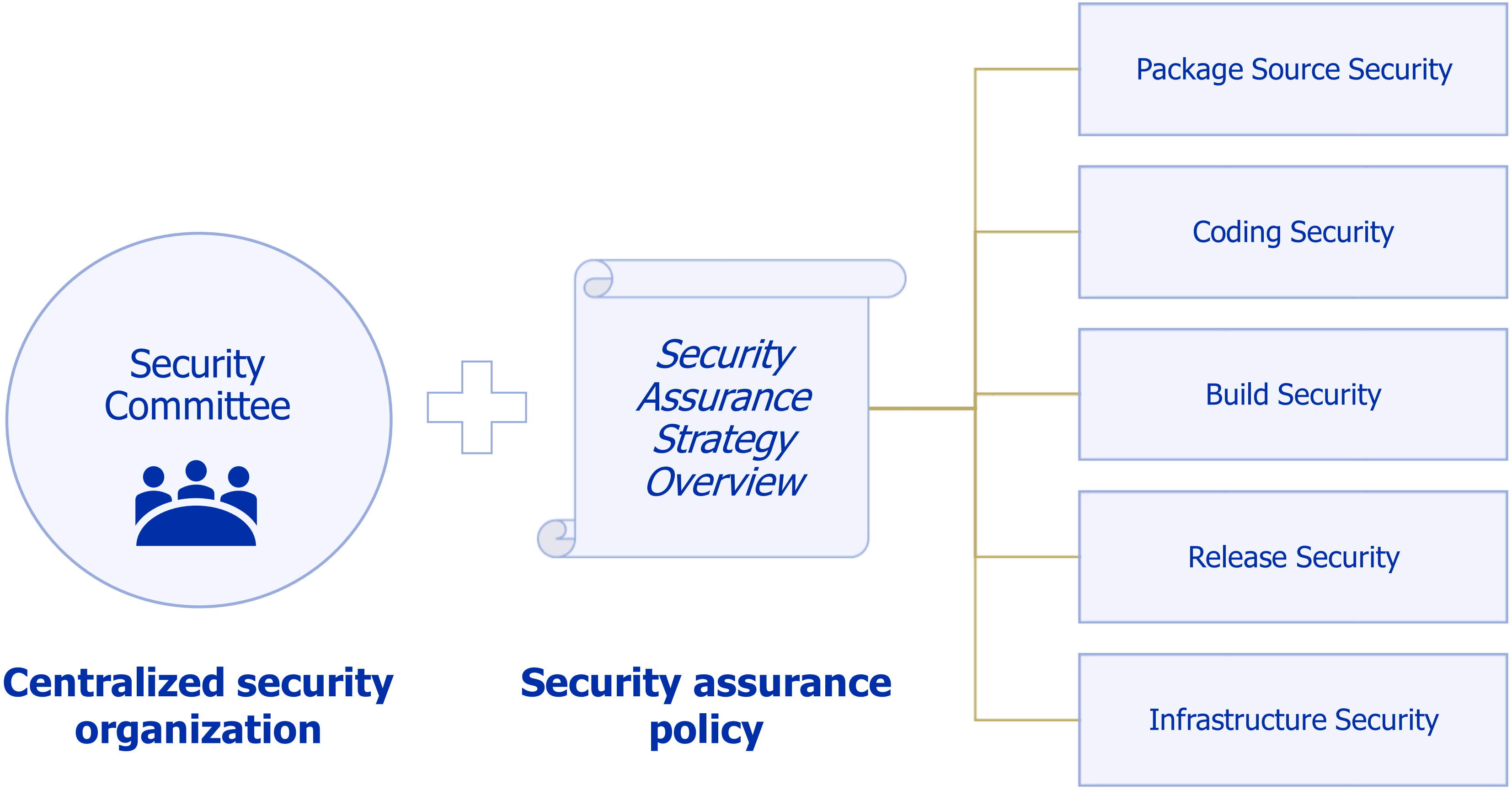
Embracing global standards

The ISO/IEC 18974 standard aligns with other standards related to open-source software. Adopting ISO/IEC 18974 provides a framework to reframe the openEuler infrastructure from a global perspective, making it adaptable to other international standards' requirements.

Moreover, it also facilitates obtaining entry-level certifications such as EUCC and CRA, thanks to the standard's thorough review and sterling industry reputation.

Our Path to Enhanced Security

Centralized security governance



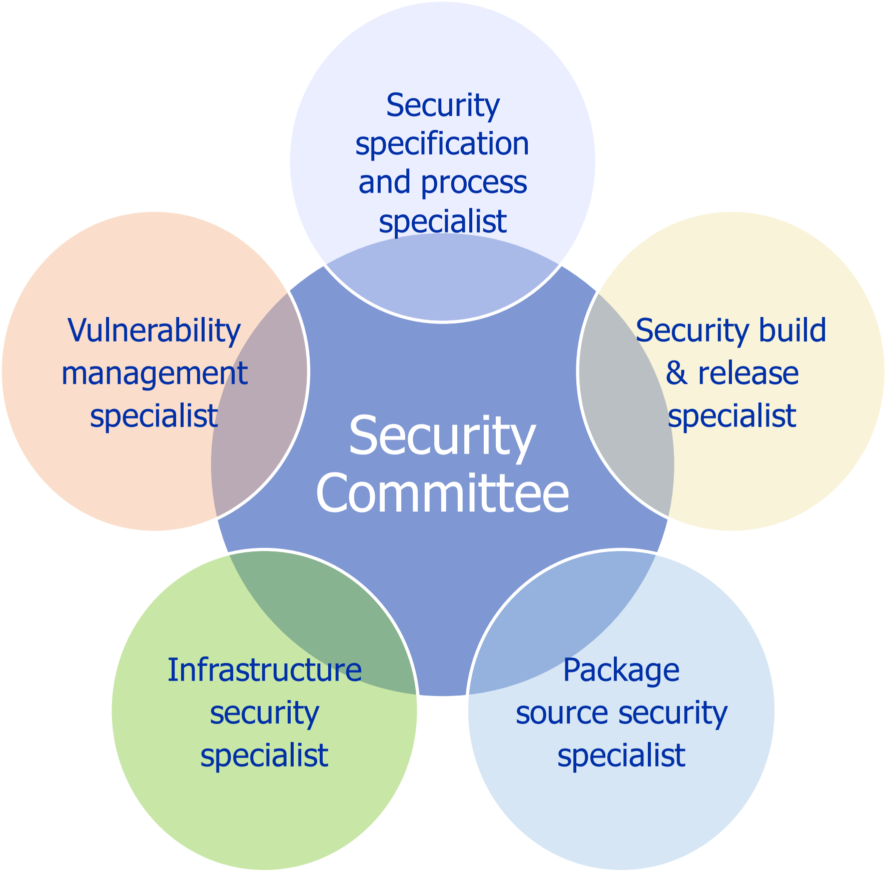
Centralized security organization

Security assurance policy

Security organization structure

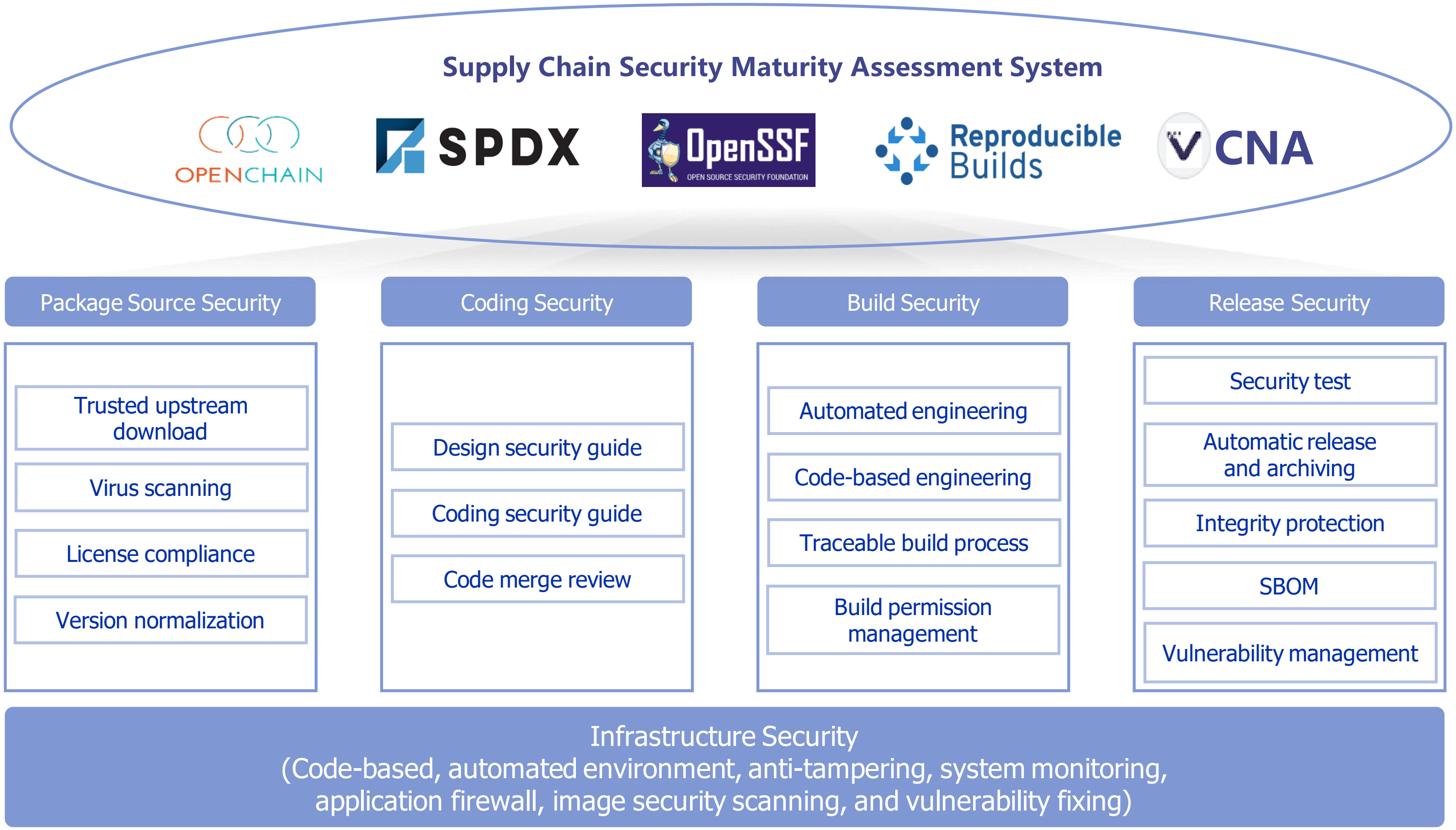
openEuler has established a Security Committee and defined security roles to assign internal responsibilities. These members collaborate with, supervise, and guide maintainers from other SIGs to ensure policy implementation.

For more information, feel free to visit our repo.


Security specification and process specialist
Vulnerability management specialist
Security build & release specialist
Security Committee
Infrastructure security specialist
Package source security specialist

Security assurance policy

Referencing the industry's open source software supply chain security maturity assessment system, openEuler has developed community security policies across the entire software development lifecycle (SDLC).



Supply Chain Security Maturity Assessment System

Package Source Security
- Trusted upstream download
- Virus scanning
- License compliance
- Version normalization

Coding Security
- Design security guide
- Coding security guide
- Code merge review

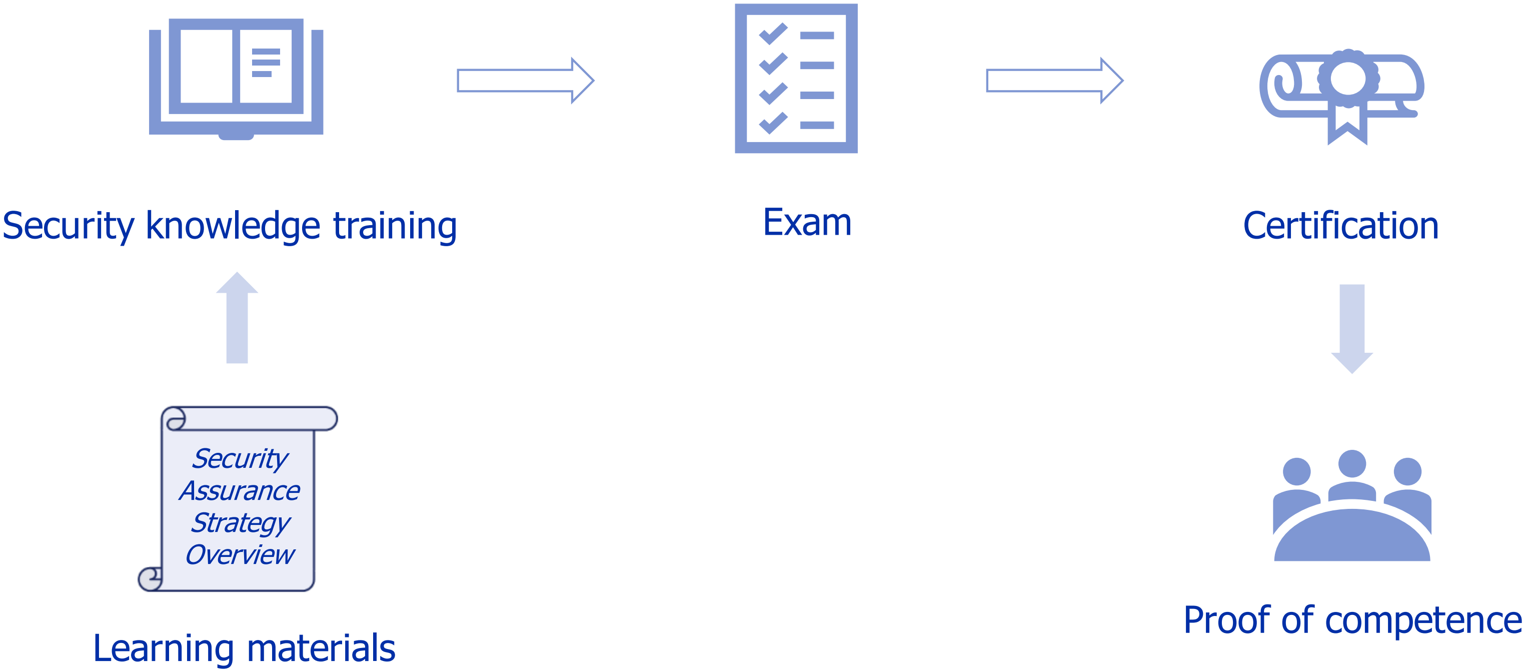
Build Security
- Automated engineering
- Code-based engineering
- Traceable build process
- Build permission management

Release Security
- Security test
- Automatic release and archiving
- Integrity protection
- SBOM
- Vulnerability management

Infrastructure Security
(Code-based, automated environment, anti-tampering, system monitoring, application firewall, image security scanning, and vulnerability fixing)

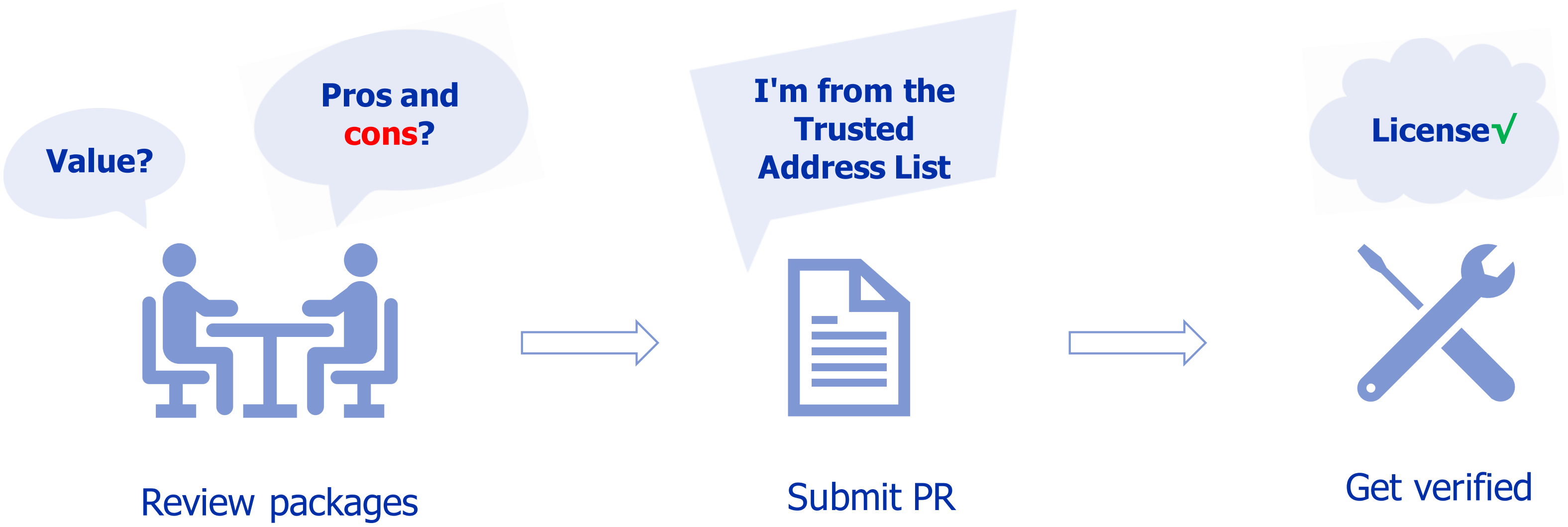
Effective Implementaion Practices

Competence & awareness


Security knowledge training
Exam
Certification
Security Assurance Strategy Overview
Learning materials
Proof of competence

To ensure each participant has sufficient competence to perform their duties, openEuler has designed a process to provide participants with a way to acquire sufficient expertise, to assess their competence and awareness and to grant them a certification as proof of competence.

Package source review



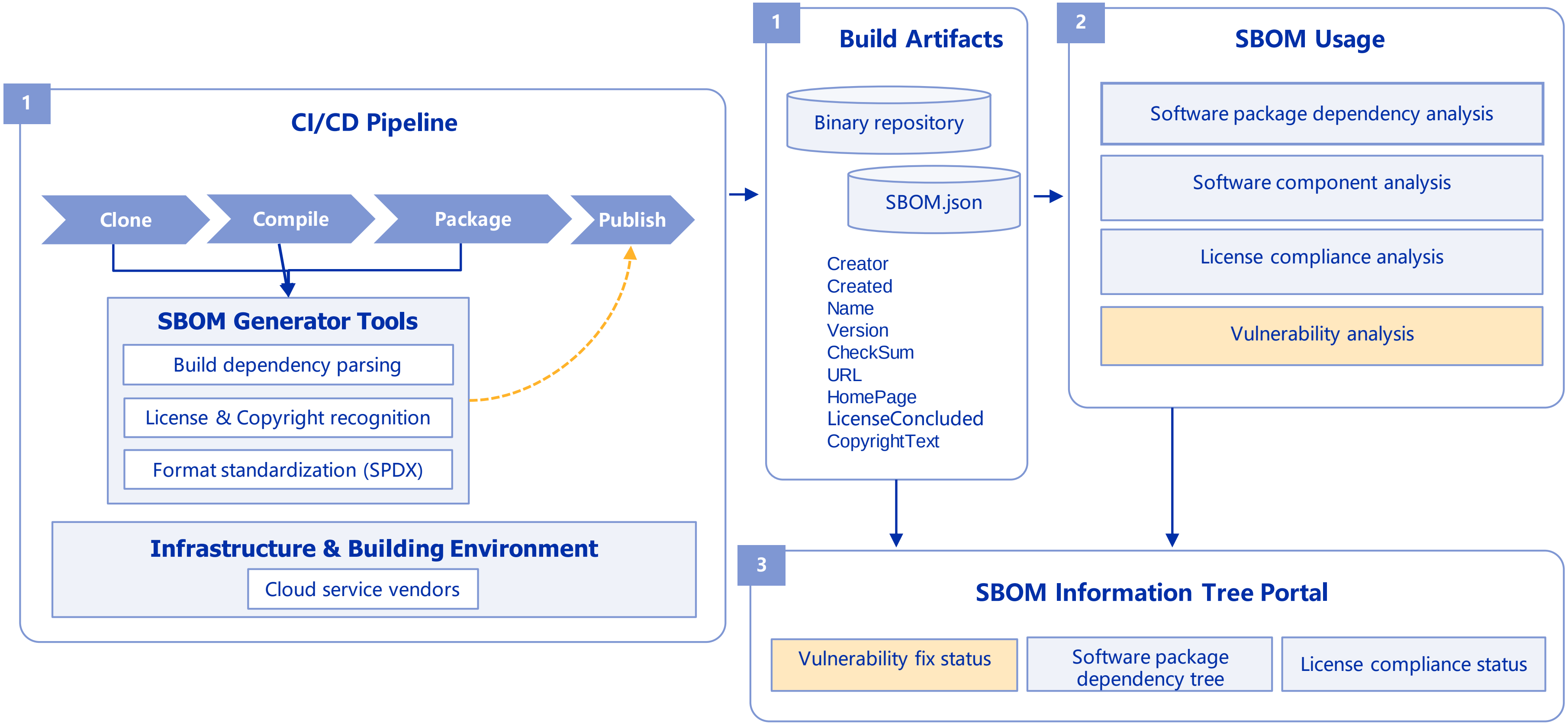
To build the provenance trust in the supply chain, every package source is thoroughly reviewed before being deployed in our releases.

SBOM-based vulnerability management

Data generation & storage: SBOM is automatically generated based on CI/CD pipeline and stored with the products.

Data consumption: Integrity verification, license compliance, and vulnerability awareness based on SBOM.

Online service: SBOM online portal, displaying package dependencies and the status of vulnerability fixes and license compliance.



Unveiling the Benefits and Impacts

By adopting ISO 18974:2023...

openEuler reaps numerous benefits:

- Opportunity for self-reflection and improvement, enabling the identification of gaps and areas for enhancement within its processes
- Alignment with international standards, promoting global compatibility and recognition
- Facilitation of compliance with assessment standards, which is crucial for market access and building user trust
- Empowering security governance in openEuler, ensuring the security of openEuler's releases

By showcasing our practices...

openEuler aims to share its experience as the first open-source community to adopt ISO 18974 for:

- Promoting our security governance improvements
- Providing a reference model
- Building a trustworthy supply chain with other open-source communities

Thanks

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler OPENCHAIN