6 ways to secure open source in enterprises

Open Source has been a part of the corporate IT landscape for years. Organizations have benefited from using open source in many ways - right from reducing total cost of ownership, enabling better innovation, faster development, and better code quality, to attracting great talent to work for you.

However, one thing that is often seen as a possible issue with open source is security. One of the common arguments heard, for example, is that if anybody can contribute code to an open source project, what is stopping bad guys from inserting malware inside the projects you will use in your enterprise? And if you are using open source security products, can seeing the source code enable attackers to break the software and as a result your information system? Also, how do you ensure that the code you are using isn't riddled with known, yet unpatched, security vulnerabilities?

This article focuses on this need for security and discusses how to secure open source usage in enterprises by developing an adequate and healthy open source risk and security governance system.

Securing open source software usage

For security to succeed, it must become the default state for all processes, products and services used, developed, or offered by an organization. Accordingly, open source security has to be made mature and sustainable for it to be a positive asset.

There are several steps in securing the use of open source:

- Create a risk profile for open source software (OSS) – risk identification, risk assessment, risk response & mitigation, risk and control monitoring & reporting. Risk management process must define the organization risk appetite as well. Also, remember that risk is not static, and continuous risk management is required.
- Establish an open source policy with the right scope that uses an enforceability instrument. There are several frameworks and standards available to use for forming an optimal policy. For example, NIST special publication 800-53 provides a catalog of security and privacy controls. A workable policy should be directly related to an enforceable set of security controls and must be incorporated into the software development lifecycle (SDLC). The security tools must be integrated in the developers' process (CI/CD, Agile, DevOps, waterfall...) to be confident that they are not introducing known security vulnerabilities into codebases inadvertently.
- Shift security to the left. Ensure security by default is embedded in the SDLC integrating security deeply into the software delivery lifecycle and that it fits the same mentality in the software and systems procurement teams. Additionally, consider the prioritization of security requirements as a part of the product core requirements. Furthermore, review and evaluate the automated tests upon code alterations in areas where the risk can be optimized. This must be part of a regular process of security testing.

- Create and validate an open source inventory, asset management and configuration management databases across the organization, as well as conduct regular audits of the open source systems, components, and third-party software vendors.
- Define measured outputs and specific metrics for OSS security initiatives. Monitor and evaluate risk and security processes with right KPIs on individual process performance as well as company-wide metrics. This gives the CISO two important data points that they need to make accurate and adequate investment decisions. First, it measures the maturity of the OSS governance. Second, it provides measurable control improvements. The CISO can link this with KPIs coming from the organization's operations center to show a return on the security investment.
- Develop a security focused organization culture. Technical security risk is only a piece of the overall state of a secure open source ecosystem. Organizations should cultivate a purposeful and conscious initiative to facilitate cultural change. This initiative must be endorsed by the executive management team, and have the consensus of all business units. Ensure that everyone in the organization realizes that they have an active role to play in the overall security and rewarding for great security work should be part of an incentive program. Deliver short, challenging security training activities that are fun, engaging and first-rate, in order to capture people's imagination and emotions.

A holistic approach to open source security governance

While open source brings several benefits to organizations and plays an important role in the digital transformation journey, ill-managed security principles harm organizations. The goal for open source security should be aligned with the overall organization security objectives. Developing an adequate and healthy OSS risk and security governance takes time and commitment but is worth the effort. It has a direct link to the cultural changes. A mature OSS governance combined with well-trained employees and right cultural mentality provides a strong defense against security threats.

About the authors

Gilles Gravier
Director, Open Source Consulting Practice, Wipro

Gilles, based in Switzerland, provides open source and blockchain strategy consulting and advisory services to Wipro's key customers worldwide. Throughout his career, Gilles has been involved in both security and open source.

Reza Alavi
Managing Consultant
Risk, Compliance, Assurance (RCA), UK/I/CE, Wipro

Reza, with over 15 years of experience in leading technology risk and security executive projects, works with Wipro's clients to analyze, develop and deliver solutions for complex risk and security challenges in digital transformation projects.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/BRD/MAY2020-APR2021