The open source community's **commitment to security**

Contributors' pride in their code has led to robust processes for ensuring the integrity of open source components

Joel Krooswyk

GitLab

Industry and government can't hire enough developers, so efficiency is the name of the game. Agencies want more, they want better, they want faster, and open source helps developers get there. It also helps them get there securely.

The beauty of open source is that if a problem is identified, we can bring it right back into the community. Scanning tools also help keep us honest when adopting the latest and most relevant code, and those tools tell us if we have included something that is out of date or unsafe from the moment we bring it in.

Open source developers take pride in their code, and it shows in the way the community responds. Open source software contains thousands of contributions from the largest companies in the world, which participate in these projects because they have a vested interest in their success. Neither corporate nor individual contributors want their names on code that has vulnerabilities. Therefore, fixes and patches are developed and submitted quickly into repositories. We all learn from one another's mistakes and work together for better solutions.

Boosting collaboration and positive outcomes

A central tenet of software development is visibility and traceability from start to finish so that a developer can follow the code through development, testing, building and security compliance, and then into the final production environment.

Along the way, there are some key activities that boost collaboration and positive outcomes, starting with early code previews, where developers can spin up an application for stakeholders to review. Other activities include documented code reviews by peers to ensure the code is well written and efficient.

In addition, DevOps components such as open source, infrastructure as code, Kubernetes as a deployment mechanism, automated testing, and better platforms and capabilities have helped developers move away from building ecosystems and instead focus on innovation.

2023: The year of compliance

It is crucial to validate performance, security and efficiency before applications reach production. Activities such as security scanning, code quality testing and fuzz testing can help agencies make sure their code is secure and won't crash when user interactions spike. The latest version of the National Institute of Standards and Technology's Secure Software Development Framework includes a checklist of scans that will give agencies a good understanding of the integrity of their applications.

Agencies should also have tools and platforms that provide

Shubham Dhage

> Neither corporate nor individual contributors want their names on code that has vulnerabilities. **Therefore, fixes and patches are developed and submitted quickly into repositories.”**

comprehensive visibility into what’s going on and whether there are critical vulnerabilities occurring in one place or across projects. Gathering data into a centralized security or vulnerability management dashboard helps agencies gain confidence in their software before it goes out the door, which will give them more confidence in its long-term ability to stay operational, run at scale and be secure all at the same time.

Given the number of mandates being released by NIST, the Cybersecurity and Infrastructure Security Agency, and the Office of Management and Budget, I believe 2023 will be the year of compliance. Agencies will be asked to institute security scanning and other testing, and they will be required to have software bills of materials and other attestation in place to verify that their vendors adhere to government mandates.

By ensuring that the applications agencies build and buy are compliant with all those requirements, agencies will be able to create secure, innovative systems and services. ■

Joel Krooswyk is federal CTO at GitLab.