Creating secure **open source repositories**

Visibility and automation allow agencies to identify and mitigate the risks of open source software components

Maury Cupitt

Sonatype

Roughly 80 to 90% of most modern applications are made up of open source or third-party components. Federal agencies will continue to use open source so they don't have to spend time and effort rebuilding what has already been built. Although that approach comes with some risk, gaining visibility into those components helps mitigate that risk.

President Joe Biden's Executive Order on Improving the Nation's Cybersecurity mandates visibility. In addition, programs like the Defense Department's Platform One and Kessel Run provide visibility into open source components via software bills of materials (SBOMs), static code analysis and scans. When a company publishes software to Platform One, for example, it is scanned for vulnerabilities. Based on those results, the application is either processed or it is not.

Uncovering malicious components at any stage

Protecting the software supply chain requires looking at every single thing that might come into an agency's environment. To understand that level of visibility, I like to use the analogy of a refrigerator. All the ingredients necessary to make a cake or pie are in the refrigerator. We know they are of good quality, and other teams can use them instead of having to find their own.

At Sonatype, our software equivalent of a refrigerator is the Nexus Repository Manager. A second aspect of our offering, called Lifecycle, allows us to evaluate the open source components in repositories at every stage of the software development life cycle.

One piece of software can download a thousand other components. How do we know if one of those components is malicious? Making those determinations at scale requires automation, which is how Sonatype's technology can look at every single published version of, for example, NPM and PyPy, and run analyses to answer the question: Does this look suspicious? We can see the SBOMs and a list of vulnerabilities or policy violations at any point and fix issues immediately.

A long-term commitment to the community

If a component is marked as suspicious, we can create a firewall that blocks developers from using it. In addition, our Nexus Repository Manager can be air-gapped for agencies that want their developers to go through a central repository that is not connected to the internet.

When open source components were becoming more prevalent in the early 2000s, Sonatype created the Maven Central Repository as a shared place to store all those components. We continue to maintain the repository as part of our ongoing commitment to the open source community because we strongly believe open source is the key to government innovation. ■

Maury Cupitt is regional vice president of sales engineering at Sonatype.