Challenges and a Practical Approach to Consumer Software Labelling

Authored by Chris Wysopal, Veracode founder and CTO

Veracode is a software security testing company that provides automated and manual software security testing as a service. We have been in business for 15 years and have had a consumer software labeling program, named *Veracode Verified,* for over 5 years. A directory listing of the software that has achieved a Veracode Verified label is at https://www.veracode.com/verified/directory.

We created this Veracode Verified labelling program out of requests from our software vendor customers. They needed a way to communicate to *their* customers during the sales process of what activities they undertook in the development of the software to achieve a certain level of software assurance. The activities are a mix of security testing, remediation processes and developer training.

Software vendors required a tiered program because they wanted to quickly attain some labelling recognition with a lower tier and progress to more rigorous tiers over time. Some vendors also had no desire to achieve the more rigorous tiers as they would add no more value for their software risk profile. We settled on a three-tier system as the best balance of time to a minimum assurance level with enough differentiation still for higher tiers of assurance.

Three Tiers for Veracode Verified

Each tier adds increasing levels of testing types and scope, and increasing levels of mitigation of the results of that testing. Also added is an increased cadence of testing and increased developer education. Here are the their-tiers and the requirements for each. Veracode verifies all these activities with the vendor. Many of the activities are fully automated and can be verified by simple inspection of test results.

Veracode Standard

Assess first-party code with static analysis.

- Establish a scanning cadence of at least every six months.
- Document that the application does not allow Very High flaws in first-party code.
- Provide developers with remediation guidance

Veracode Team

Includes requirements of Verified Standard, plus:

- Document that the application does not include Very High or High flaws, and that you have a 60-day remediation grace period to remain in compliance.
- Establish a scanning cadence of at least every 90 days.
- Identify a security champion within the development team to serve as a peer resource to development team members, ensuring secure coding practices across the development lifecycle.
- Provide training or labs on secure coding for the identified security champion.
- Assess open source components for security, and document that they don't contain any Very High or High vulnerabilities.
- Provide developers with remediation guidance for both 1st party code flaws and open source vulnerabilities.

Veracode Continuous

Includes requirements of Verified Team, plus:

- Integrate security tools into development workflows.
- Complete a post-product security assessment (dynamic analysis or penetration testing).
- Document that your application does not include any Very High, High or Medium flaws.
- Undergo Veracode's biannual mitigation review as well as a 30-day remediation grace period to remain in compliance.
- Establish a scanning cadence of at least every 60 days.
- Provide advanced training or labs on secure coding for the security champion identified on the development team.
- Provide development team with training or labs on secure coding.
- Assess open source components for security, and document that they don't contain any Very High, High, or Medium vulnerabilities.

We have created the following labels for software vendors to display where their software is sold or downloaded.

Lessons Learned

Most vendors just want the basic level so they can demonstrate some third party assurance to their software assurance efforts. However, once they get feedback on their level from customers and their customers understand what the level means they often strive for higher tiers. There definitely is a market dynamic for vendors to achieve more.

We have seen competitive pressures cause competitors of a vendor that has achieved a Veracode Verified label get a label themselves. This dynamic plays out in an individual software category area. When one vendor in the category achieved a label and started marketing with it, their competitors came to us and wanted toto achieve the label too and some even wanted to “one up” the competitor by achieving a higher tier. This is exactly the market dynamics we wanted to see.

I would be happy to participate in the workshop and additionally like to participate on a panel to describe our experiences.