insignary

About Insignary

Insignary was incorporated in 2016 in South Korea. We are backed by venture capital and have significant business and technical talent in our executive team, with extensive experience in the IT industry; the founding team specializes in open source software, compliance, and security. By leveraging our fingerprint-based binary scanning solution Clarity™, we aim to help companies detect, prioritize, and address known security vulnerabilities in open source code.

About Today's Predicament

More than 90% of the software written today integrates open source code. Open source code is used in IoT firmware, operating systems, network platforms, and applications. This trend will only continue to grow because by employing open source, developers can lower assembly costs and quickly add innovations. Yet within this ubiquitous open source code hide known security vulnerabilities – the favorable target for hackers. And by neglecting to patch these security vulnerabilities, companies are at risk for major computer system data breaches. Take Equifax for example. A well-documented Apache Strut vulnerability was left unpatched, resulting in a massive data breach that triggered a number of multi-billion dollar lawsuits. To prevent business-interrupting breaches and litigations, software development teams bear the responsibility of locating and eliminating known security threats prior to product deployment and usage. Yet companies often receive their purchased software or third-party code in binary format, making it challenging for OEMs, enterprises, managed service providers (MSP), and development teams to know exactly what open source code components are in their product. Consequently, it has been nearly impossible to identify known open source security vulnerabilities. Until Now.

About Clarity

Enter Clarity, Insignary's premier fingerprint-based binary code scanner. Clarity is unique in that it scans for "fingerprints" from a binary to examine and then compare against the fingerprints collected from open source components hosted in numerous open source repositories. Unlike checksum or hash-based binary scanners, Clarity does not necessitate separate databases of checksums or hash values for different CPU architectures. This significantly increases Clarity's flexibility and accuracy in comparison to legacy binary code scanners. Once a component and its version are identified through Clarity's fingerprint-based matching, comparing them to more than 180,000 known security vulnerabilities catalogued in vulnerability databases, such as NVD and VulnDB, is straightforward. Clarity also adds enterprise support, "fuzzy matching" of binary code, and support for automated build systems like Jenkins.

Clarity makes it simple for companies to take proper, preventative action before the deployment of their products. By leveraging this solution, MSPs, resellers, and auditors can capitalize on the growing security vulnerability detection market. Partners can also increase revenue opportunities and strengthen customer relationships in application security, software development, managed services implementation, and open source audits.