Software Composition Analysis

Essential for modern software development

Using open source or third-party code components (frameworks, plug-ins and libraries) significantly reduces software development time. It’s been predicted that most IT organizations will use some type of open source software in mission-critical applications, out of sheer necessity. Furthermore, third-party code can comprise up to 90% of typical applications. Using third-party components can accelerate app development, but it can also introduce potential licensing issues and critical vulnerabilities. These vulnerabilities are often difficult to identify, and even more difficult to fix in a timely way. Which puts your enterprise applications and ultimately your business at risk.

Keeping up with the number and prevalence of vulnerabilities is challenging. According to the National Vulnerability Database more than 4,000 new vulnerabilities are disclosed in open source software each year. Many frequently downloaded third-party components contain critical vulnerabilities, which can lead to serious exploits and attacks. Because of this, various security standards have added specific requirements for addressing component level vulnerabilities, including PCI-DSS, OWASP Top 10 and FS-ISAC. Organizations need to stay ahead of the curve and continuously monitor all their applications code including third-party components in their development environment.

Full inspection of third-party components

In order to fully understand your application vulnerabilities and the overall security posture of your web and mobile applications, you need in-depth visibility into the third-party components that you are using. WhiteHat Sentinel Source Software Composition Analysis (SCA) can provide you with a deeper understanding of the open source code being used in your applications.

Sentinel Source supports commonly used dependency management frameworks, such as Nuget, Maven, and Gradle so that dependencies declared within configuration files can be programatically inspected and downloaded for analysis. This makes it possible to retrieve versioning and licensing information and facilitates SCA for maximum visibility.

With Software Composition Analysis, you can accelerate the time-to-market for your applications by safely and confidently utilizing third party code, without introducing unnecessary risk.
The SCA report includes

- Per application breakdown of every component that is used
- License information for each component
- Information on components that are out-of-date
- Component version and whether it's the most current
- Identification of Common Vulnerabilities and Exposures (CVEs)

**Keep your code safe**

Software Composition Analysis (SCA) allows you to identify third-party and open source components that have been integrated into all your applications. It informs you about the licenses for each of them and identifies out-of-date libraries that should be upgraded or patched. SCA can let you know if any open-source frameworks have open CVEs that must be addressed. Click on a specific CVE and you'll be brought to MITRE page with recommendations on how to upgrade or downgrade out of a common vulnerability. You can also write your own libraries that other apps within your organization can use, and SCA will track if they have been used in a particular app.

**KEY BENEFITS**

- **Effortless Visibility:** Easily identify third-party components in your code
- **Accurate Detection:** Discover potential licensing and security issues in third party libraries
- **Gain Confidence:** Utilize third-party code with confidence
- **Ensure Compliance:** Understand your risk exposure
- **Improved Quality:** Ensure code consistency and quality
- **Enhanced Agility:** Safely leverage open-source and third-party components for accelerated time-to-market