Scantist SCA

Scan for known vulnerabilities, security bugs and licensing risks

The widespread use of open-source and third-party components in software development has enabled organizations to build and deploy high-quality software in a fast and cost-effective manner. Typical enterprise projects contain more than 250 open-source components, making up 60-90% of the application. This growing use of open-source has posed serious challenges – 1 in 4 security breaches arise, up from 1 in 7 five years ago.

Scantist's Software Composition Analysis (SCA) is a unique solution that combines true source-code and binary-level analysis from the ground-up to provide complete visibility into the third-party components used in your applications. This enables you to proactively manage security and compliance risks that often accompany the use of such components – a key milestone in implementing DevSecOps.

The Need for Software Composition Analysis

- **Third-party Dependencies** – Be it web, mobile or native, applications today are seldom written from scratch and incorporate an ever-increasing number of third-party libraries and components. This greatly simplifies the development process and shortens time-to-market, but also exposes your organization to multiple external risks.

- **Publicly-known Vulnerabilities** – The 105,000+ CVEs maintained by NVD are the most widely known vulnerabilities – with exploits available via a simple web search. These vulnerabilities are most commonly used as entry-points by adversaries, as seen in case of the Equifax breach.

- **Security Bugs** – While the NVD database is a good starting point, an even larger number of vulnerabilities are found and patched by the third-party developers internally. These 'security bugs' never make it to the public records but can cause the same amount of damage if exploited.

- **Maintenance and Code-decay** – Security-conscious developers can ensure that a library or component they use is secure at the time of development but that does not guarantee security throughout its lifecycle. 80% of all 'secure' software suffers eventual code-decay because of the 15,000+ new vulnerabilities found every year.

- **Lack of Transparency and Accountability** – The average project has hundreds of components introduced by dozens of developers, making tracking dependencies a project management nightmare.

- **Licensing Risks** – Open-source components are often mistaken as 'free-for-all' with over 400 different types of open-source licenses in use today, each with their own intricacies. SCA can help enforce compliance policies to ensure that your organisation is clear of any potential licensing liabilities.

How Can We Help

Scantist's SCA platform is enabled by a smart vulnerability analysis engine that utilises a proprietary database of third-party and open-source component fingerprints, along with vulnerability signatures to provide highly accurate results.

Using continuous deep-learning and expert validation to process terabytes of vulnerability data from various sources, we help ensure the protection of your applications from upcoming threats. Scantist's SCA integrates seamlessly into your existing software development lifecycle by plugging in to your version control systems, CI/CD pipelines and issue trackers.

The platform is capable of analysing source-code as well as binaries, allowing you to scan an application irrespective of its stage of development.

The Scantist Advantage

- **Accurate Results** – Our true code and binary-level analysis combined with our proprietary vulnerability databases allows us to find vulnerabilities with an unparalleled level of accuracy.

- **Comprehensive Coverage** – We cover the most widely used languages at the source-code level and over a dozen binary formats within a single unified platform – allowing you to scan almost any web, mobile or native application.

- **Actionable Remediation Reports** – Scantist's SCA not only finds vulnerabilities, it also provides extremely targeted remediation advice to allow quick and accurate fixes. This saves your organisation precious time and resources.

- **Cost-effective Security** – A radical new approach propelled by extensive academic research in close collaboration with industry partners has enabled us to provide a better platform at a huge fraction of the price of our next-best competitor.

Freely used open-source components

Reduced time to market

Business Impact of Scantist Solutions

Direct Impacts

- **Reduced Risk of Data Breach** – An average data-breach costs US$ 3.86 million globally. By eliminating open-source related vulnerabilities, our users reduce their risk of data breach from 32% to 24% - meaning an annualised saving of US$ 310,000 on average.

- **Reduced Identification Time** – Scantist's SCA solution reduces the time taken to identify vulnerabilities by up to 90%, leading to tremendous cost savings from an operations and quality assurance standpoint.

- **Reduced Remediation Time** – An 85% reduction in time and effort required to fix vulnerabilities can be achieved using Scantist SCA, allowing for further cost savings and resource optimisation.

Improved compliance

Indirect Impact

- Greatly **improved release times** with automated security checks

- **Higher velocity** of development and maintenance enabled by risk-free use of open-source

- **Reduced friction** between security and development personnel

- Improved **license compliance and risk management** with regards to open-source use

- **Legal defensibility** in case of a breach

Lower security and compliance costs

Proactive checks for code-decay

About Scantist

At Scantist, we believe that security is a critical enabler of success. Founded in late 2016 as an NTU spin-off, we build upon our deep scientific expertise and extensive research base to create vulnerability management solutions that help organisations better navigate the ever-changing cyber-security landscape.

To find out more, visit scantist.com
Drop us a line at contact@scantist.com
For press related enquires, contact marketing@scantist.com