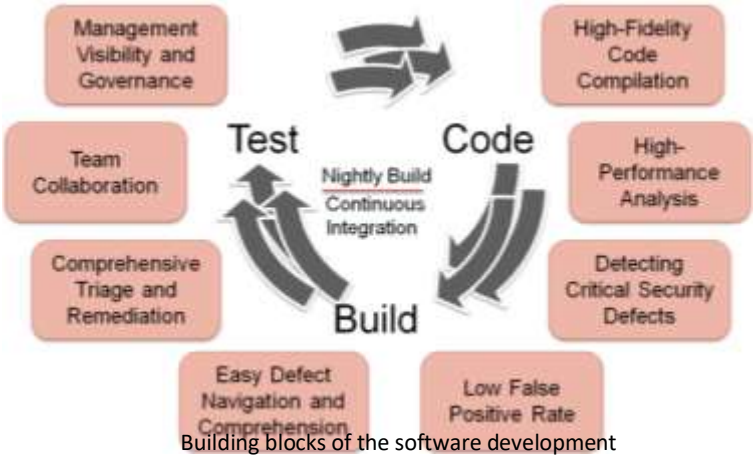
Introduction

Security & Quality Software GmbH offers services and tools for application protection with automatic, integrated testing of the security and quality of software during development with measurable results. OpenSource code and snippets are detected, legal information, versions and known exploits shown. When combining solutions to obfuscate the executables and protect against tampering in conjunction organizations can more securely build, analyze and release applications into production. The tools are integrated in your workflow, IDE's, bug tracking systems, dashboards and build environments. You save money, improve process efficiencies, shorten development cycles and reduce risk measurably.

Software In-house Development

Developers are supported to find critical security & quality flaws in the software early. Bugs are described, explained and the sources indicated. Security & Quality Metrics and Coding Guidelines are automatically applied. Results are:

- Improved Performance and Stability of the application and product
- Identification of security flaws and open doors for attackers
- Security & Quality of the software is measurable
- Information for a better planning of in-house and external software development
- Faster availability of the products/software with cost reductions
- Controlling and planning of delivery times (risk analysis)
- Increased customer satisfaction with more stable and secure products
- Better software maintainability and faster product changes
- Automatization of software development and testing leads to an increase of productivity



Building blocks of the software development

External developed Software

Possible third party software in your code

Using external developed software causes a residual risk. The same security & quality metrics and KPI's as for the in-house development described above have to be applied.

<u>Situation</u>

- Most of the IT departments lack the tools, specialists and money to test external developed code
- The traditional way to test and evaluate the code is expensive, In-complete and doesn't scale
- Supplier don't deliver or give access to their source code

<u>Possible Solutions</u>

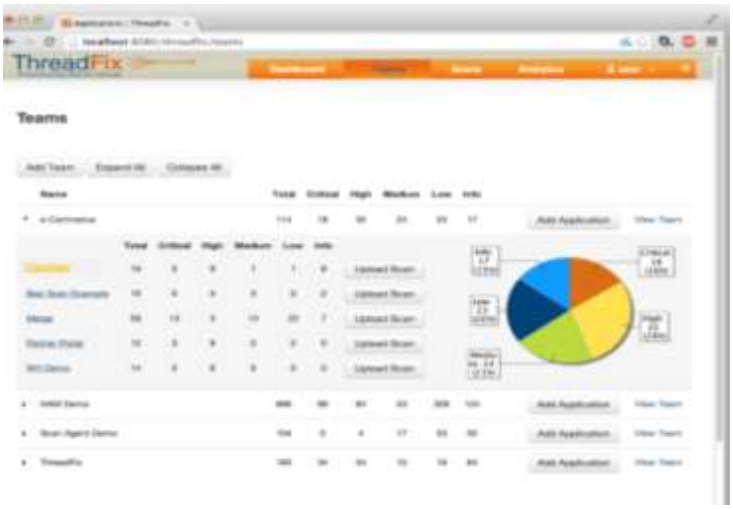
1. You set up a Security & Quality Gate with all the metrics the software has to meet and give the supplier access to. This can be organized in a private cloud.
2. The supplier has tools in-house and tests the software according to your rules and metrics to generate a certificate as point of prove.
3. SQ Software tests the supplier Software according to your rules and delivers a certificate.

Find, prioritize, aggregate and visualize software vulnerabilities

ThreadFix brings together a variety of code analysis tools that enable you to locate and fix potential vulnerabilities in the code you write in the languages you use.

THE PROBLEM

- Application development and security teams use software scanning tools as well as manual testing to assess the security of an application
- Each test delivers results in different formats and duplicates are created because test platforms describe the same flaws differently
- Workflow Implementation is difficult or impossible
- Development teams receive unmanageable reports



THE SOLUTION

- Imports dynamic, static and manual testing results into a centralized platform
- Removes duplicate findings across testing platforms to provide a prioritized list of security faults
- Reduces the time required to fix vulnerable applications.
- Exports prioritized result lists into defect tracker of choice to streamline software remediation efforts for development
- Auto generates web application firewall rules to protect data during vulnerability remediation to reduce risk
- Empowers managers with vulnerability trending reports to pinpoint issues and illustrate application security progress

Consolidated View of Application Test Results
Consolidate and de-duplicate imported results to get a complete view of the state of your applications.

Reports
Get the latest security status of your applications immediately

Defect Tracker Integration
Translate application vulnerabilities into software defects

Virtual Patching
Create virtual Web Application Firewall (WAF) rules to help block malicious traffic while vulnerabilities are being resolved.

Compatible with Open Source and Commercial Products
Dynamic and static scanning technologies, SaaS testing platforms, IDS/IPS, WAFs and defect trackers

Commercial & Free Tool Support:
Dynamic/Static Scanners: OWASP Zed Attack Proxy, Arachni, w3af, Skipfish, Microsoft CAT.NET, FindBugs, Brakeman, CPPcheck *Commercial tools*: Checkmarx, Virtual Forge and other major vendors / WAF, IDS, IPS: Mod Security, Snort / Compliances: PCI, OWASP, Top10, OCI DSS, HIPPA, DISA STIG and more

Freimanner Strasse 14 85737 Ismaning, Germany
Phone: +49 (89) 388 699 84 Kontakt: contact@sq-software.com
www.sq-software.com