GRAMMATECH

DATASHEET

CODESonar®

"CodeSonar helps us to achieve the safety and security that we need eff!ciently, allowing engineers to spend more time developing new and innovative features for our customers."
– Stoneridge, Inc.

Accelerate Application Security

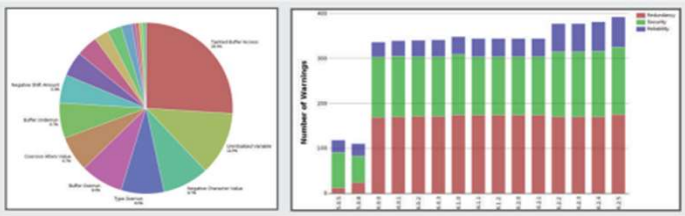
Software teams are under constant pressure to staff their teams and deliver more content with higher complexity, in shorter timeframes, with increased quality and security. Static Application Security Testing is a proven best practice to help software teams deliver the best code in the shortest timeframe. GrammaTech has been a leader in this field for over 15 years with CodeSonar delivering multi-language SAST capabilities for enterprises where software quality and software security matter.

- **DevSecOps – Speed and Scale.** Software developers need rapid feedback on security vulnerabilities in their code. CodeSonar can be integrated into distributed software development environments, works unobtrusively to the developer and provides rapid feedback, with cloud options for analysis in the cloud.
- **Language Support.** CodeSonar supports many popular languages, including C/C++, Java, C# and Android, as well as support for native binaries in Intel, ARM and PowerPC instruction set architectures. CodeSonar also supports OASIS SARIF, for exchange of information with other tools in the DevSecOps environment.
- **Reporting**. CodeSonar provides built-in reports for security standards such as OWASP and SANS Top 25. CodeSonar also includes a custom report builder for the development of specific reports your organization can use to develop a better understanding of the quality and security of your software projects.
- **Security – Depth**. GrammaTech SAST tools use the concept of abstract interpretation to statically examine all the paths through the application, understand the values of variables and how they impact program state by exposing vulnerabilities, and offers hybrid cloud options in response to digital business initiatives and geographically dispersed teams.

Examples of Defects Reported

- Buffer over- and underruns
- Cast and conversion problems
- Command injection
- Copy-paste error
- Concurrency
- Ignored return value
- Memory leak
- Tainted data
- Null pointer dereference
- Dangerous function
- Unused parameter / value

And hundreds more



- **Security.** Broad coverage of security vulnerabilities, including OWASP Top10, SANS/CWE 25. Support for third-party applications through byte code analysis.
- **Quality**. Integration into DevSecOps to improve quality of the code and developer efficiency. Find code quality and performance issues at speed.
- **Privacy**. Checkers that detect performance impacts such as unnecessary test for nullness, creation of redundant objects, or superfluous memory writes.

Team Support Built In

CodeSonar is designed to support large teams. Defects are persistent and tracked across builds, even if code changes. They can be annotated, ranked, assigned, searched for and compared. Support for many team-tools is provided out of the box.

Project Management	Repositories	IDEs	Containers	Orchestration & Automation	Business Intelligence
Jira	GitHub GitLab	eclipse Visual Studio Visual Studio Code	docker		Qlik

Use Cases

- **Enterprise** customers are developing in many languages in their internal applications, either in-house built, or built by a third-party. Static analysis is needed to to improve security and quality to drive business continuity.
- **Mobile and Client** customers are on end-points, sometimes in an internet-of-things deployment, or to provide information to mobile users. Security is critical due to the diverse environment, privacy is top-of-mind as well.
- **Web Apps** drive dynamic content for websites and web-based applications. In a hostile environment tainted data analysis is crucial to assist developers to understand where their applications may be vulnerable.
- **Embedded** application development has seen a tremendous growth in the software component of devices, including a greater reliance on connectivity for control and monitoring. This has increased the pressure on organizations to add static application security testing alongside quality testing in order to ensure reliable and secure operation of their embedded platforms.

Built-In DevSecOps Integration

CodeSonar enables the shift to DevSecOps by integrating with the most popular CI tools such as GitLab, GitHub, Jenkins and others, and offers hybrid cloud options in response to digital business initiatives and geographically dispersed teams. Managers can report on the application security state with their preferred reporting tool. Developers can view and remediate security issues and quality defects within their familiar CI/CD environments, and access more detailed information from CodeSonar with a single mouse click.

Code Understanding

Finding problems is not sufficient, the developer needs to understand the problems that have been uncovered. CodeSonar provides comprehensive code understanding capabilities, helping developers understand and fix issues rapidly.

1. **Textual Descriptions**
Easy, clear textual descriptions describe what the problem is.
2. **Path Visualization**
Shaded background and annotations explain the defect path.
3. **Call Tree Visualization**
To understand how a function fits in the larger application.

- **Metrics and Trends.** CodeSonar allows graphing of complexity and quality trends over time to give the management teams the information they need. Data can be visualized and interactively explored inside of the CodeSonar user interface, or programmatically exported via SARIF and/or XML to be used in third party dashboarding applications.
- **Scalability**. CodeSonar is ultimately scalable. It can do quick scans on subsets of the code on developers' desktops, as well as deep and exhaustive checks including concurrency analysis during regression testing and anything in between. It supports incremental builds and analysis and can use highly parallel and distributed compute farms and GrammaTech Cloud resource for work offloading. CodeSonar can adjust to your software development environment and process.
- **Dashboarding**. An advanced, interactive dashboard plug-in allows managers and security analysts to understand current status and track progress, whether the analysis is hosted on-premises or within the GrammaTech Cloud.

- **Metrics**
- **Dashboards**

- **Process Integration**. CodeSonar is flexible and can provide output in a variety of different formats such as PDF, XML, CSV, and SARIF for easy integration in your process.

The CodeSonar Difference

- **Accurate Analysis.** CodeSonar's highly advanced analysis engine can provide fast analysis of the largest codebases and empower developers to pinpoint defects with greater precision.
- **Functional Safety.** Static analysis is an important technology for developing software that needs to achieve high levels of functional safety. CodeSonar is pre-qualified for the highest levels of safety for the IEC 61508, ISO 26262 and CENELEC EN 50128 standards. Artifacts for qualification according to DO-178C / DO-330 are also available.
- **Analyze Third-Party Code.** CodeSonar for Java and C# analyzes bytecode and then reflects these warnings back into your source-code. This allows the analysis of both your own code as well as third-party applications where source code may not be available.

GRAMMATECH

Corporate Headquarters
6903 Rockledge Drive,
Suite 1250
Bethesda, MD 20817

U.S. Sales: 888-695-2668
International Sales: +1-607-273-7340
Email: sales@grammatech.com

CodeSonar C/C++

Compiler Model Support

- ARM Real View
- Borland
- Clang
- CodeVision
- Cosmic
- Freescale CodeWarrior
- Green Hills
- Gnu
- Keil
- Hi-Tech
- IAR
- Intel
- Microsoft
- MPLAB
- QNX
- Renasas
- SHARC, TigerSHARC, Blackfin
- TASKING
- Texas Instruments
- Wind River

Functional Safety

- Pre-qualified for the highest levels of safety for the IEC 61508, ISO 26262 and CENELEC EN 50128 standards.
- Artifacts for qualification according to DO-178C / DO-330 are also available.

Safety and Security Standards Support

- **Safety Critical**: MISRA-C and MISRA-C++, AUTOSAR C++-14, JSF++
- **Security**: CERT, DISA STIG, OWASP, CWE

CodeSonar Java and C#

Warning Classes

CodeSonar includes a complete range of checkers for security, quality, efficiency and style, some examples:

Security

- Injections
- Cryptography
- External Entity Reference
- Cookies
- Passwords
- LDAP

Quality

- Nullness
- Approximation
- CloseResource
- DeadCode
- BadEq
- EqualsHashCode

Frameworks Supported

- **Java**: Apache-CXF, AspectJ, EJB, JAX-RS, JAX-WS, JPA, JSP, Jersey, RESTeasy, RESTlet, Servlet, Spring, Android
- **C#**: Unity, WebForms, WindowsForms, MVC

IDE Support

- Eclipse
- Microsoft Visual Studio
- Microsoft Visual Studio Code

System Requirements

- **Host**: Windows, Linux, FreeBSD, NetBSD
- **Hardware**: 2+ Cores, 2+GB of RAM, 15+GB of disk
- **Compilers**: Supports most popular and embedded compilers
- **Languages**: C/C++, Java, C#, Binaries
- **Output**: SARIF, XML, CSV, PDF, HTML