CODESONAR FOR BINARIES

Intel and ARM Processors

PRODUCT DATA SHEET

Static Analysis for Binary Code

Don't compromise. Validate your application and system software, as well as your whole software supply chain, even when you don't have access to source. Use CodeSonar's highly innovative binary analysis technology to find security vulnerabilities and bugs in third-party libraries, drivers, middleware, and more.

Analyze Whole Executables with **VR-Mode**

When you don't have access to source code, use CodeSonar's **VR-Mode**. CodeSonar can analyze binary executables, enabling you to perform security and quality analyses on code you didn't write.

Because CodeSonar doesn't rely on debugging or symbol-table information, it can examine the stripped binary executables that third-party software vendors typically ship, allowing you to perform a security audit on software, ensuring you don't ship defective software.

Additionally, machines execute binary code, and high-level languages such as C/C++ leave many matters unspecified, which a compiler must resolve. By analyzing code that has already been compiled, you include any bugs, optimizations, or unplanned behaviors that have been introduced by the compiler's decisions.

Analyze Libraries with **Mixed Mode**

CodeSonar's **Mixed Mode** is perfect for customers concerned about the robustness or security of either their own or third-party software for which a source-code-level analysis is either unavailable, or insufficient for the level of confidence needed in the software.

Within **Mixed Mode**, you can leverage CodeSonar's binary analysis and source code analysis platforms together, to perform an audit on your entire software, including both the code you've written and the third-party libraries your application relies on, i.e. drivers, middleware, etc.

Analyzing application source code together with binary code enables CodeSonar to understand how the application interacts with the libraries.

Sample Checks:

Security

- Buffer Overrun / Underrun
- Command Injection Vulnerability
- Integer Overflow of Allocation Size
- Double Free
- File System Race Condition
- Free Non-Heap Variable
- Shift Amount Exceeds Width
- SQL Injection Vulnerability
- Unreasonable Size Argument
- Use After Close/Free
- Unsafe Format String

Reliability

- Deadlock
- Division By Zero
- Null Pointer Dereference
- Resource Leak

Redundancy

- Free Null Pointer

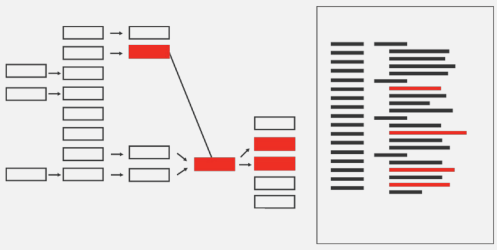
Style

- High Risk Loop

Fix Bugs Fast

Harness CodeSonar's award-winning code visualization technology and other workflow features to fix defects more efficiently.

Machine code can be complicated, subtle, and difficult to understand. CodeSonar provides English explanations about what's happening in the code at the particular point of a detected error, to help engineers who might not know all of the subtle details of machine code.



With CodeSonar's tainted data analyses, you can track input data through the code, even if you only have access to the program binaries.

GRAMMATECH

FOR MORE INFORMATION
www.grammatech.com

U.S. SALES 888-695-2668
INTERNATIONAL SALES +1-607-273-7340
EMAIL sales@grammatech.com