

# Armament SEC

## Software Architecture and Integration Lab

The Software Architecture and Integration Lab (SAIL) was established to improve software security and reliability through early and continuous vulnerability detection of source code flaws and weaknesses. Many programs are seeking to simply “check the box” when it comes to Software Assurance (SwA), and do not realize the benefits of integration into the development cycle or at least early coding vulnerability assessment. Vulnerability analysis, through the use of automated tools and manual review by experienced software analysts, will improve code quality and reduce system adversary exploitation. SAIL will also serve to train developers on the use of effective techniques that will maintain and continuously improve code quality while reducing vulnerabilities. During development, vulnerabilities and functional defects can be identified, resulting in increased software security and decreased development/sustainment costs.

SAIL integrates the output from multiple tools into a consolidated report. A combination of government, commercial, and open source tools are selected based on the target software language. Multiple tools are used to obtain full spectrum coverage, allowing our experienced analyst to generate the highest quality reports with minimal false positive and negative findings.

Mandated by the 2013 and 2014 Defense Authorization Acts, our goals are to incorporate SwA capability into the ARDEC SEC software development lifecycle, and to provide ARDEC SwA expertise and services to PEOs/PMs.

