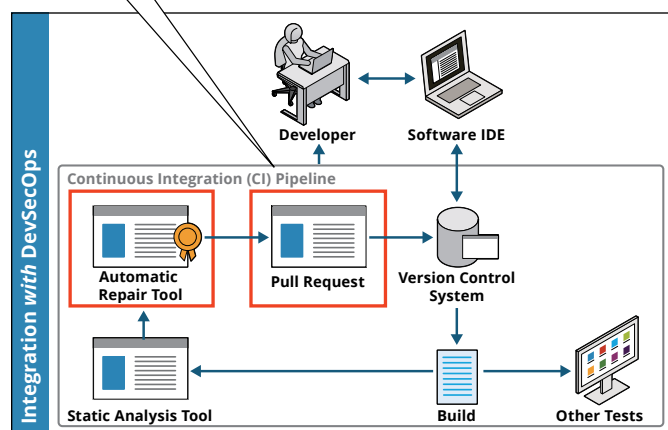
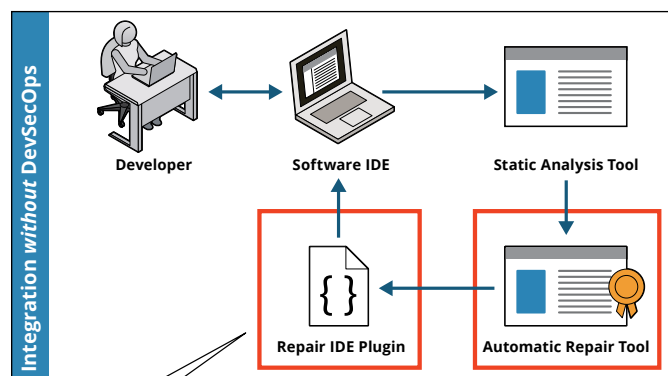


Static Analysis-Targeted Automated Repair: Securing Code and Reducing Effort

Automated Program Repair (APR) with the Redemption Tool

Static analysis tools often produce **too many** alerts to audit them all. Even if we knew which alerts were true positives, there are still **too many true positives** to repair all of them manually.

Our tool, Redemption, automatically repaired source code for **100%** of static analysis alerts for two types of code flaws—**EXP34-C/CWE-476** and **EXP33-C/CWE-908**—even if the alert was a false positive, in a way that **preserves soundness** and **resolves** the alert. It can also repair **MSC12-C/CWE-561**.



Our Tool Currently Repairs

Category	CERT Rule	CWE	Repair
Null Pointer Dereference	EXP34-C	476	Insert null check.
Uninitialized Value Read	EXP33-C	908	Initialize variable at declaration.
Ineffective Code	MSC12-C	561	Delete ineffective code.

Sample Alert Test Results on OSS Codebases

CERT Rule	CWE	zeek	zeek	zeek
		clang-tidy	cppcheck	rosecheckers
EXP33-C	908	100.0%	100.0%	
EXP34-C	476	100.0%	100.0%	100.0%
MSC12-C	561		40.0%	

CERT Rule	CWE	git	git	git
		clang-tidy	cppcheck	rosecheckers
EXP33-C	908	100.0%	100.0%	
EXP34-C	476	100.0%	100.0%	100.0%
MSC12-C	561		20.0%	

Timing Git Tests

	User	System	Elapsed
Unrepaired	337.99	308.69	11:24.65
	341.06	318.04	11:38.17
Repaired	339.08	313.82	11:31.41
	339.54	311.17	11:28.83



Scan the QR code with your smartphone camera or point your web browser at the link below for more information about our tool on GitHub.

github.com/cmu-sei/redemption



Scan the QR code with your smartphone camera or point your web browser at the link below to learn more about our Redemption project.

sei.cmu.edu/projects/automated-repair-of-static-analysis-alerts-redemption-of-false-positives

About the SEI

The Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD).

Contact Us

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu