KDM Analytics

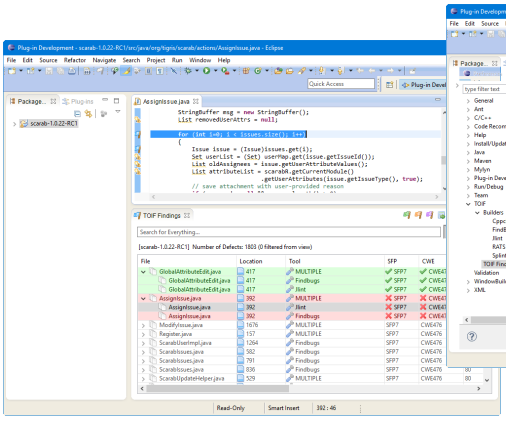
PRODUCT INFO

Quantify, Measure, & Prioritize CyberSecurity Risk

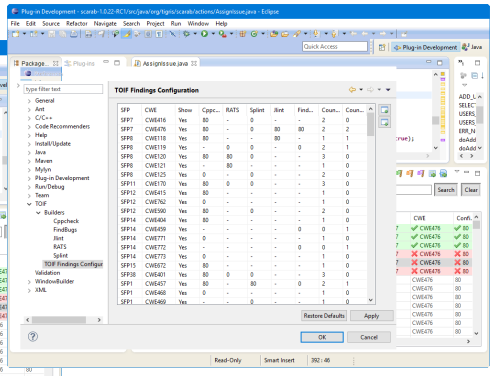
Blade Tool Output Integration Framework

Overview

Blade Tool Output Integration Framework (TOIF) is a powerful software vulnerability detection platform. It provides a standards-based environment that integrates the outputs of multiple vulnerability analysis tools in a single uniform view with unified reporting. It leverages OMG Software Assurance Ecosystem standards, Software Fault Patterns (SFPs), and Common Weakness Enumerations (CWEs).



Blade TOIF Prioritized Findings Report & associated source file



Blade TOIF Findings Report priority settings

Composite Vulnerability Analysis & Reporting

Blade TOIF's plug-and-play environment provides a foundation for composite vulnerability analysis by normalizing, semantically integrating, and collating findings from existing vulnerability analysis tools.

- Improves breadth and acccuracy of off-the-shelf vulnerability analysis tools.
- Provides powerful vulnerability analysis and management environment for analyzing, reporting and fixing discovered weaknesses.

Seamless Integration

Out-off-the-box, Blade TOIF seamlessly integrates into the Eclipse Development Environment and with five open-source vulnerability analysis tools:

- CppCheck
- RATS
- Splint
- SpotBugs
- Jlint

It enables strategic use of commercial and open-source vulnerability analysis tools and, in conjunction with its unified priority reporting, reduces the overall costs of performing a vulnerability assessment by 80%.

Blade TOIF Integration

Integrates into Eclipse development environment:

- Execute Blade TOIF (desktop deployment) from within Eclipse with progress bar
- Automatically see defect findings in Eclipse
- Use the "Run TOIF" easy button in the Eclipse toolbar and in the Project main menu
- Run it on a sub-set of project files/ directories
- Filter the defect findings listed in the Blade TOIF Findings view, based on the selected project data in the Project Explorer in Eclipse

KDM Analytics helps to answer the most important question of cybersecurity risk management: where should you focus your budget and resources?

Blade Tool Output Integration Framework

Blade TOIF Features & Options

Blade TOIF is offered on a per-seat subscription basis. The Blade TOIF package includes two components: server/load build, and desktop deployments. Results from the server can be shared at all subscribed desktops.

	Blade TOIF Server	Blade TOIF Desktop
Targeted to load build type of environment	✓	
SCA tools are run outside of TOIF environment and results are imported and merged inside TOIF	✓	
SCA tools run as command lines; results must be manually imported to Findings Viewer	✓	
Configurable prioritized reports	✓	✓
Export to .csv format to view data in spreadsheet or import into Blade TOIF Desktop	✓	✓
Results from server shared at all subscribed desktops	✓	✓
Default confidence per tool per SFP/CWE	✓	✓
Targeted to integrated development environment (Eclipse) developers at the desktop		✓
SCA tools are run within the integrated development environment (Eclipse); results are automatically passed to Report Viewer		✓
SCA tools take compile environment (includes, defines, etc.) from integrated development environment (Eclipse) project file/settings		✓
Installation wizard and preferences of SCA tools options		✓
Thread pooling of some SCA tools		✓

Combining Blade TOIF with our automated risk analysis platform, Blade Risk Manager, provides a comprehensive cybersecurity risk management solution that includes:

- Automated risk analysis
- Automated vulnerability detection and analysis
- Traceability
- Measurement and prioritization that make it easy to plan how to best leverage the risk management budget and resources for greatest impact.

Blade TOIF Key Capabilities

- Integrates multiple vulnerability detection tools and their findings as “data feeds” into a common repository
- Addresses wider breadth and depth of vulnerability coverage
- Common processing of results
- Normalizes and collates “data feeds” based on discernable patterns described as Software Fault Patterns (SFPs) and CWEs
- Provides one prioritized report with weighted results across tools/vendors
- Uses an RDF repository and provides external Java API for additional analysis capabilities
- Integrates out-of-box with: CppCheck, RATS, Splint, SpotBugs and Jlint
- Defect Description view provides information related to the cluster, SFP, and CWE description of the selected defect instance in the Blade TOIF Findings view
- Defect findings, including citing information, can be exported to *.tsv file and subsequently imported to another Blade TOIF project
- Installation wizard, auto-detection and configuration of open source software (OSS) static code analysis (SCA) tools
- Supports load build integration to import results generated from the server/load build to the desktop

KDM Analytics

For more information, please visit www.kdmanalytics.com or contact us at info@kdmanalytics.com

Washington, DC, U.S.A.
Phone: (202) 756-2488
Fax: (866) 238-0184

Ottawa, Ontario, Canada
Phone: (613) 627-1010
Fax: (866) 238-0184