



What We've Learned from SATE

Arthur "Code Curmudgeon" Hicken

Chief Evangelist

3/25/14



More security
rules

Better handling
of large code
bases

Better multi-
core
performance

Smaller
memory use

Faster

How do you compare tools?

Baseline for accuracy and performance

Repeatable results

No need to justify

Easier
Suite
Analysis

More
code

Publish
unfound

Better dead-
code
method

Improve
code vs
"other"
issues

.NET

Android

universally
unfound

Unexpected
unfound

CWE status

- Too broad
- Ambiguous

CWE to map tools

- Ballpark – maybe
- Precise – no
- Two “rules” for the same CWE may look for entirely different things
- Two engines look in different ways, find different instances

Always:

More rules

More accurate

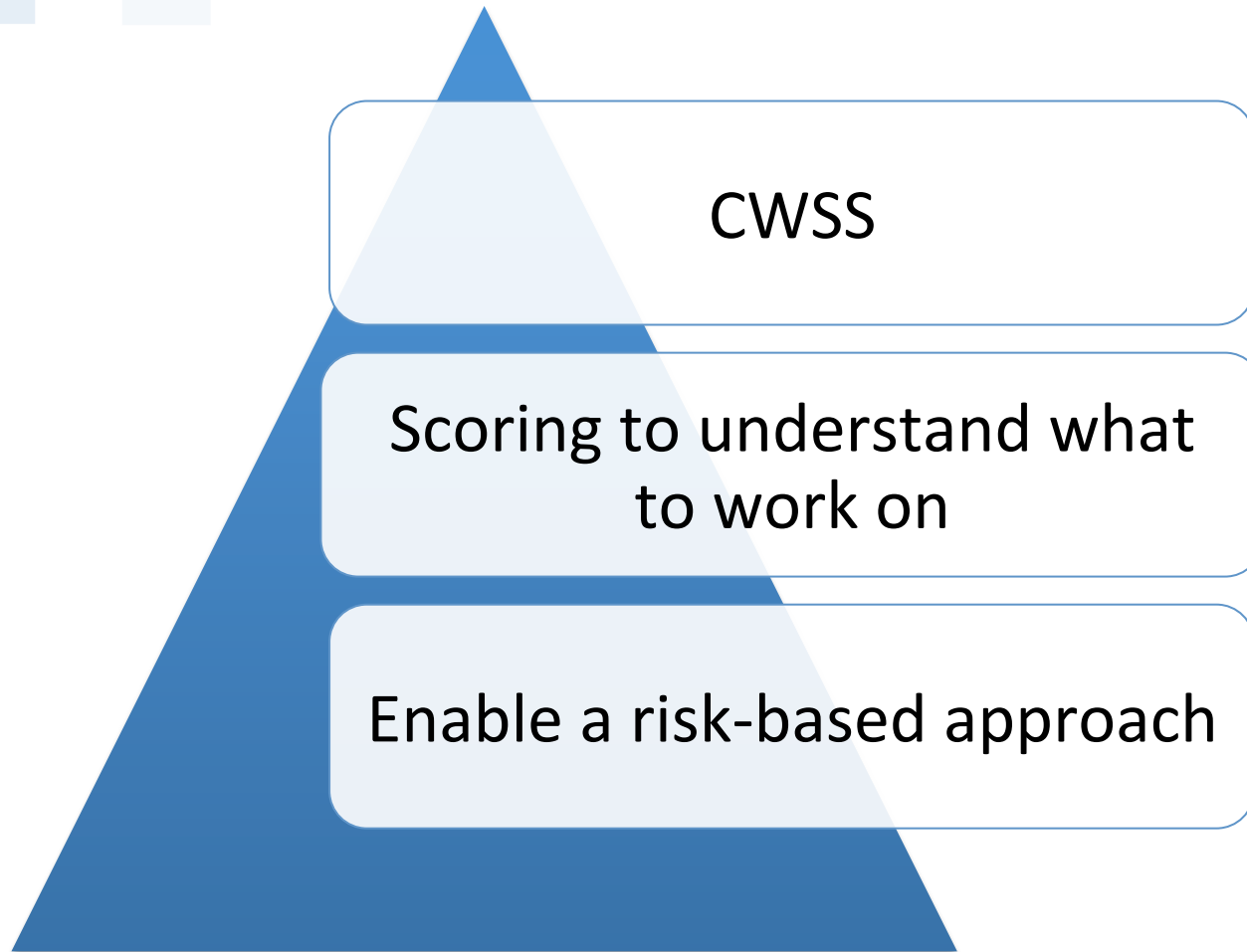
Lighter/
faster

Full CWE map

Possible new
CWE
items

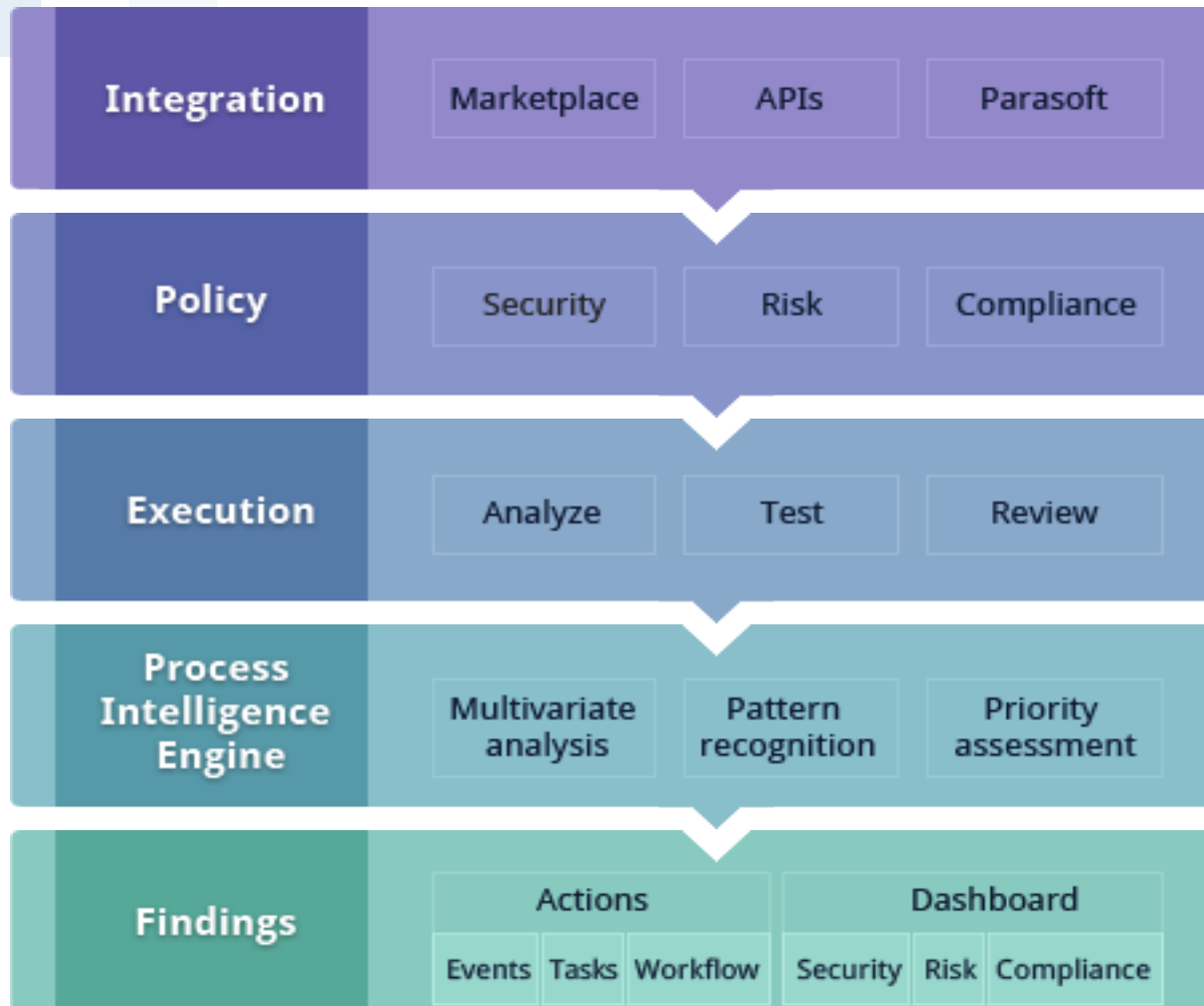
Analytics

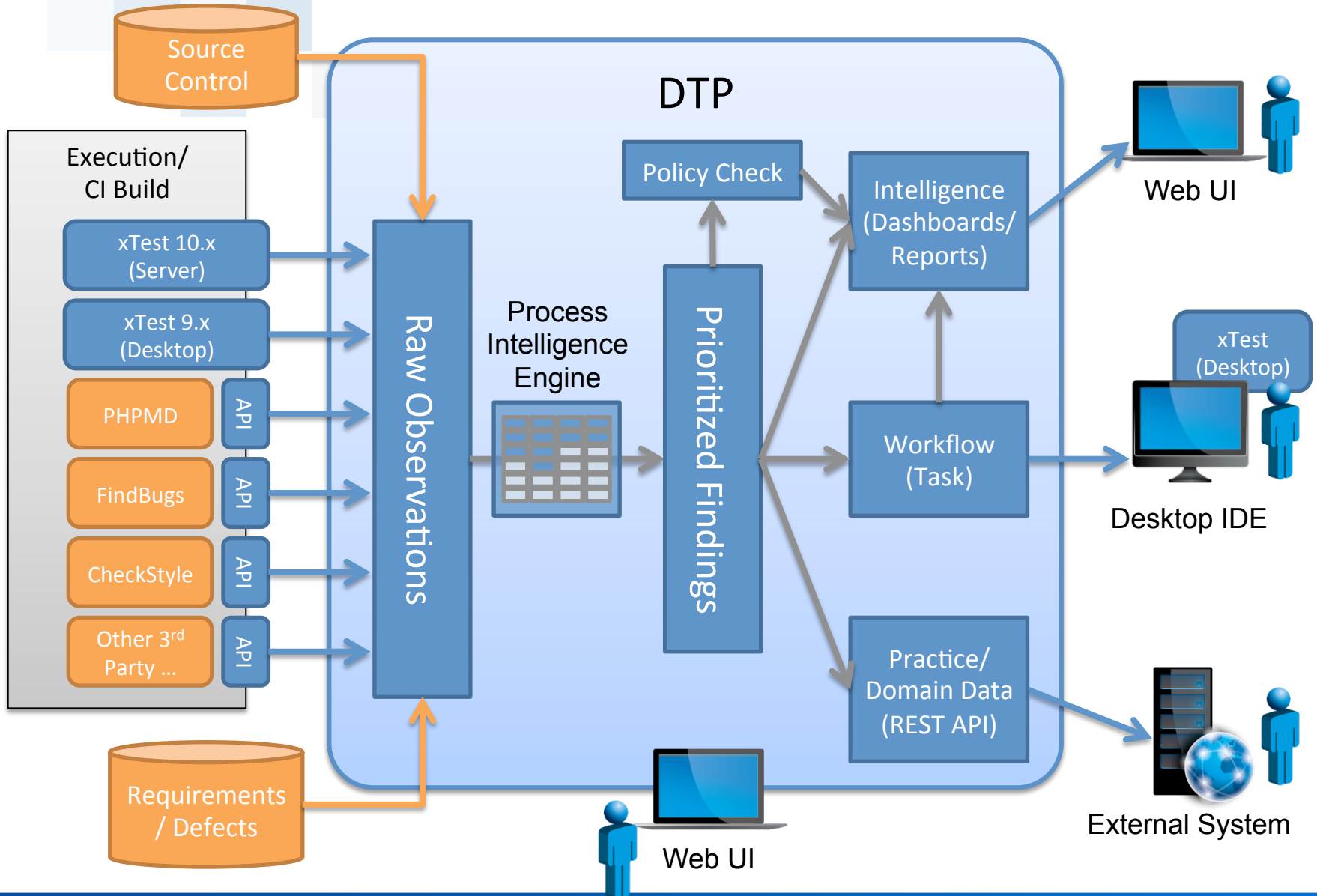
- False Positives – Perception vs. reality
 - It's not just semantic
- False negatives
- Compare/combine tool results
- Finding what's most important
- Coverage – what was really checked?



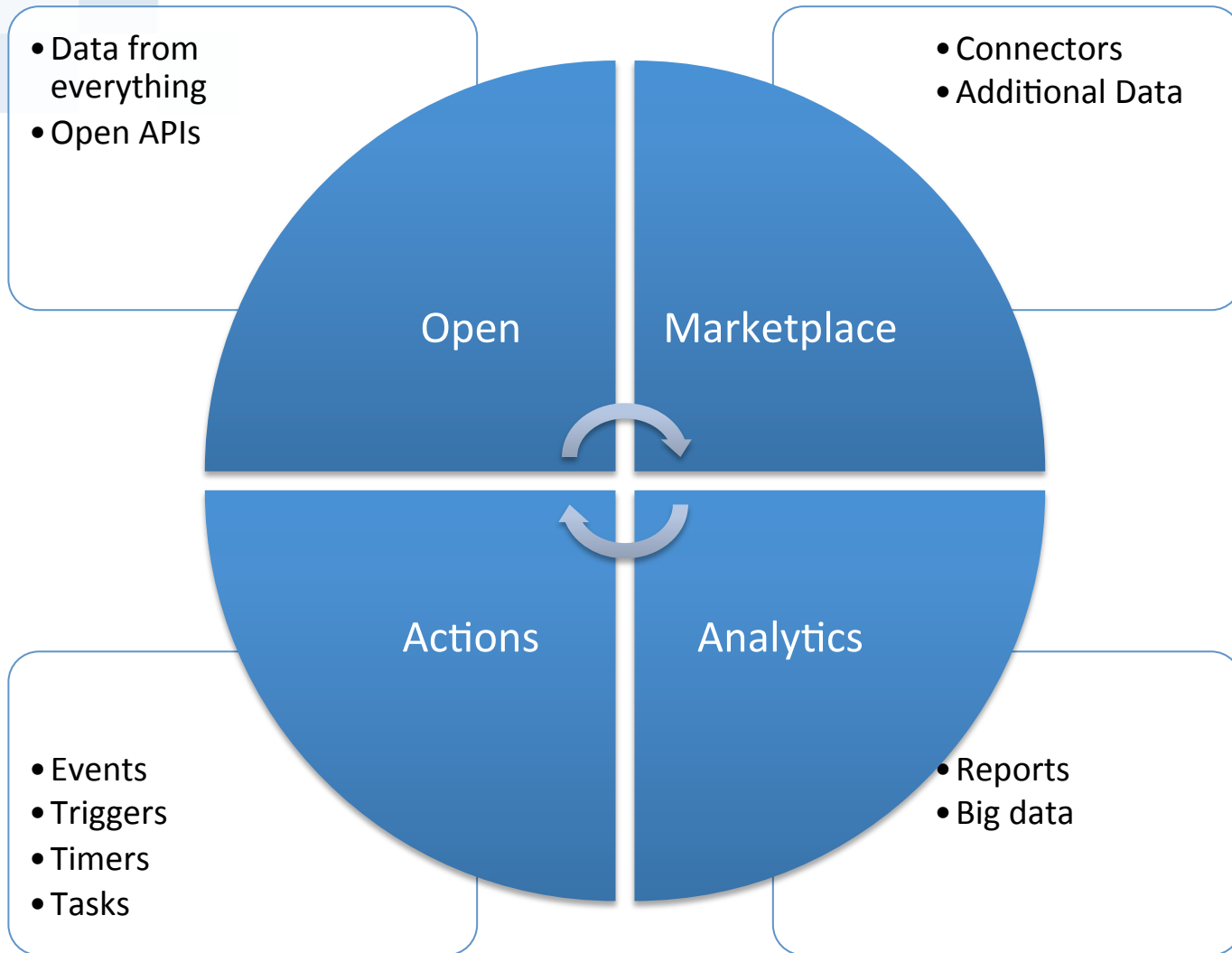
Parasoft's **Process Intelligence Engine**











- Microsoft apps without programming
- Test alerts via iOS
- CWSS via Android
- NVD - Protecode



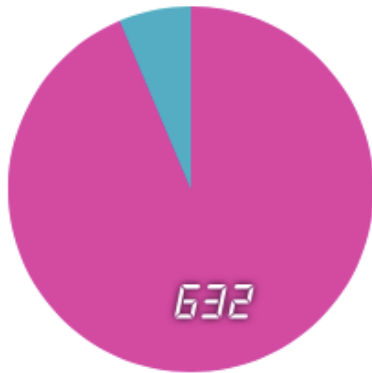
Samples outside the server

iOS Simulator - iPhone Retina (3.5-inch) / i
Carrier 1:45 AM

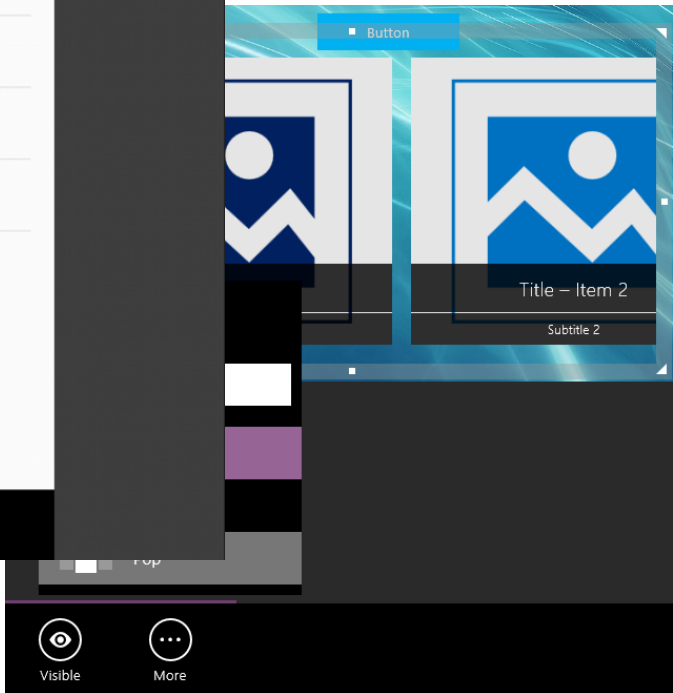
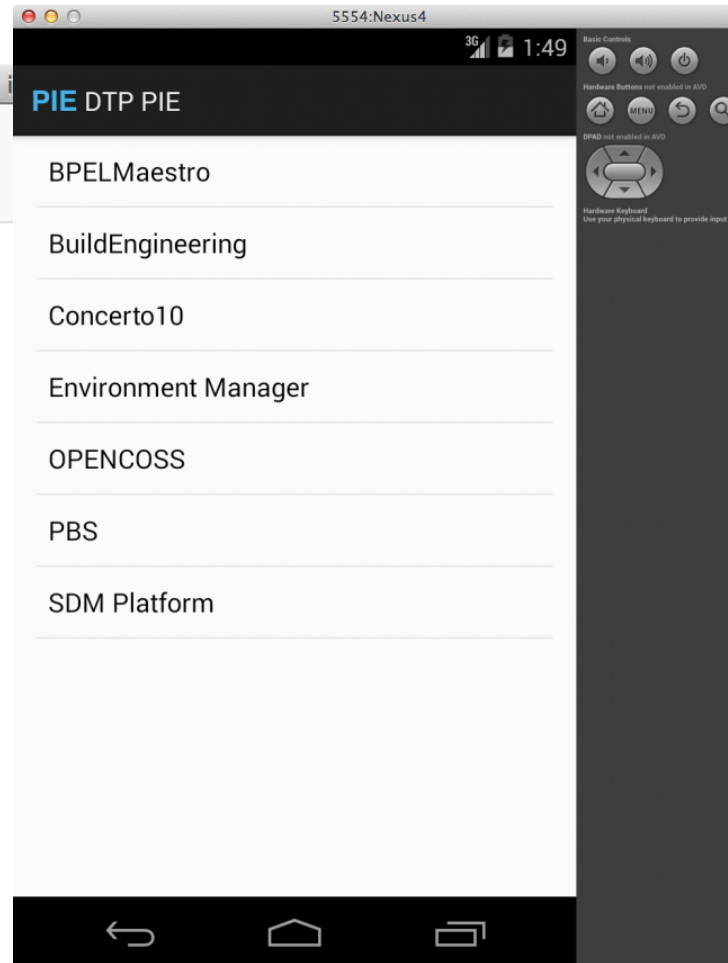
Projects ProserveTools

Static Analysis Violations: 632

Unit Test Failures: 43



Warn Team!



STATIC ANALYSIS

Add Widget

Statistics

Project Statistics

KLOC	689
Files	125
Packages	3,250
Functional Points	28,524

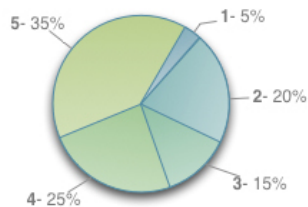
Run Statistics

Run Time	2:25
Total # of Rules	92
-Security	29
-Optimization	12
-Performance	21
-Reliability	25
-Maintainability	5

Violations Overview

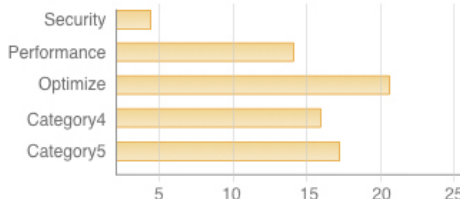
Total Violations	Density per Code	Average Density for Authors	Rules in Compliance
4213 ↑133	42 /KLOC ↑0.03%	210 ↑5.24	85% ↑3%

Violations by Severity



Severity	# of Violations
1	28
2	99
3	62
4	125
5	184

Violations by Category



Top 5 Author with Most Violations

Author	Total	Per Code
W. Ariola	54	3.80
A. Hicken	12	1.70
I. Kirilinko	6	0.80
R. Jaamour	4	0.70
J. Min	2	0.35

Compliance

Rule Categories	Passed / # of Rules	0%	% of Compliance	100%
Security Rules	19/20	95%		
Performance	25/30	83.3%		
Category 3	10/15	66.7%		
Category 4	46/50	92%		
Category 5	43/45	95.6%		

Security

Security Category	Status
Category 1	2 Failed
Category 2	Passed
Category 3	Passed
Category 4	5 Failed
Category 5	Passed

Top 5 at Risk Files

File	Severity	Error Density
UnitSuccess.java	High	High
SuccessTest.java	High	Low
RunUnitTest.java	High	Medium
UnitSuccessTest.java	Medium	Medium
RunTest.java	Low	High

Parasoft Marketplace x

https://marketplace.parasoft.com/

Parasoft Marketplace guest

Marketplace

Show: All File Types All Marketplaces

Previous 1 2 Next

Reset Filters

Public Marketplace

Nolio

Nolio's multi-release solution enables continuous delivery across the application lifecycle. By connecting to the Parasoft Virtualize REST API via Parasoft's Environment Manager, Nolio

Tool Extension [Details](#)

Tags: Accelerate API Automate Build Connector Continuo...

Sentinel

Connector for the Sentinel Application Performance Management software API. Allows you to, monitor, troubleshoot, and automate your application using the Sentinel API. This

Tool Extension [Details](#)

Tags: API APM Application Automate Connector Manage...

dynaTrace

Connector for the dynaTrace Application Performance Management software API. Allows you to, monitor, troubleshoot, and ex your application using the dynaTrace API. This will

Tool Extension [Details](#)

Tags: API APM Application Automate Connector dynaTrac...

HP ALM

Connector for the HP Application Lifecycle Management API. Allows you to easily manage your application through the Software development life cycle using the HP ALM management

Tool Extension [Details](#)

Tags: ALM Application Connector Development HP Lifecyc...

AppDynamics

Connector for the AppDynamics Application Performance Management software API. Allows you to, monitor, troubleshoot, and automate your application using an AppDynamics API.

Tool Extension [Details](#)

Tags: API APM AppDynamics Application Automate Conne...

Connector

Connector for the IBM Quality Manager Application Lifecycle Management API. Allows you to easily manage your application through the Software development life cycle using the IBM

Tool Extension [Details](#)

Tags: ALM Application Connector Development IBM Lifecy...

Splunk

Connector for the Splunk Application Performance Management software API. Allows you to, monitor, troubleshoot, and automate your application using the Splunk API. This

Tool Extension [Details](#)

Tags: API APM Application Automate Connector Manage...

Microsoft TFS

Connector for the Microsoft Team Foundation Server Application Lifecycle Management API. Allows you to easily manage your application through the Software development life cycle using

Tool Extension [Details](#)

Tags: ALM Application connector Development Foundation...

Wily

Connector for the Wily Application Performance Management software API. Allows you to, monitor, troubleshoot, and automate your application using the Wily API. This will

Tool Extension [Details](#)

Tags: API APM Application Automate Connector connecto...

Virtualize HTTP Traffic File Merge Tool

A tool that can automatically merge any number of Virtualize HTTP traffic files. Can be added to either TST files or PVN files.

Network Virtualization Controller

Tool for communicating with a Network Virtualization server and configuring 'Single User Mode'

Version: 1.0

Wireshark PCAP file conversion tool

A tool that takes the .pcap file format that can be created using the Wireshark network protocol analyzer and creates an output file that is consumable as a traffic file by Parasoft



- Web
 - <http://www.parasoft.com/jsp/resources>
- Blog
 - <http://alm.parasoft.com>
- Social
 - **Twitter:** @Parasoft @CodeCurmudgeon
 - **LinkedIn:** <http://www.linkedin.com/company/parasoft>
 - **Google+:** +Parasoft +ArthurHickenCodeCurmudgeon
 - **Google+ Community:** Static Analysis for Fun and Profit