PARASOFT®

What We've Learned from SATE

Arthur "Code Curmudgeon" Hicken
Chief Evangelist

3/25/14

Improvements since SATE IV

PARASOFT

More security rules

Better handling of large code bases

Better multi-core performance

Smaller memory use

Faster

Using Juliet as a standard

PARASOFT

- How do you compare tools?
- Baseline for accuracy and performance
- Repeatable results
- No need to justify

Juliet wish-list

PARASOFT

Easier Suite Analysis

- Better dead-code method
- Improve code vs "other" issues

More code

- .NET
- Android

Publish unfound

- universally unfound
- Unexpected unfound

CWE wish-list

PARASOFT

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

Parasoft Next Steps

PARASOFT

Always:

- More rules
- More accurate
- Lighter/ faster

Full CWE map

- Possible new CWE items

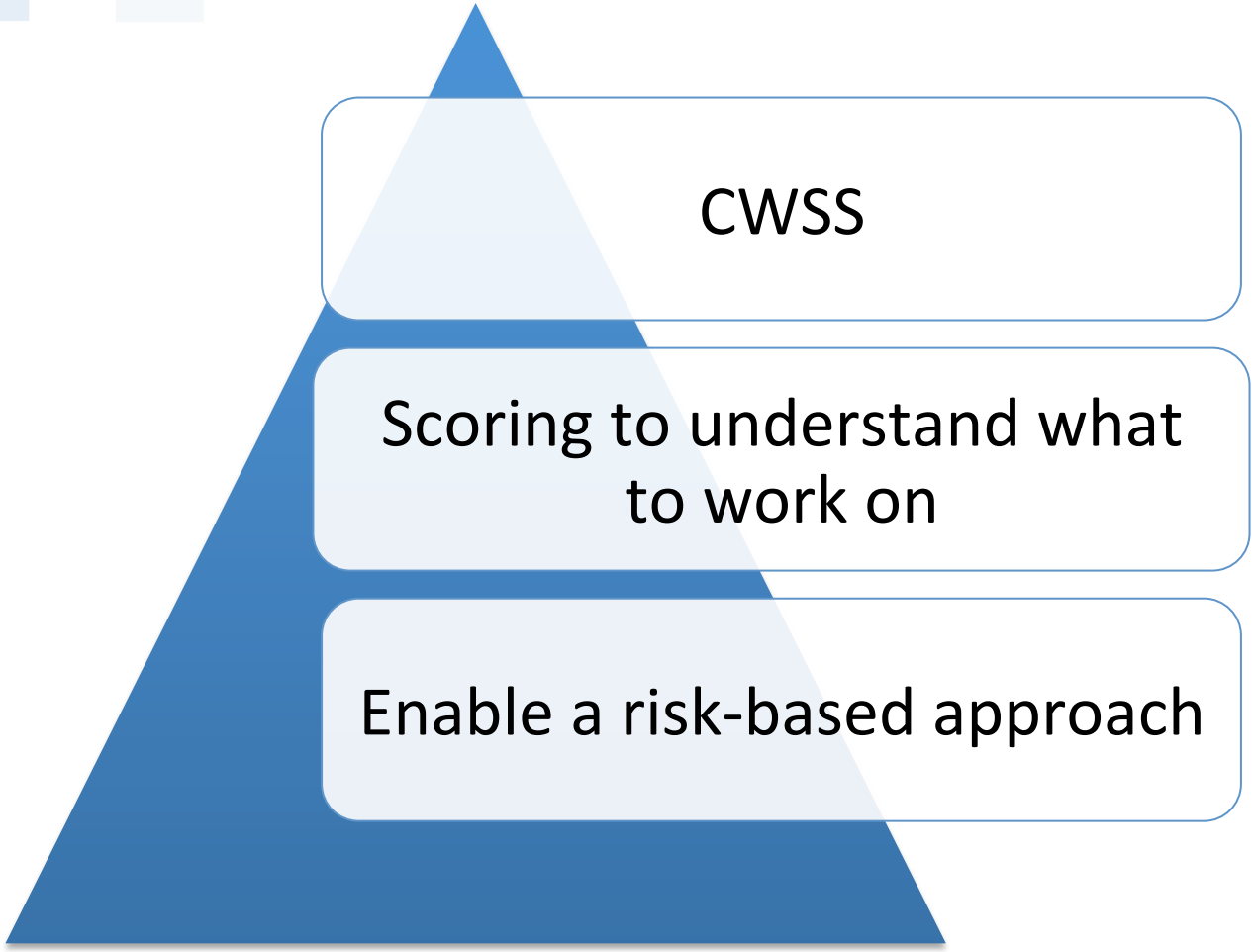
Analytics

Current problems with Static Analysis

PARASOFT

- 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?

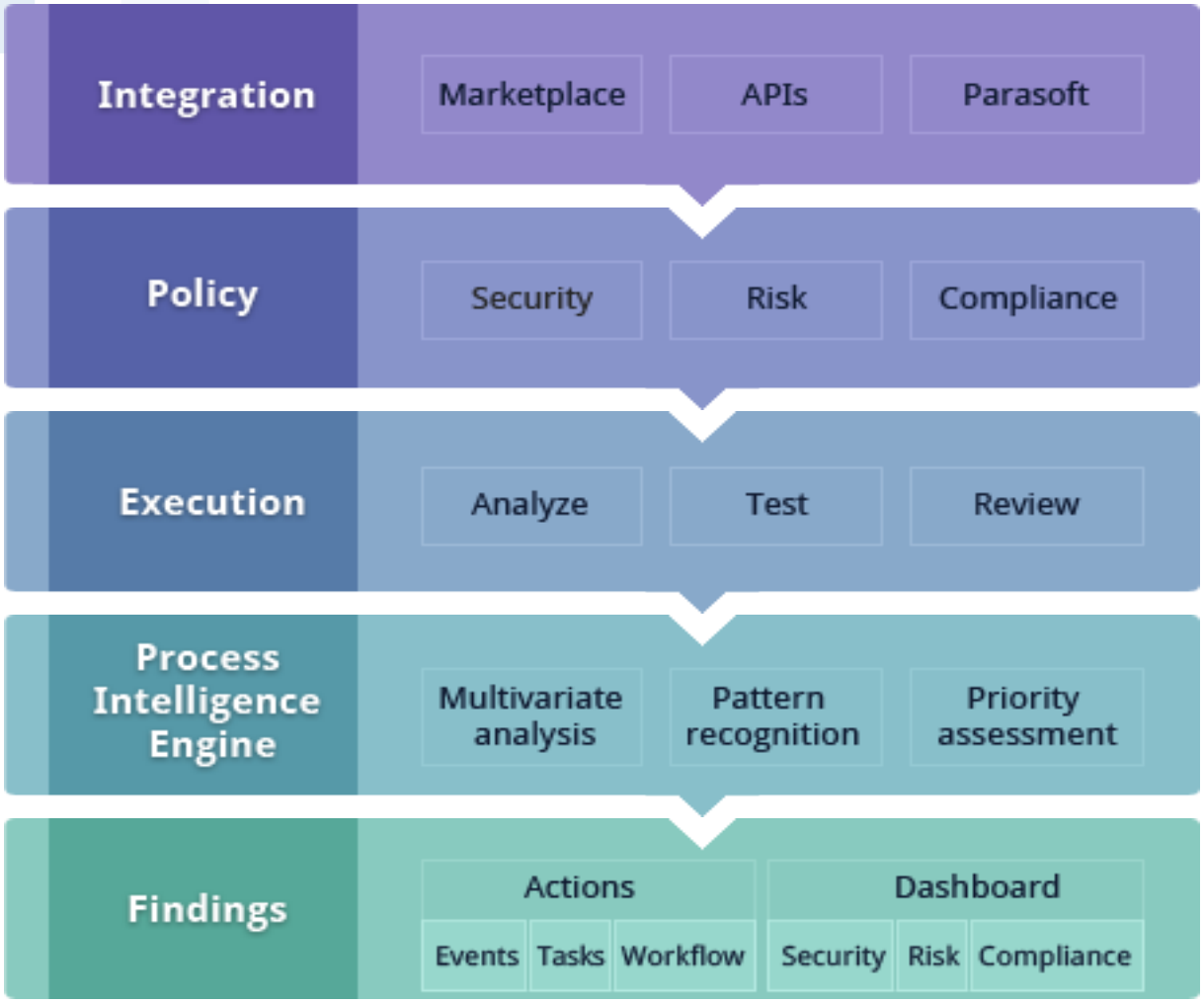
Pleasant discovery



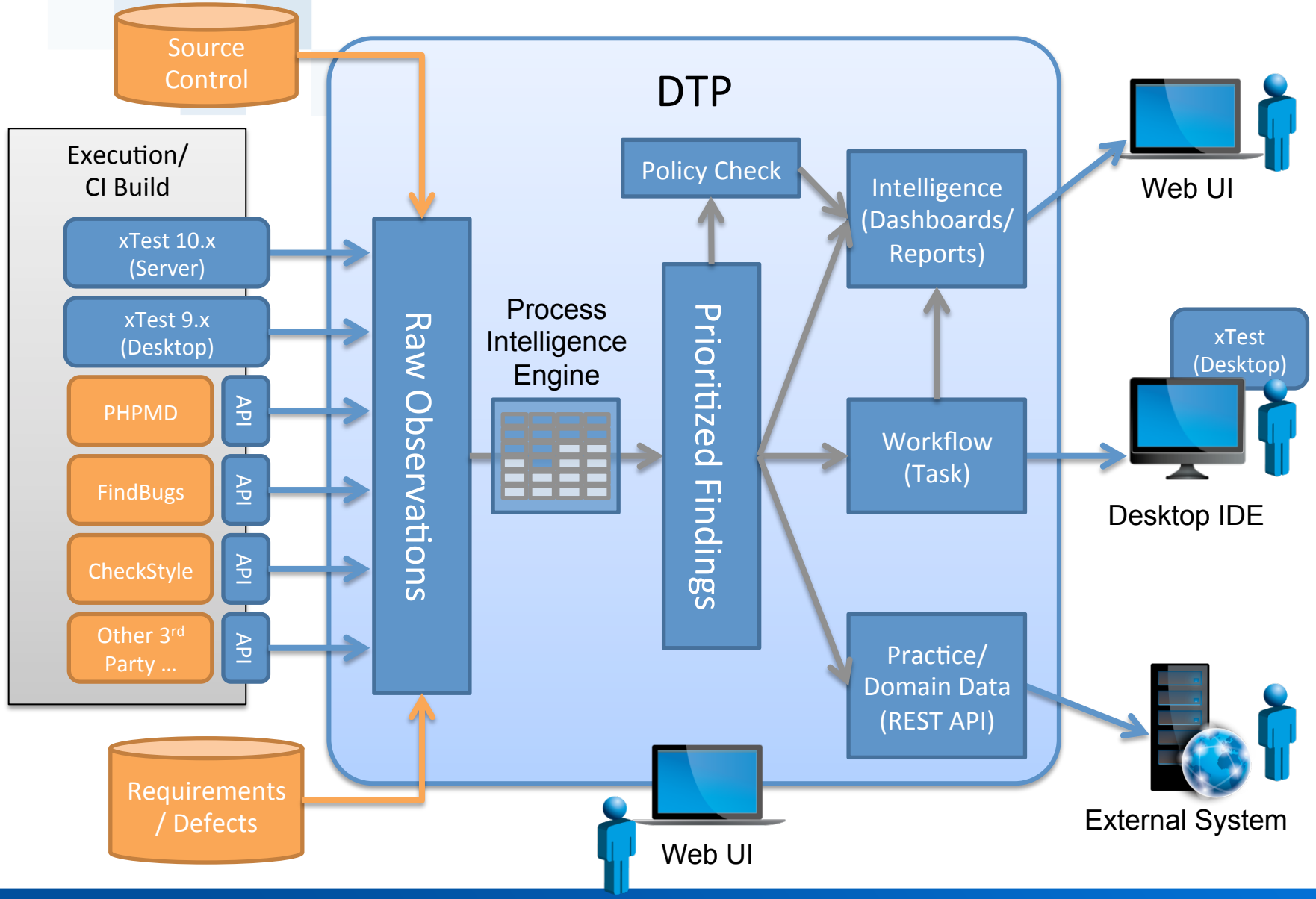
PARASOFT

Parasoft's Process Intelligence Engine

Parasoft Development Testing Platform

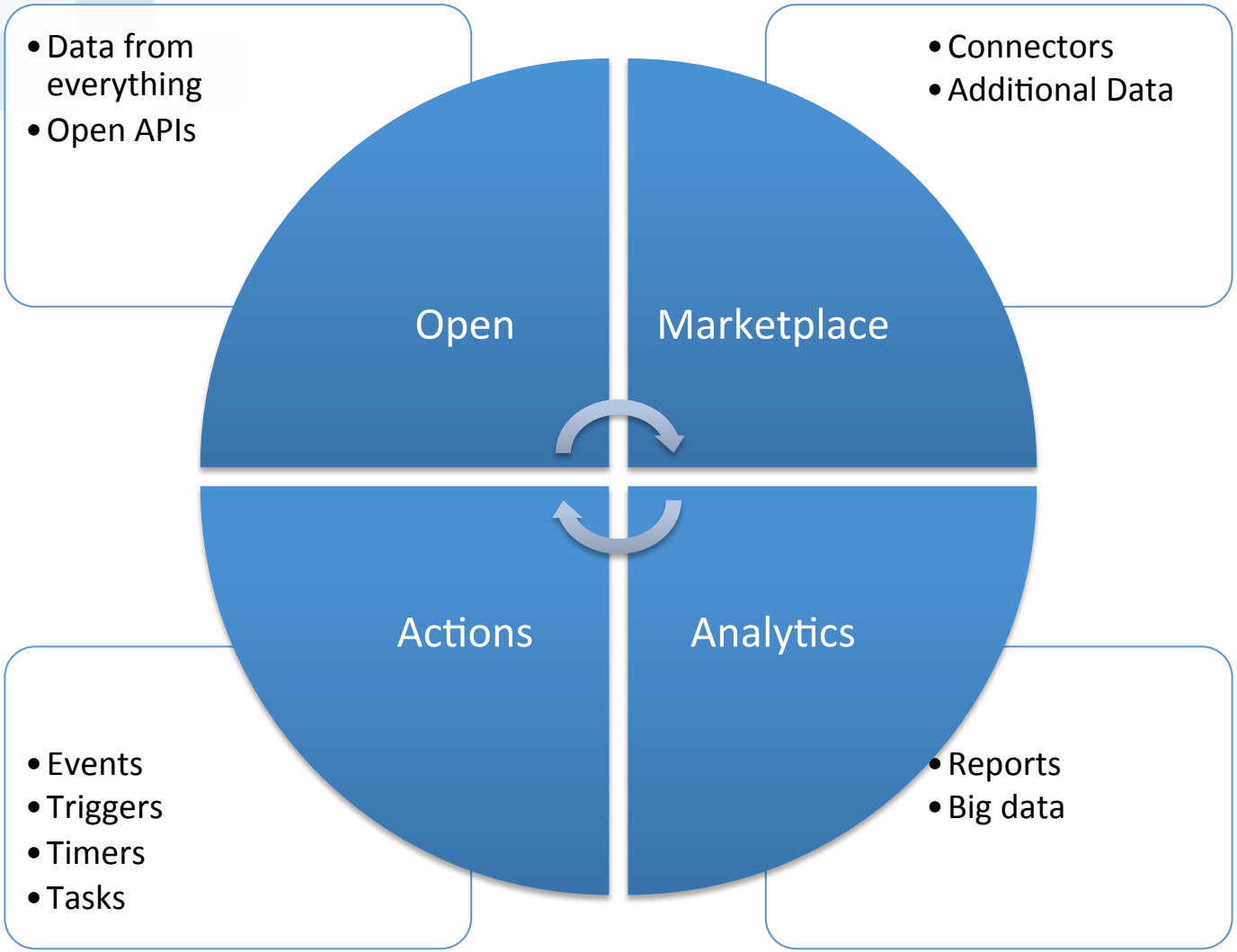


Parasoft Development Testing Platform



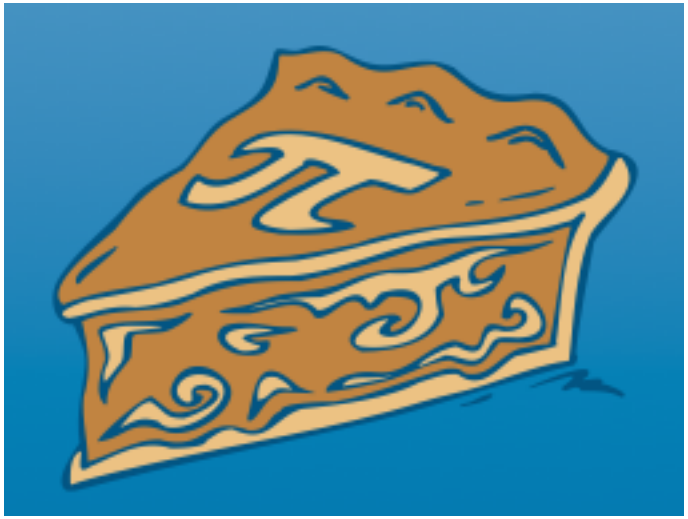
Data from everywhere

What is P.I.E.

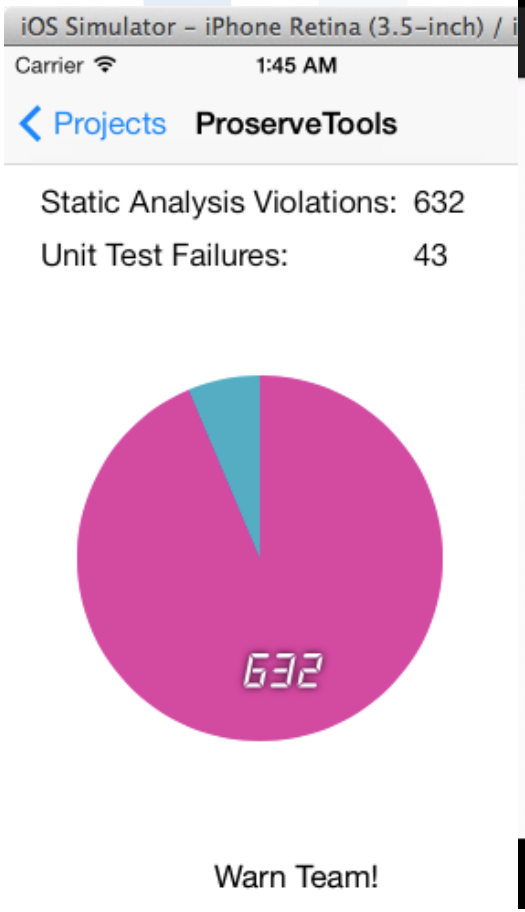

• Data from everything
• Open APIs
• Connectors
• Additional Data
Open
Marketplace
Actions
Analytics
• Events
• Triggers
• Timers
• Tasks
• Reports
• Big data

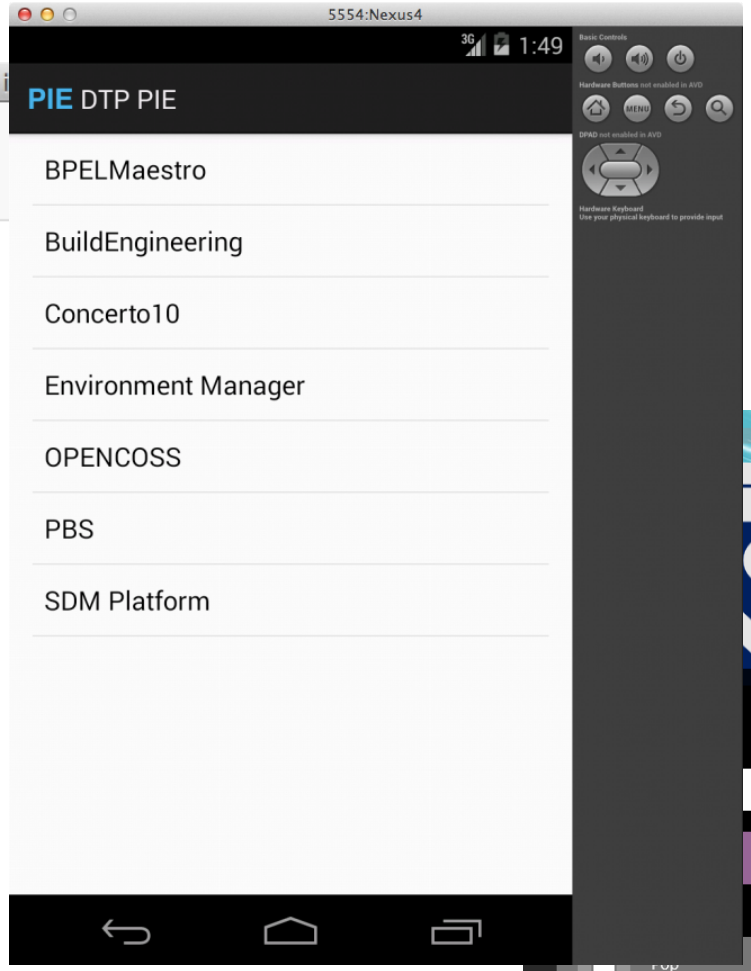
Piedeas

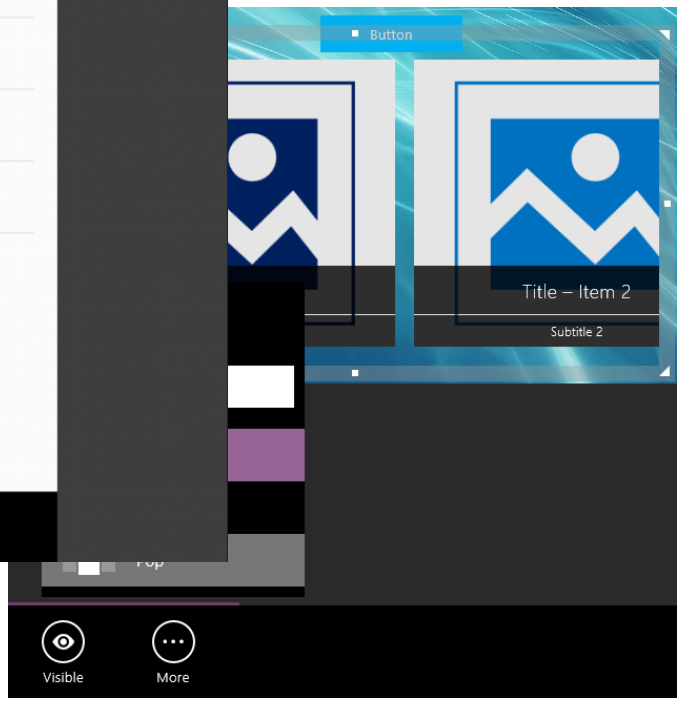
- Microsoft apps without programming
- Test alerts via iOS
- CWSS via Android
- NVD - Protecode



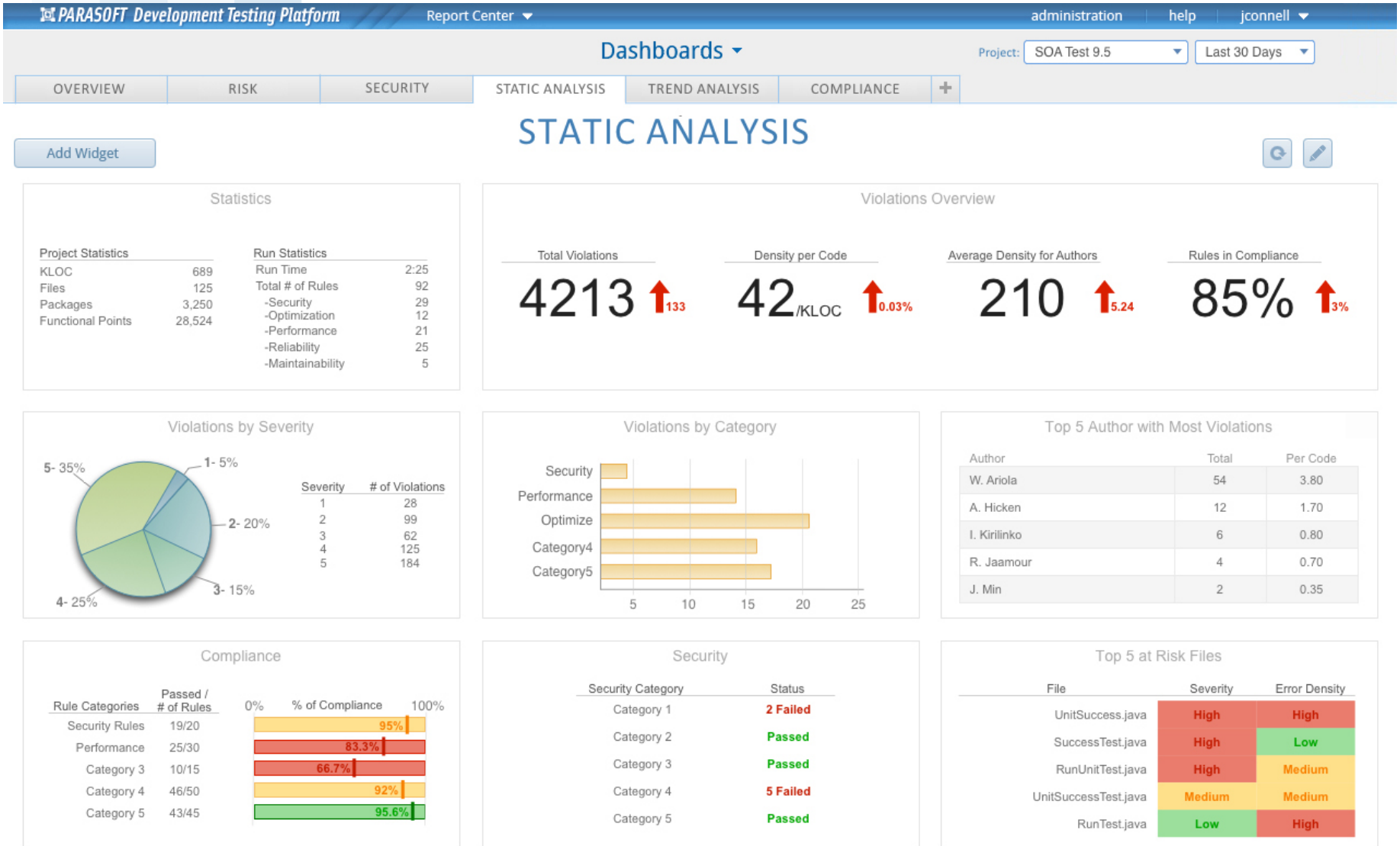
Samples outside the server



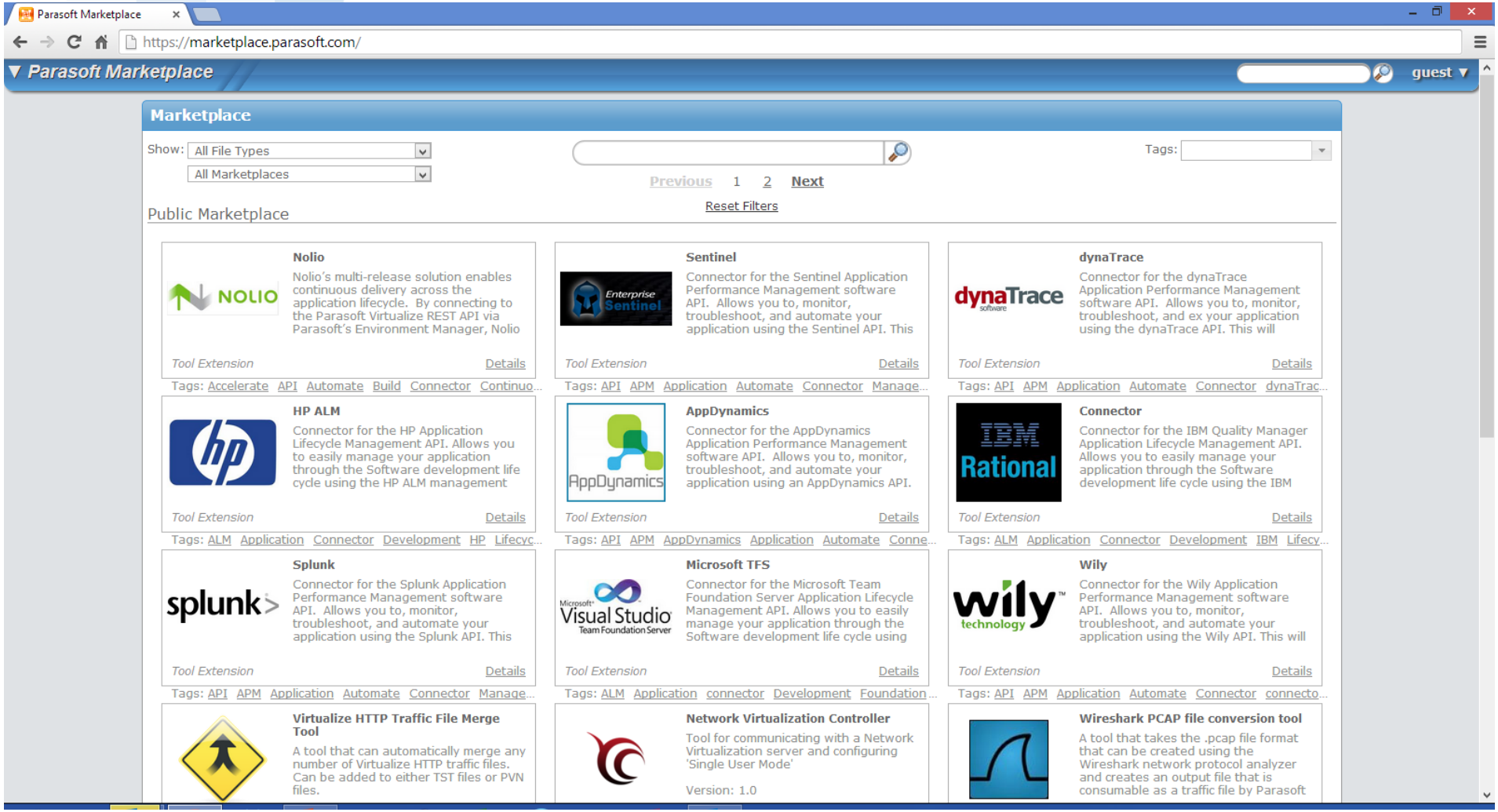




Report Center



Marketplace



- 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