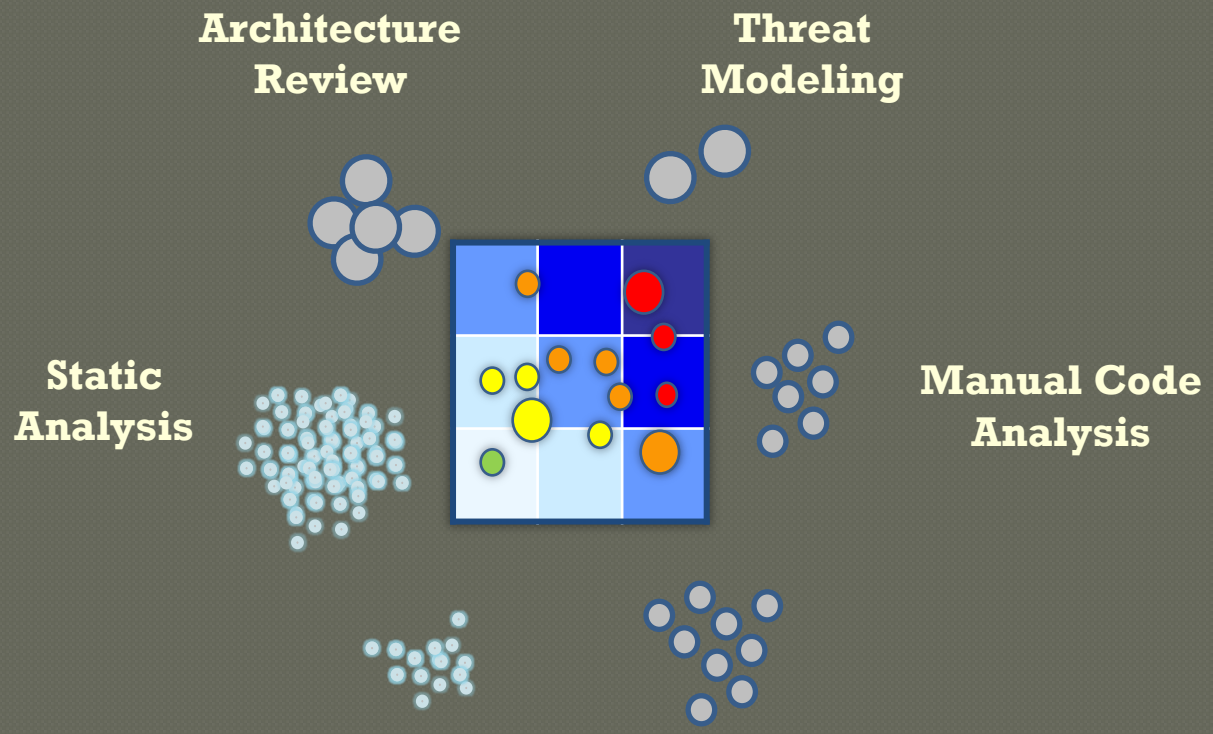
Understanding IAST

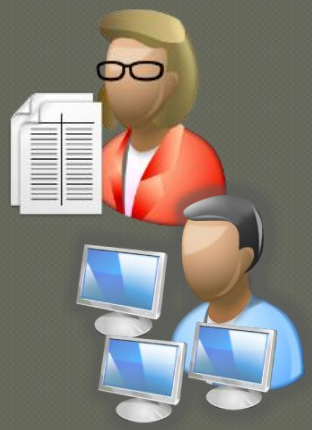
"Intrinsic" Application Security Testing

Jeff Williams, CEO

ASPECT SECURITY
Application Security Experts

OWASP AppSec DC
April 4, 2012





How do we find vulns?

Portfolio Assurance Strategies

Scan

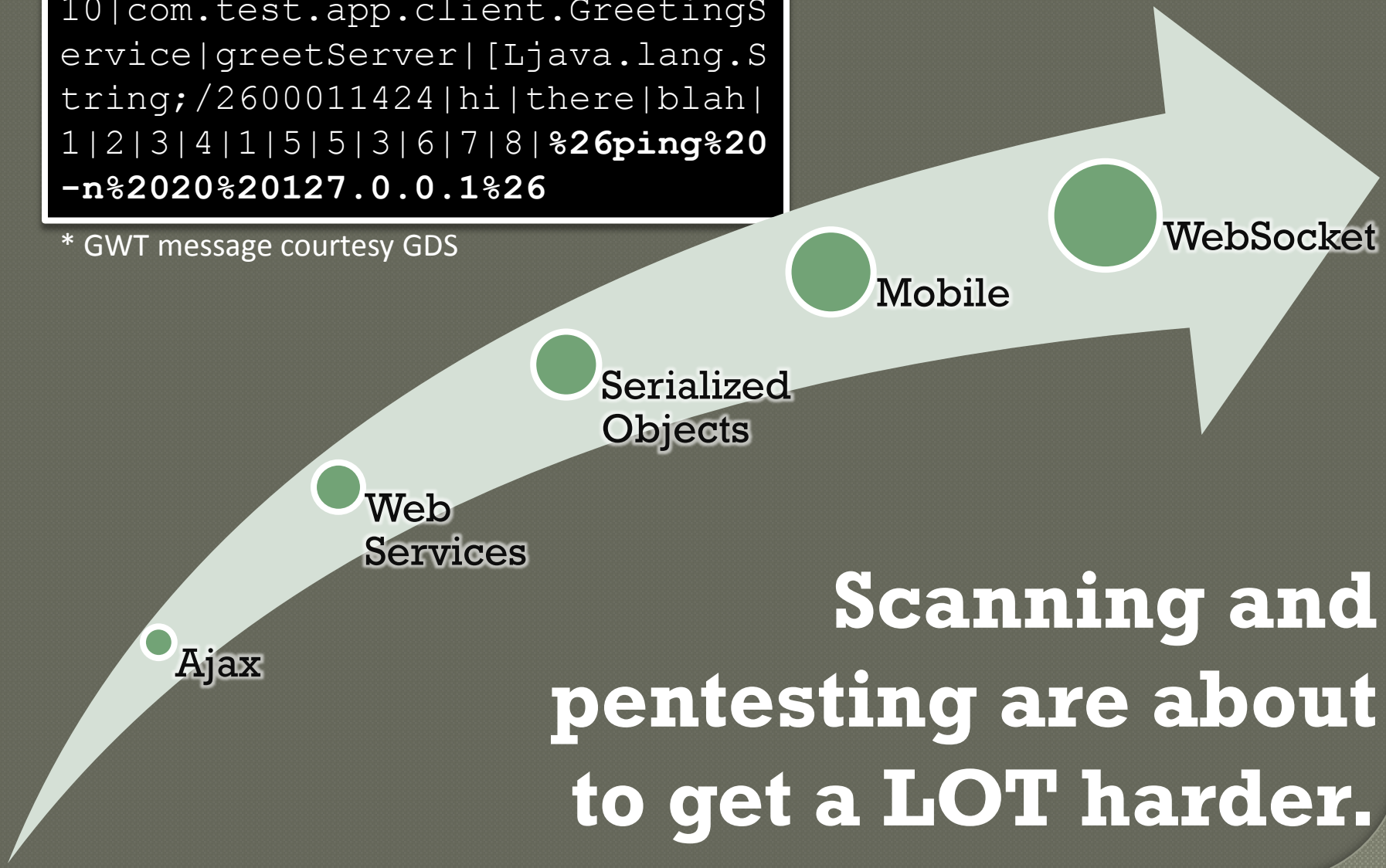
Manual

Spend

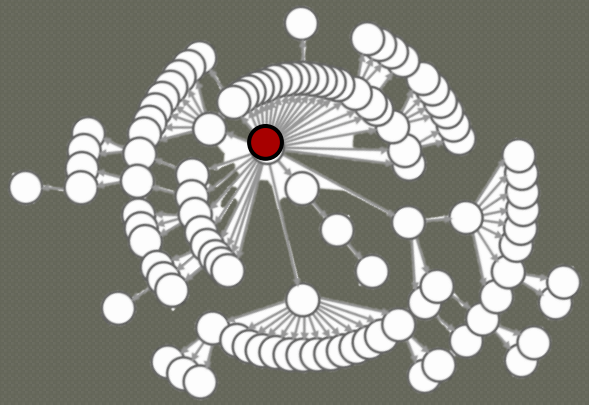
Pray

```
5|0|8|http://tester:8888/testapp
/|9E4CB3D5635C548906BFB576DD18C7
10|com.test.app.client.GreetingS
ervice|greetServer|[Ljava.lang.S
tring;/2600011424|hi|there|blah|
1|2|3|4|1|5|5|3|6|7|8|%26ping%20
-n%2020%20127.0.0.1%26
```

* GWT message courtesy GDS



Scanning and pentesting are about to get a LOT harder.



Lines of Code

Libraries and Frameworks

AOP

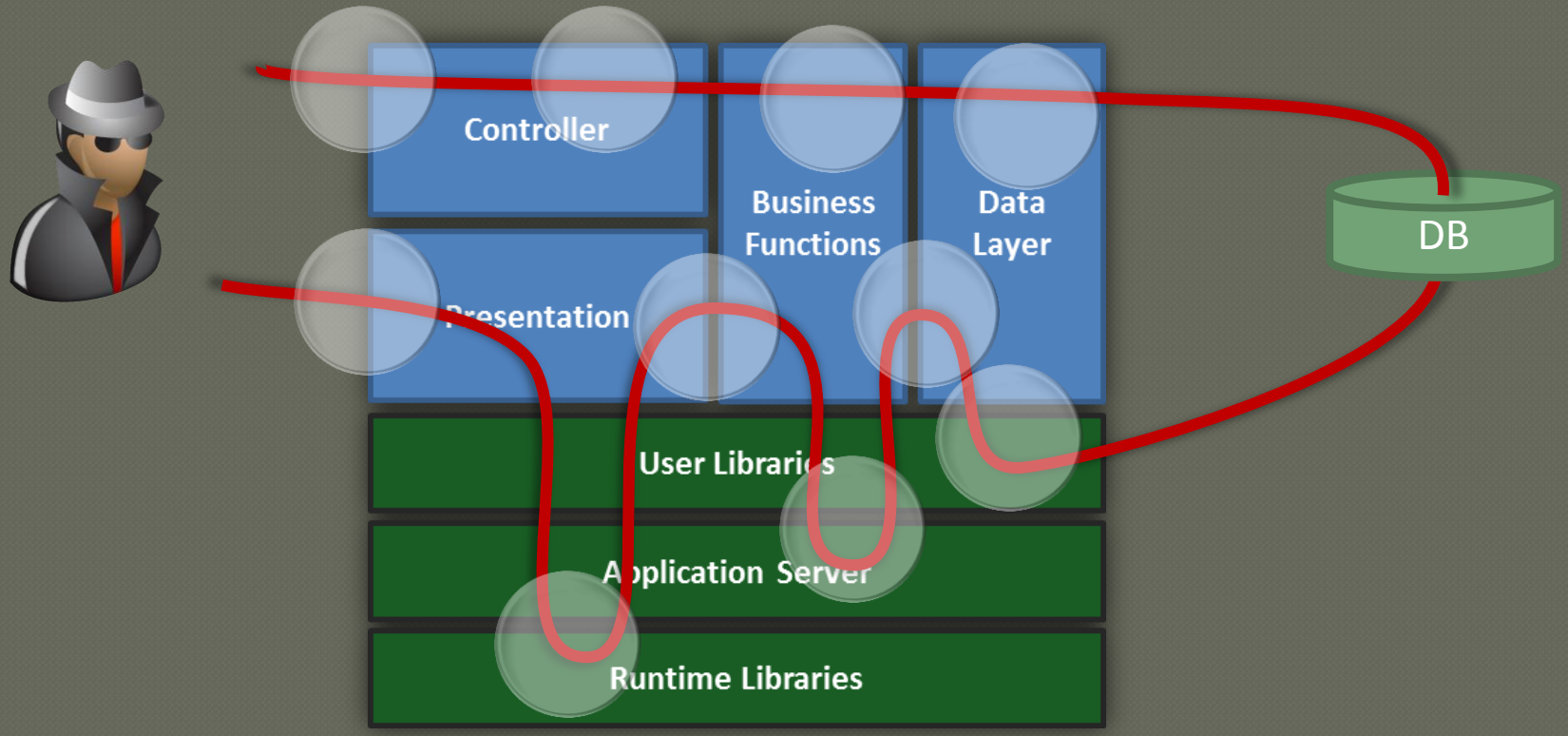
Custom Controls

DevOps

Static analysis and code review are about to get a LOT harder.

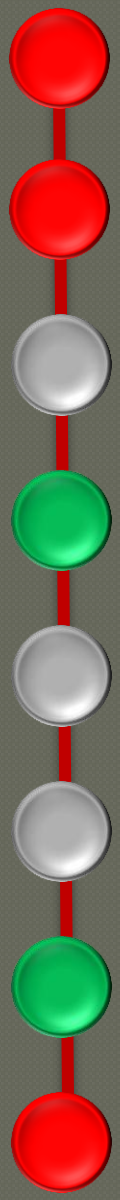
We can do better.

We have to do better.



What does a vuln look like?

Vulnerability Trace



Untrusted Input

Source

Propagator

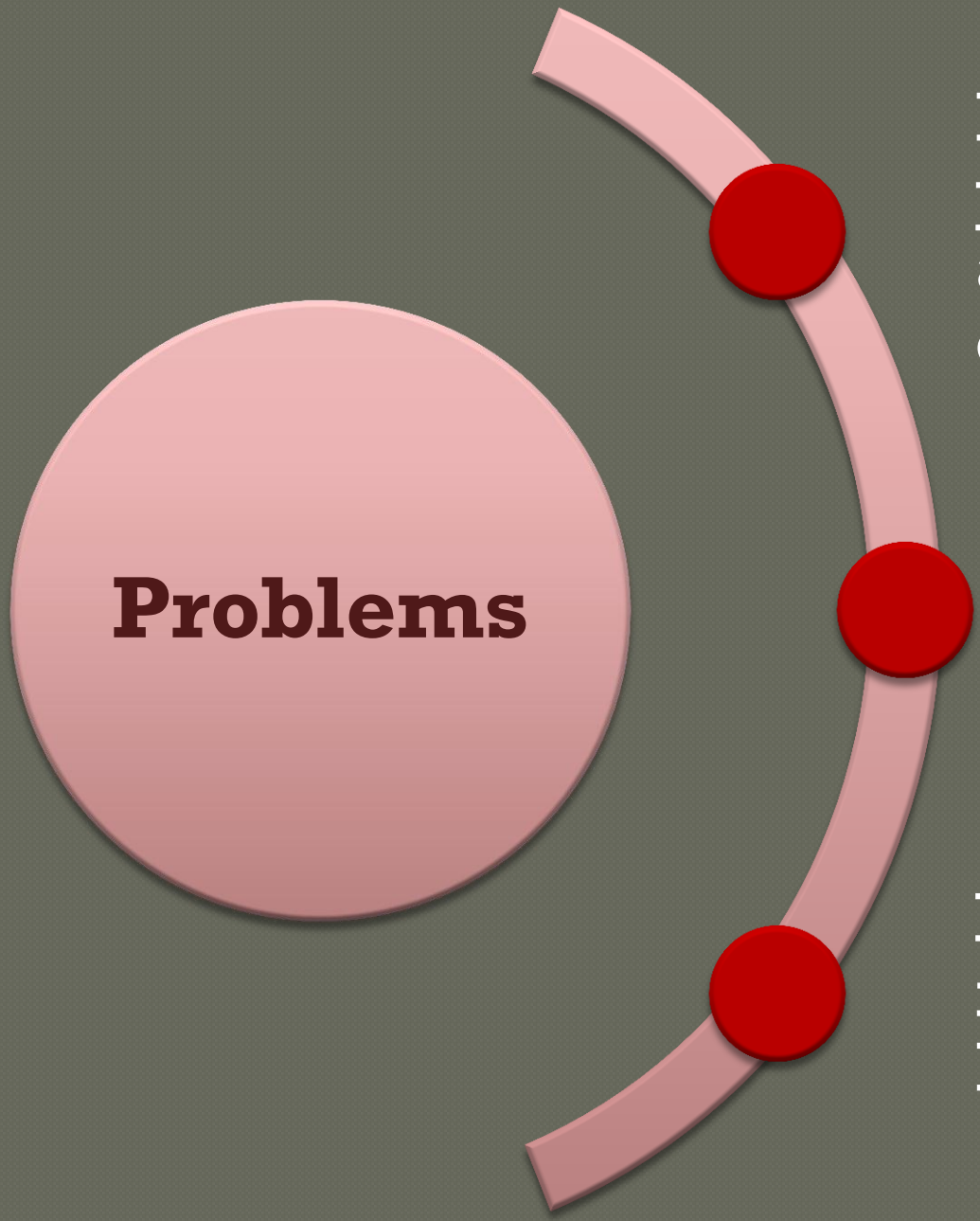
Control (Validator)

Propagator

Propagator

Control (Encoder)

Trigger



Manual pentesting and DAST can't see in

SAST and code review can't see out

No way to map code to HTTP

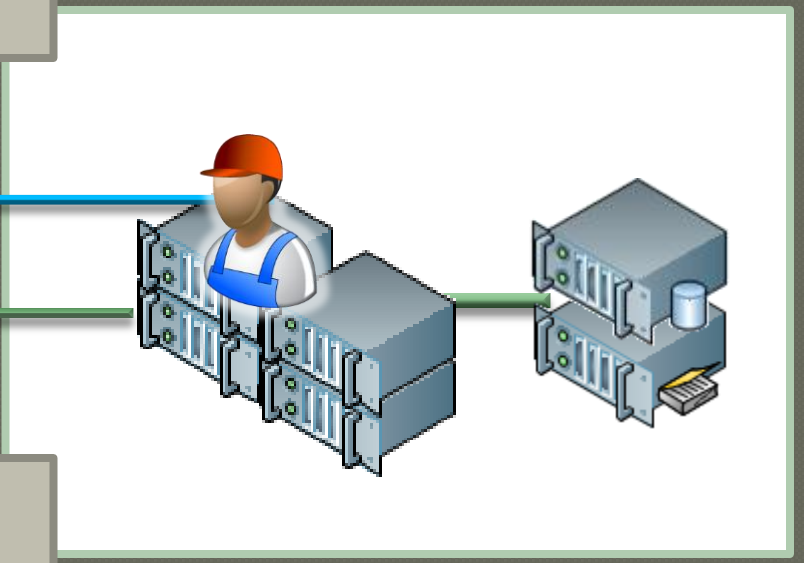
Reimagining the pentest.

“Manual” IAST

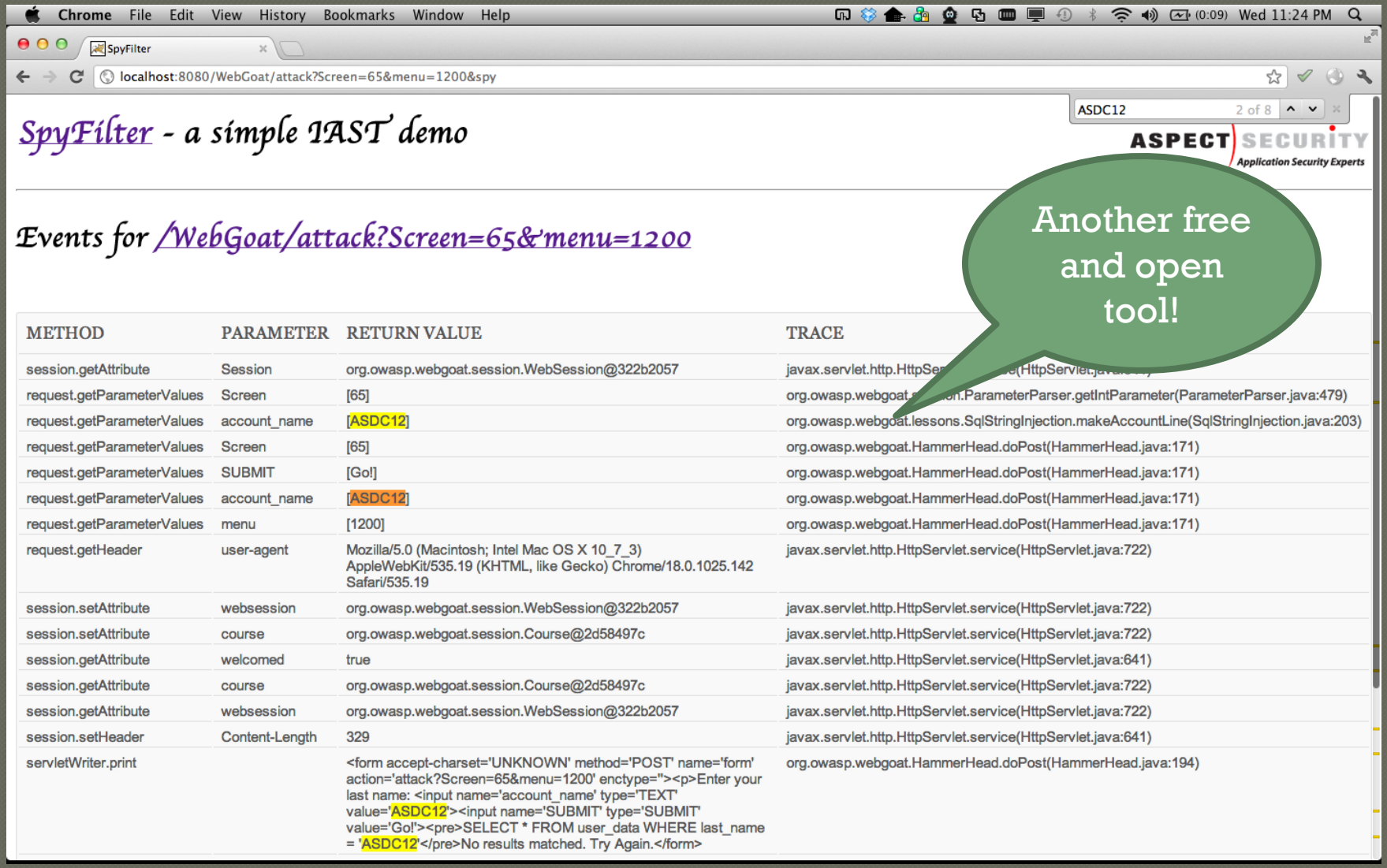
Parameter use
Session update
Dangerous call

Security Intel

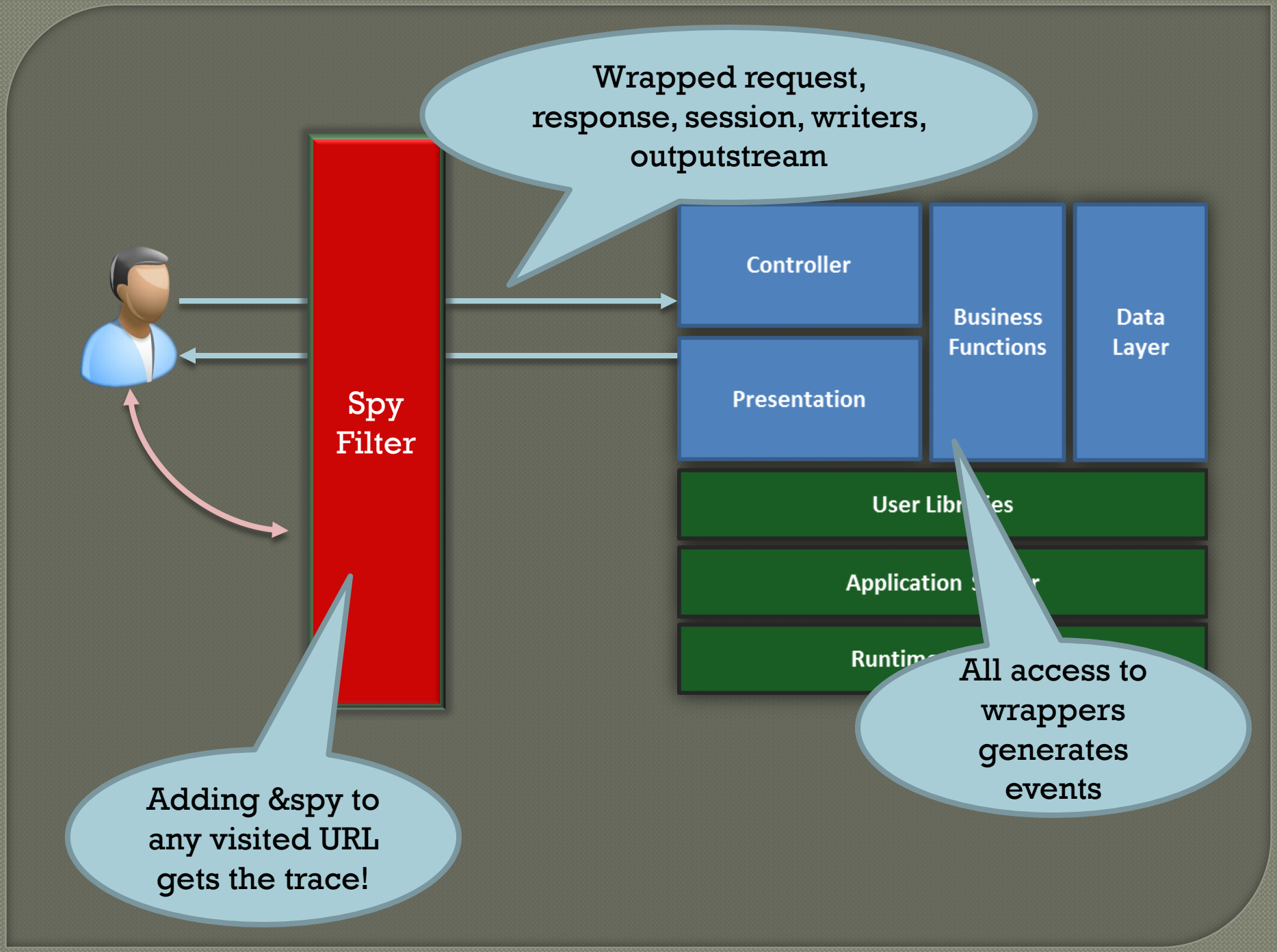
Application Tests



Test for XSS…
…HTML

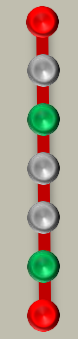


https://www.aspectsecurity.com/spyfilter/

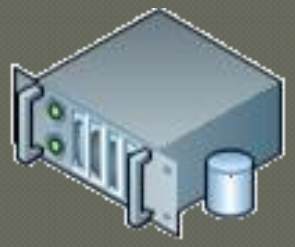

Wrapped request, response, session, writers, outputstream
Controller
Presentation
Business Functions
Data Layer
Spy Filter
Adding &spy to any visited URL gets the trace!
All access to wrappers generates events

Better scanning.

"Basic" IAST

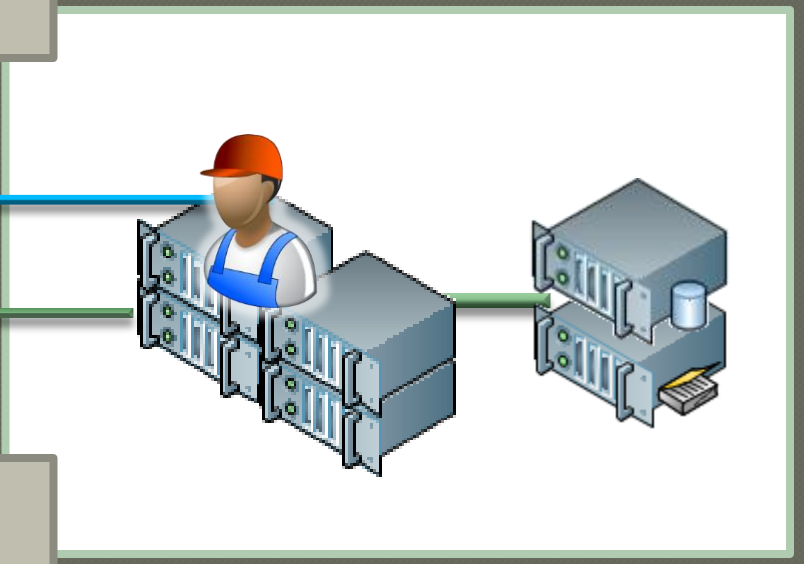


Queries,
Exceptions,
Logs…



Results

Application Tests



Test for SQLi…
…HTML

“Wrap the Sink”

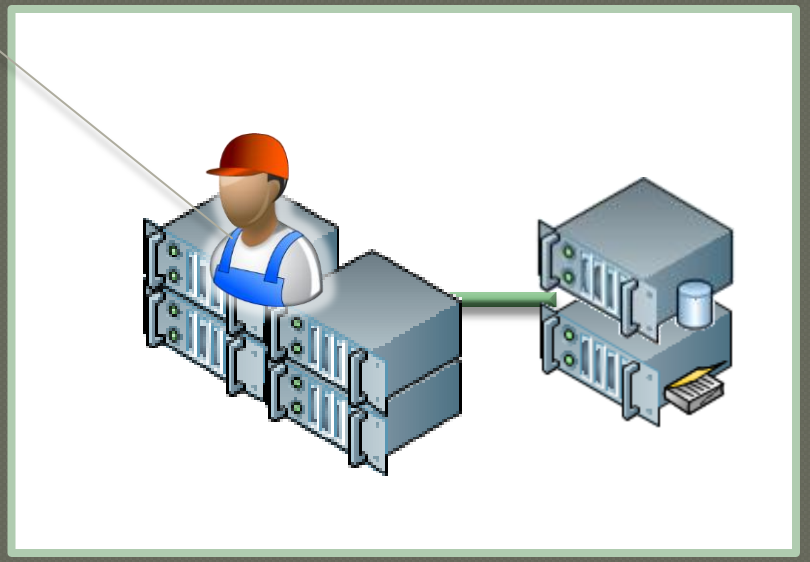
- HP WebInspect SecurityScope
- IBM GlassBox
- Acunetix

Basic IAST Benefits

1. Improve DAST Coverage

2. Validate DAST Vulnerabilities

3. Correlate with Code for DAST Findings

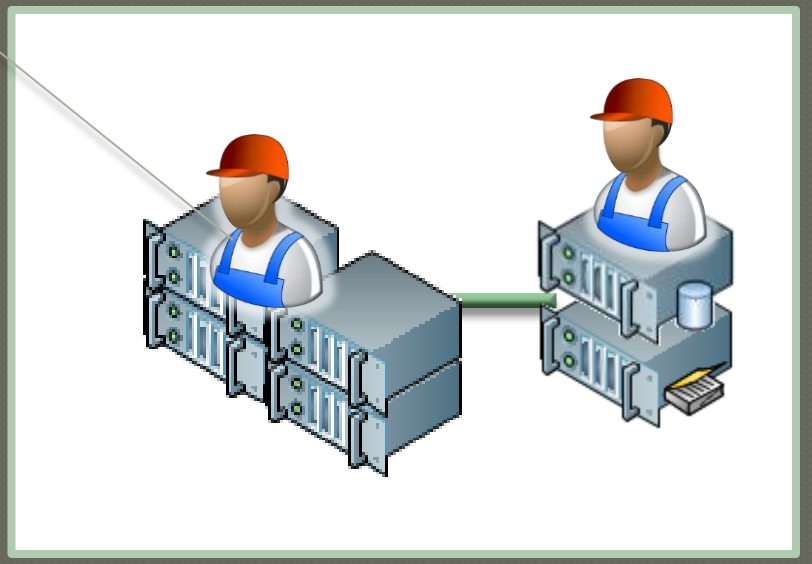


Architecture review?

"Advanced" IAST

Basic IAST plus:

- All libraries used
- Exact SLOC count
- Backend connections
- System configuration
- Security controls
- Directory structure
- Entry points



Instrumentation Techniques

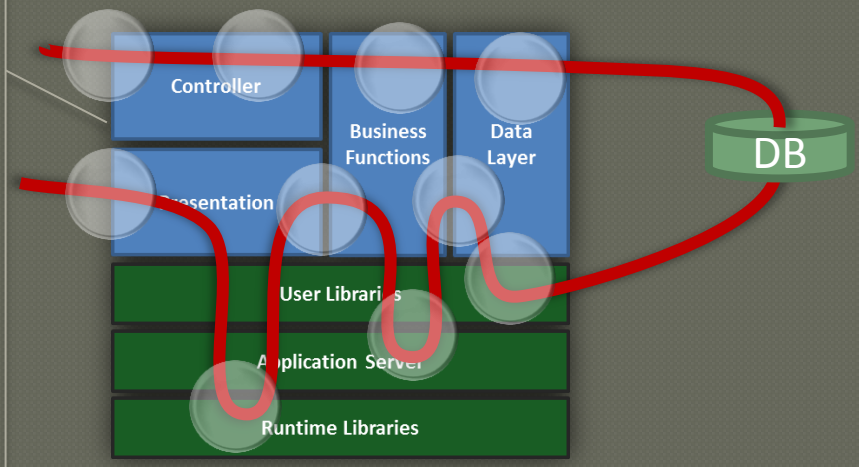
- Add calls to source code
- Use Aspect-oriented programming
- Modify class files on disk
- Modify bytecode of running application with “Instrumentation API”

The Future!

“Pure” IAST

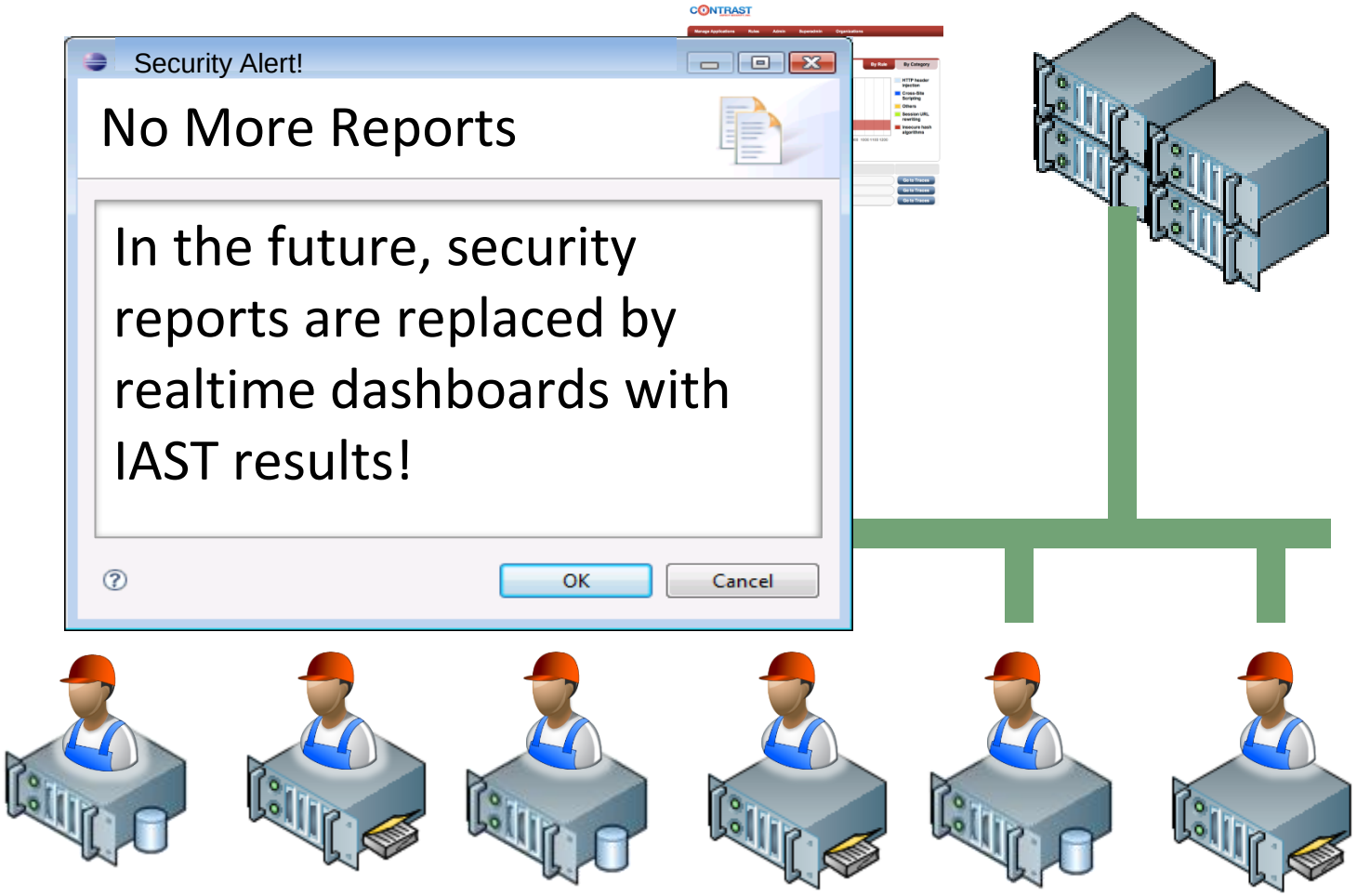
Detailed IAST plus:

- No SAST/DAST
- Powerful rule engine
- Easy install
- Data flow analysis
- Continuous security
- Leverage QA testers



Aspect “Contrast” in private beta

Continuous Security!

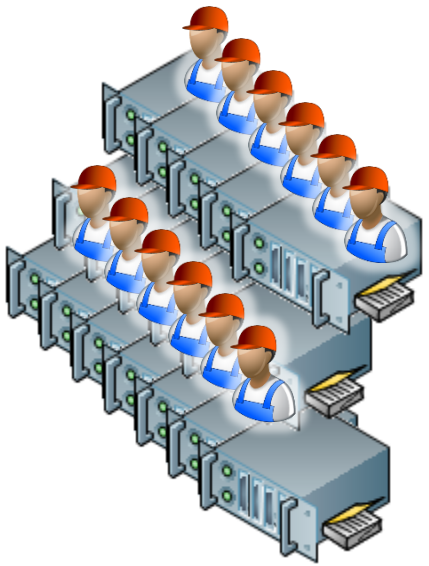

Security Alert!
No More Reports
In the future, security reports are replaced by realtime dashboards with IAST results!
OK
Cancel

The Future of IAST

Automatic:

- Portfolio (prioritized)
- Libraries (analyzed)
- Architecture (summary)
- Vulnerabilities (traced)

GOAL: continuous testing with an enterprise ruleset!



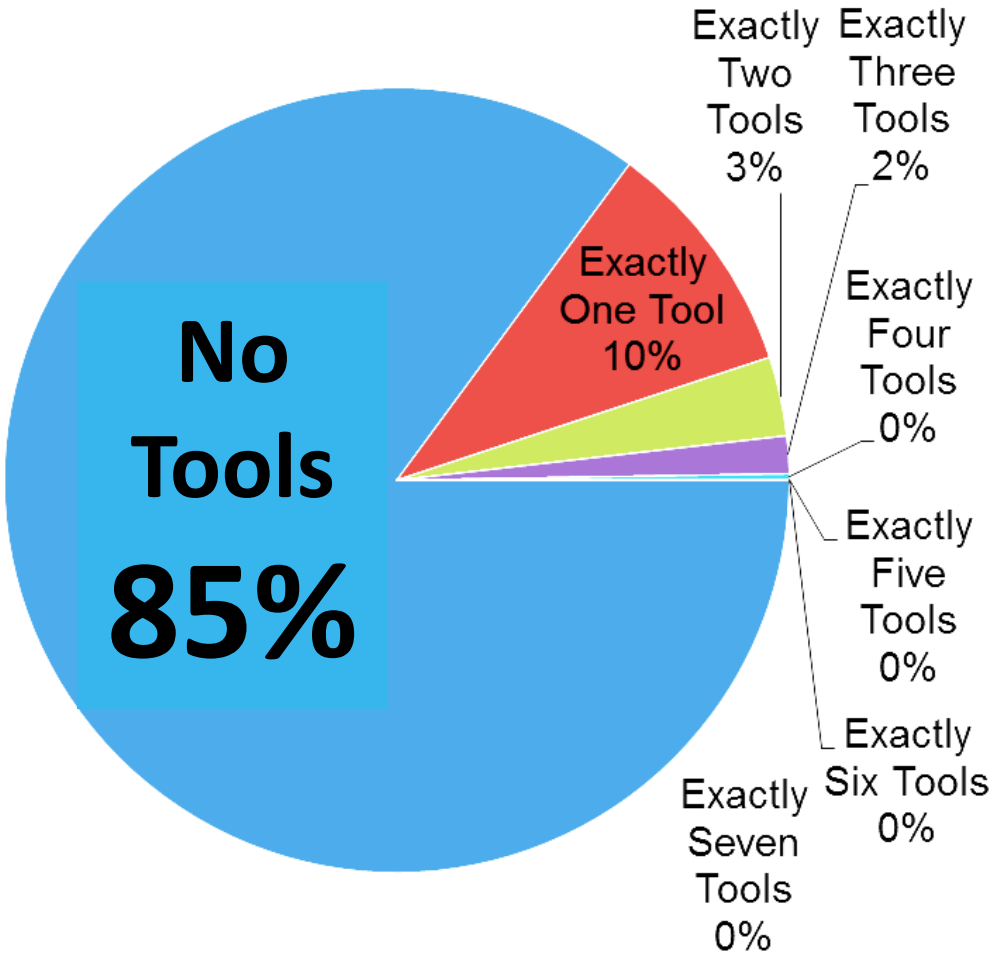
Instrumented Enterprise

Jeff Williams
Aspect Security CEO
jeff.williams@aspectsecurity.com
http://www.aspectsecurity.com

NSA Center for Assured Software

- Seven tools
- 13,801 Test Cases
- 527 flaw types
- Various data and control flows

- 85% of problems were not “discriminated” by ANY tools



http://www.appsecusa.org/p/nsacas.pdf

Results with False Alarms