

DevSecOps – Security at Devops Speed

Ilkka Turunen – Solutions Architect Lead EMEA

Sonatype

@IlkkaTurunen

iturunen@sonatype.com

FLASHBACK HACK ATTACK —

Muni system hacker hit others by scanning for year-old Java vulnerability



DATA CENTER

Security Backups meant SFMTA didn't have to pay 100-Bitcoin ransom demanded by the attacker.

HipChat

SEAN GALLAGHER - 11/29/2016, 4:26 PM

They're g

25 Apr 2017 at

IRC-for-biz H
service allowThe ytalk-for-
powering its i
consisting of
and messageThe Atlassiar
salt, and has
email."As a precau
sent thos
security offic"If you are a
these instrucWhile HipCh
into the HipC
third-party lib

BREAKING NEWS

Baltimore's Union Memorial is one of the hospitals hit
servers.

OBAMA ORDERS UNPRECEDENTED PUNISHMENT FOR RUSSIA HACKING



BUSINESS CULTURE DESIGN GEAR SCIENCE SECURITY TRANSPORTATION

ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts | Health | World News TV | More ▾

Health

NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017 | Health



The ransomware involved has been defeated before, reports the BBC's Chris Foxx

NHS services across England and Scotland have been hit by a large-scale
cyber-attack that has disrupted hospital and GP appointments.

Top Stories

Trump 'shared secret info with
Russia'

22 minutes ago

Mexican drug trade reporter shot
dead

9 minutes ago

N Korea link suspected in cyber-
attack

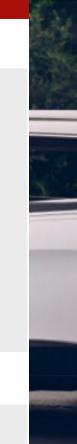
5 hours ago

ADVERTISEMENT

Features



Is France's Socialist Party dead?



SITUATION ROOM



SOFTWARE EATING THE WORLD
HAS ALREADY CONSUMED

~ Marc Andreessen 2011

Source: Security is Dead. Long Live Rugged DevOps: IT at Ludicrous Speed - Josh Corman, Gene Kim

ON TIME



ON BUDGET



ACCEPTABLE
QUALITY/RISK



Incentives
incentivise



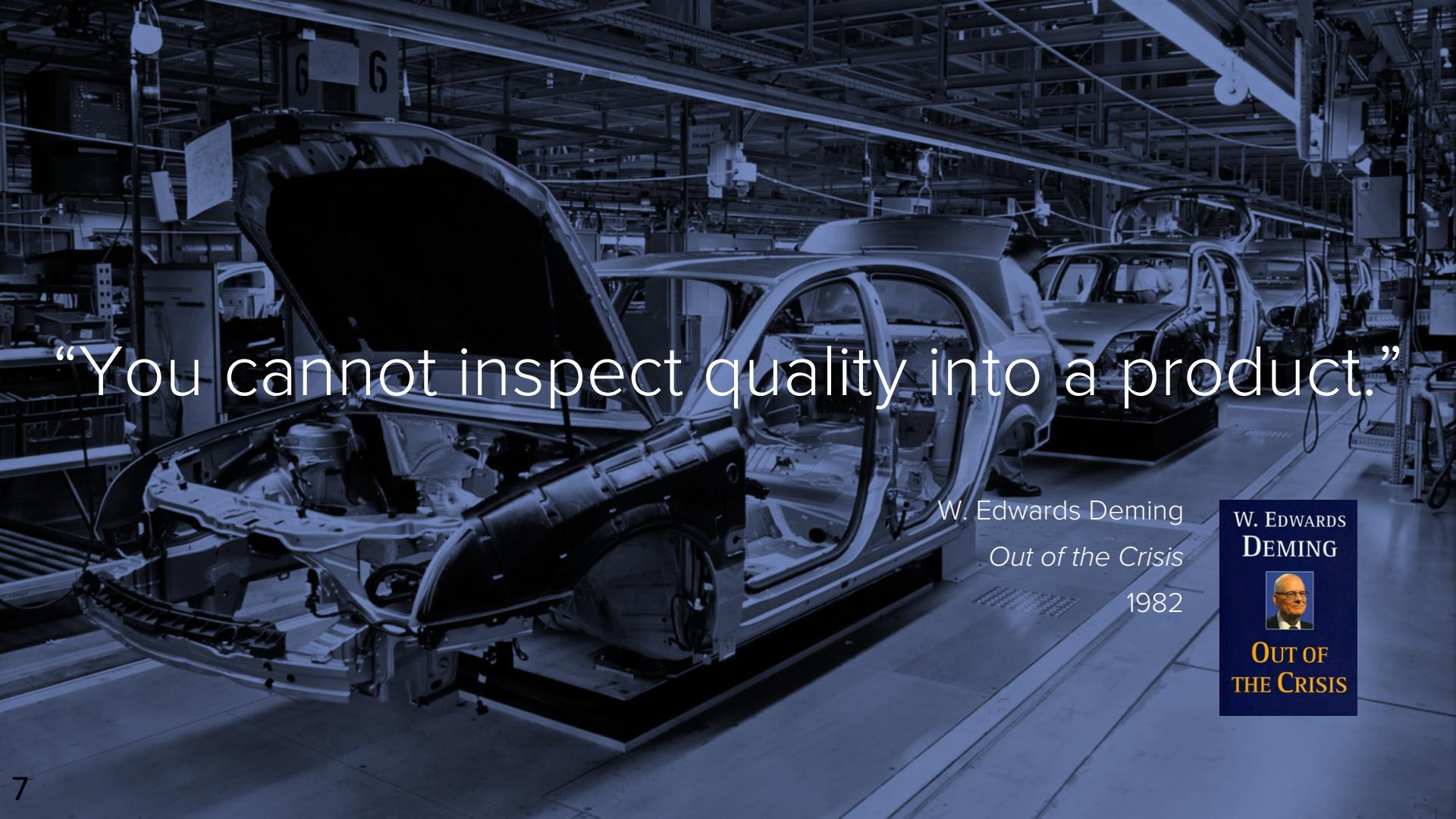


100:1

developers outnumber application security

Natural
implications





“You cannot inspect quality into a product.”

W. Edwards Deming

Out of the Crisis

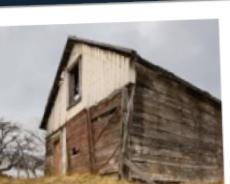
1982

W. EDWARDS
DEMING



OUT OF
THE CRISIS

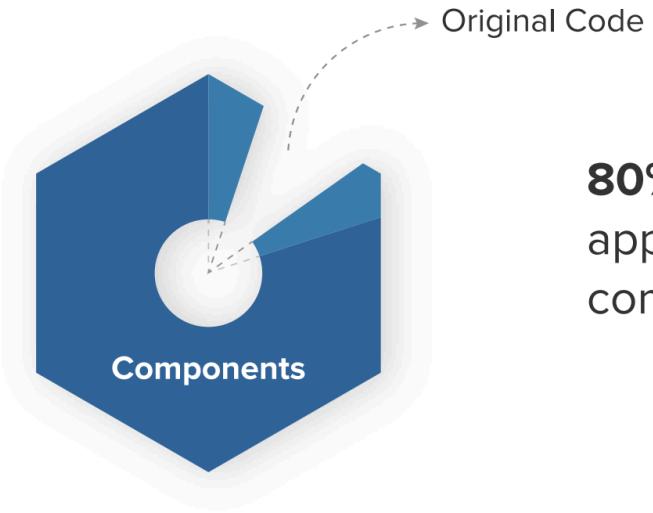
The domains of security



Source: Security is Dead. Long Live Rugged DevOps: IT at Ludicrous Speed - Josh Corman, Gene Kim



**Modern
applications
are *mostly*
*assembled***

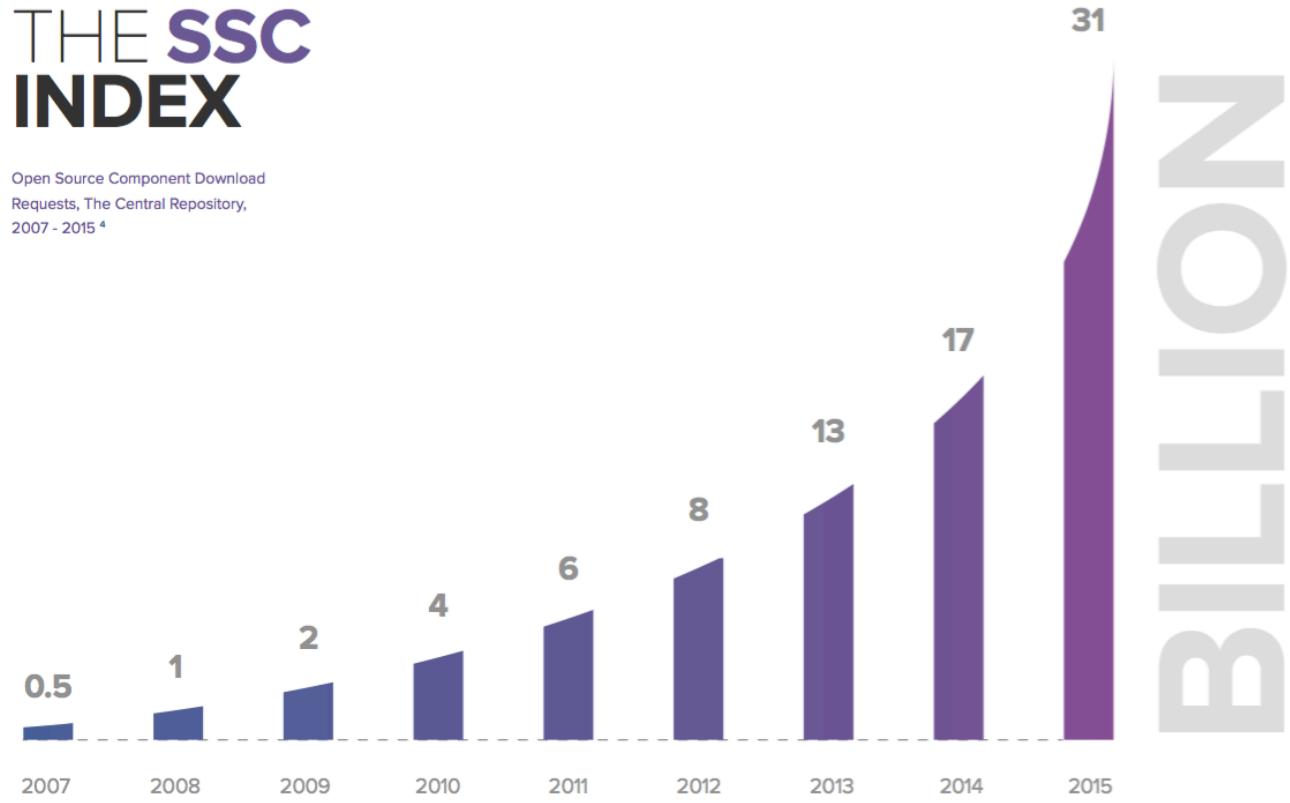


80% to 90% of a typical application is composed of components.

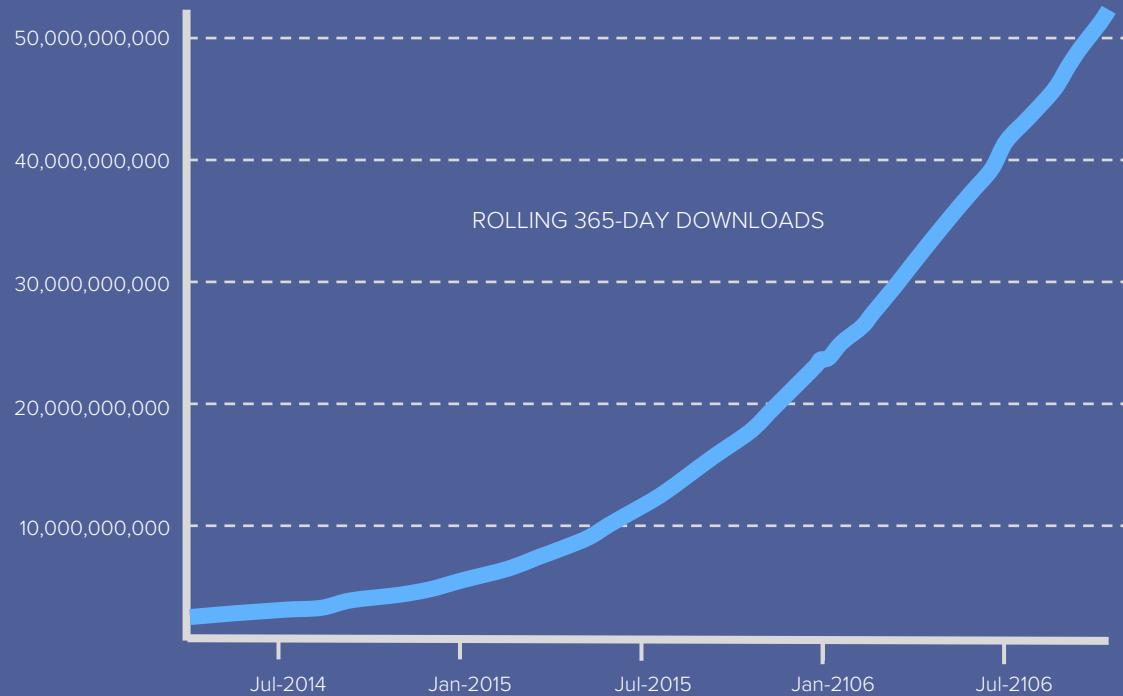
The Perspective of Maven Central

THE **SSC** INDEX

Open Source Component Download
Requests, The Central Repository,
2007 - 2015 ⁴



DOWNLOAD RECORDS FOR **npm**



DOWNLOAD RECORDS FOR PyPI



Donald Stufft
@dstufft

Following ▾

Cool things: In the last month PyPI has served half a petabyte worth of content with 4.4 billion requests.

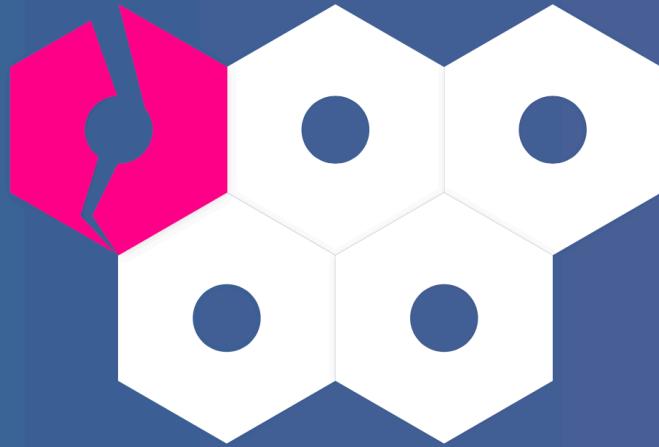
RETWEETS LIKES

60 123



8:38 AM - 14 Feb 2017

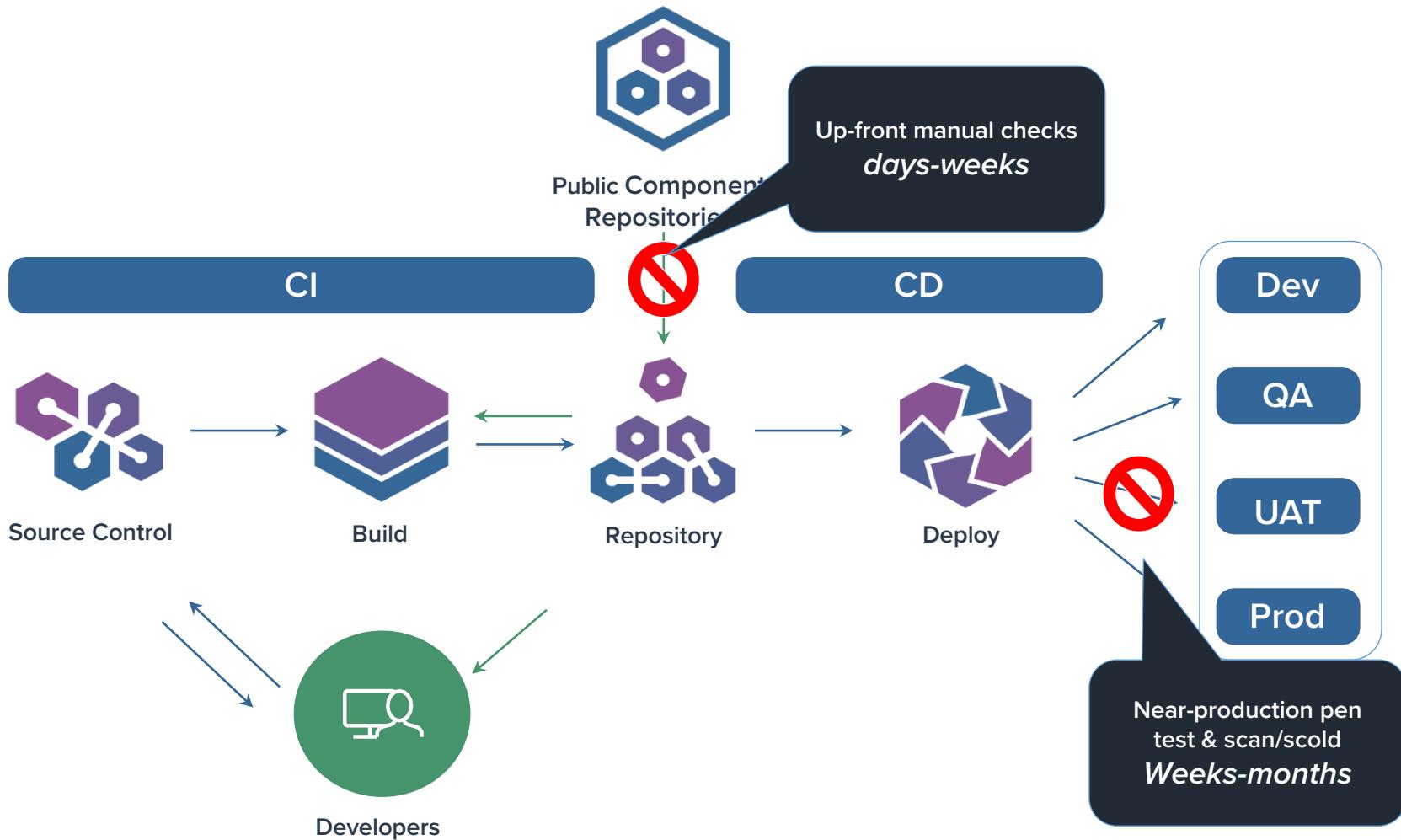
↪ 60 ❤ 123



1-in-5 had or suspected a breach related
to an open source component in the
past 12 months.

Analysis of 25000+ Applications





Implications

Open Source Repositories



6.1%

component downloads are
vulnerable

DEFECT RATIO FOR JAVASCRIPT

37%
websites include
at least one
library with a
known
vulnerability



87%

of handlebars inclusion were known vulnerable



37%

of jQuery inclusion were known vulnerable

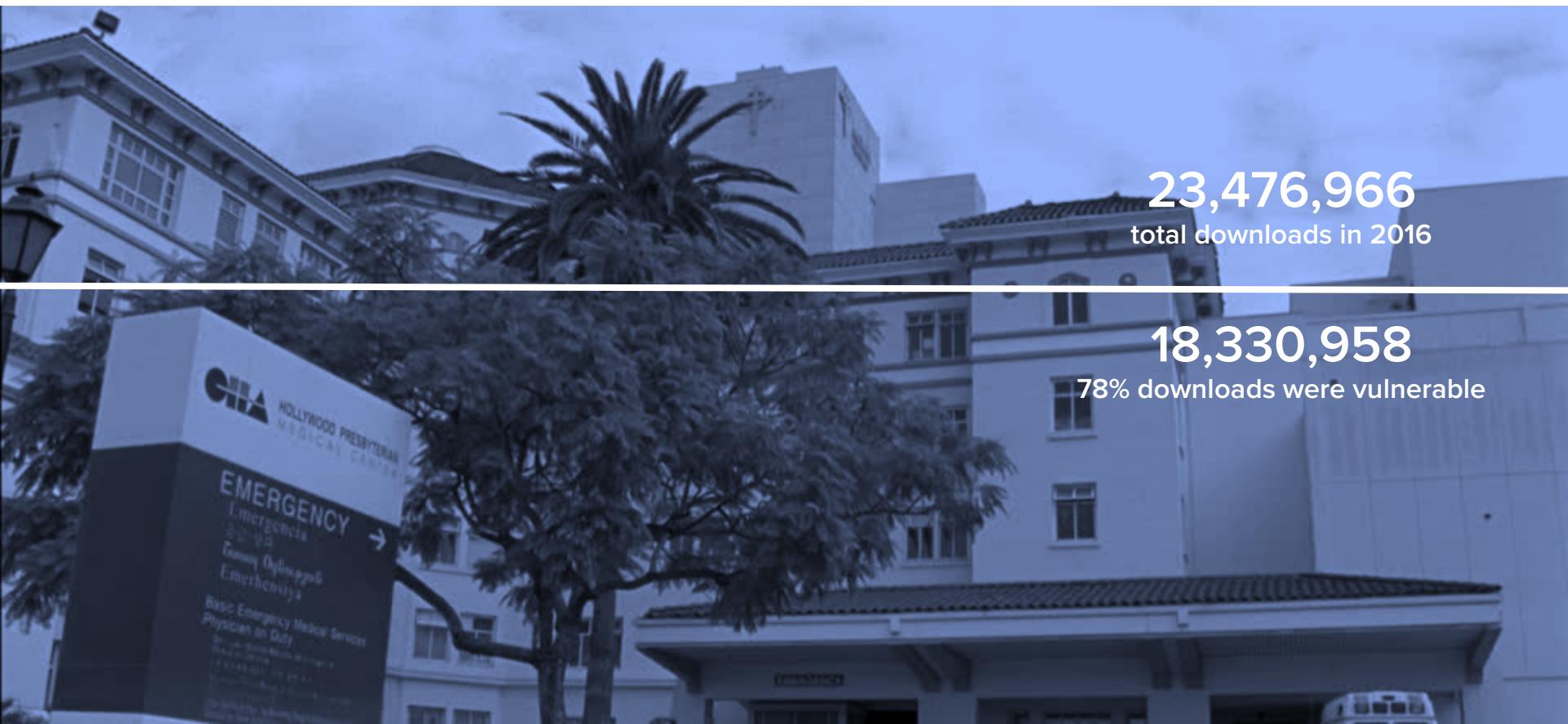


40%

of Angular inclusions were known vulnerable

COMMONS COLLECTION

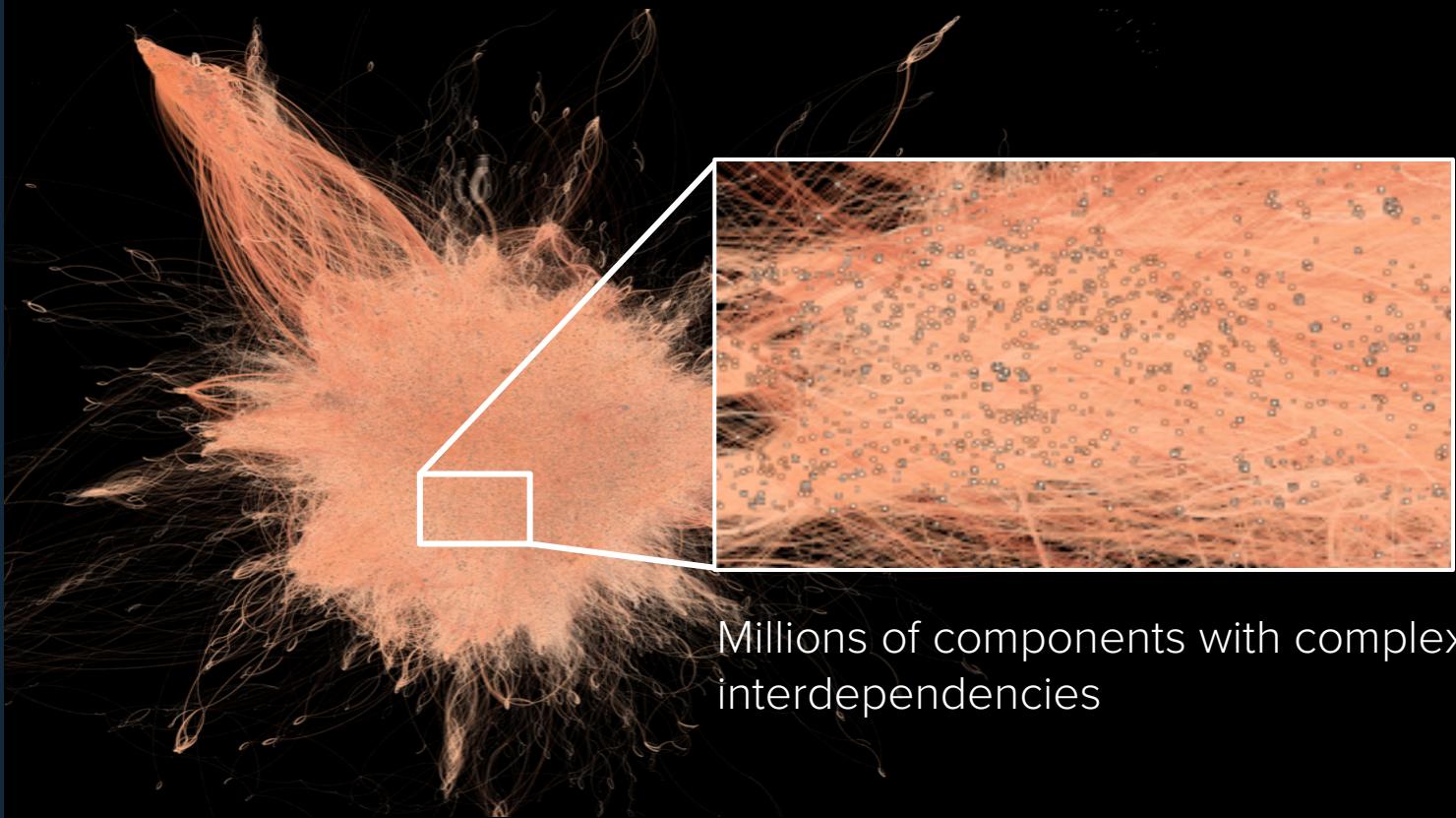
CWE-502



23,476,966
total downloads in 2016

18,330,958
78% downloads were vulnerable

Transitive dependencies – Maven Central 2015



IDEVSECOPS

Leaning in over Always Saying “No”

Data & Security Science over Fear, Uncertainty and Doubt

Open Contribution & Collaboration over Security-Only Requirements

Consumable Security Services with APIs over Mandated Security Controls & Paperwork

Business Driven Security Scores over Rubber Stamp Security

Red & Blue Team Exploit Testing over Relying on Scans & Theoretical Vulnerabilities

24x7 Proactive Security Monitoring over Reacting after being Informed of an Incident

Shared Threat Intelligence over Keeping Info to Ourselves

Compliance Operations over Clipboards & Checklists



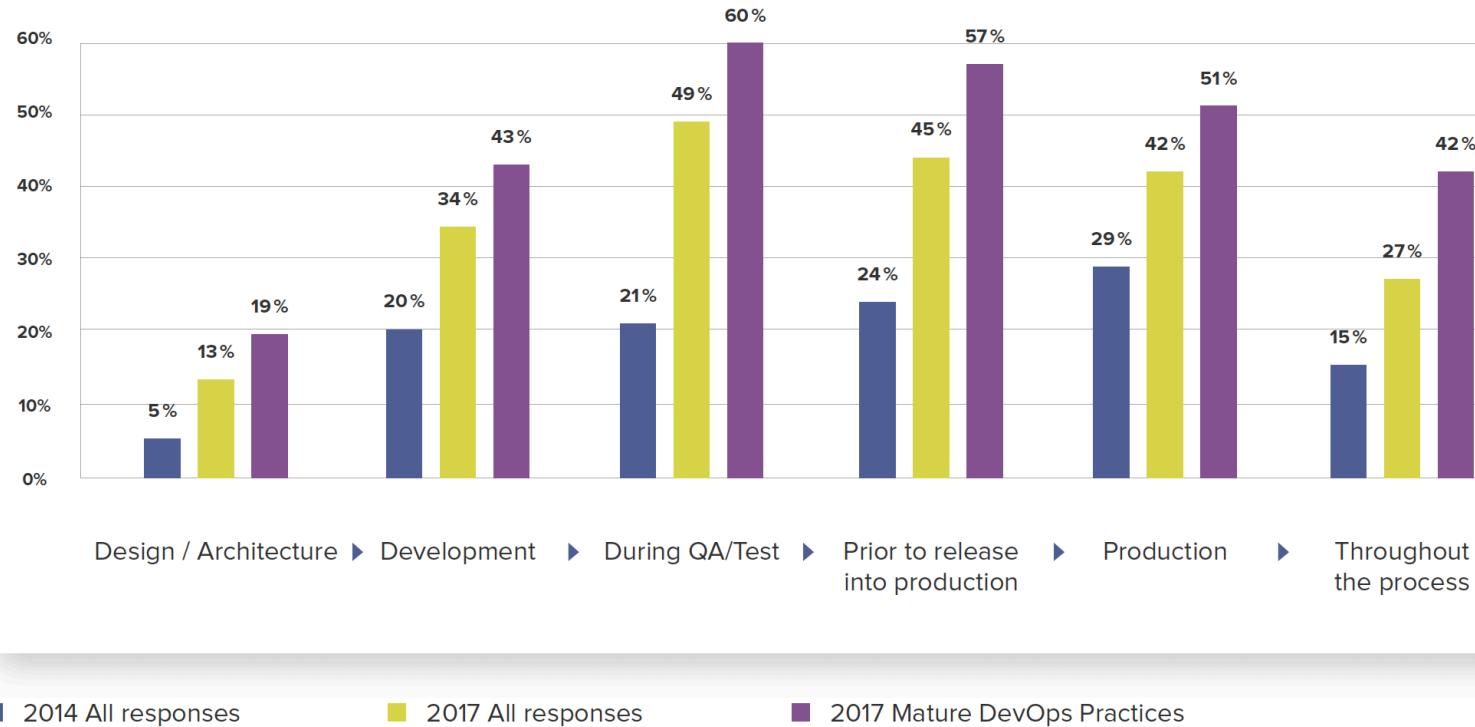
OWASP

The Open Web Application Security Project

OWASP Top 10 - 2013

The Ten Most Critical Web Application Security Risks

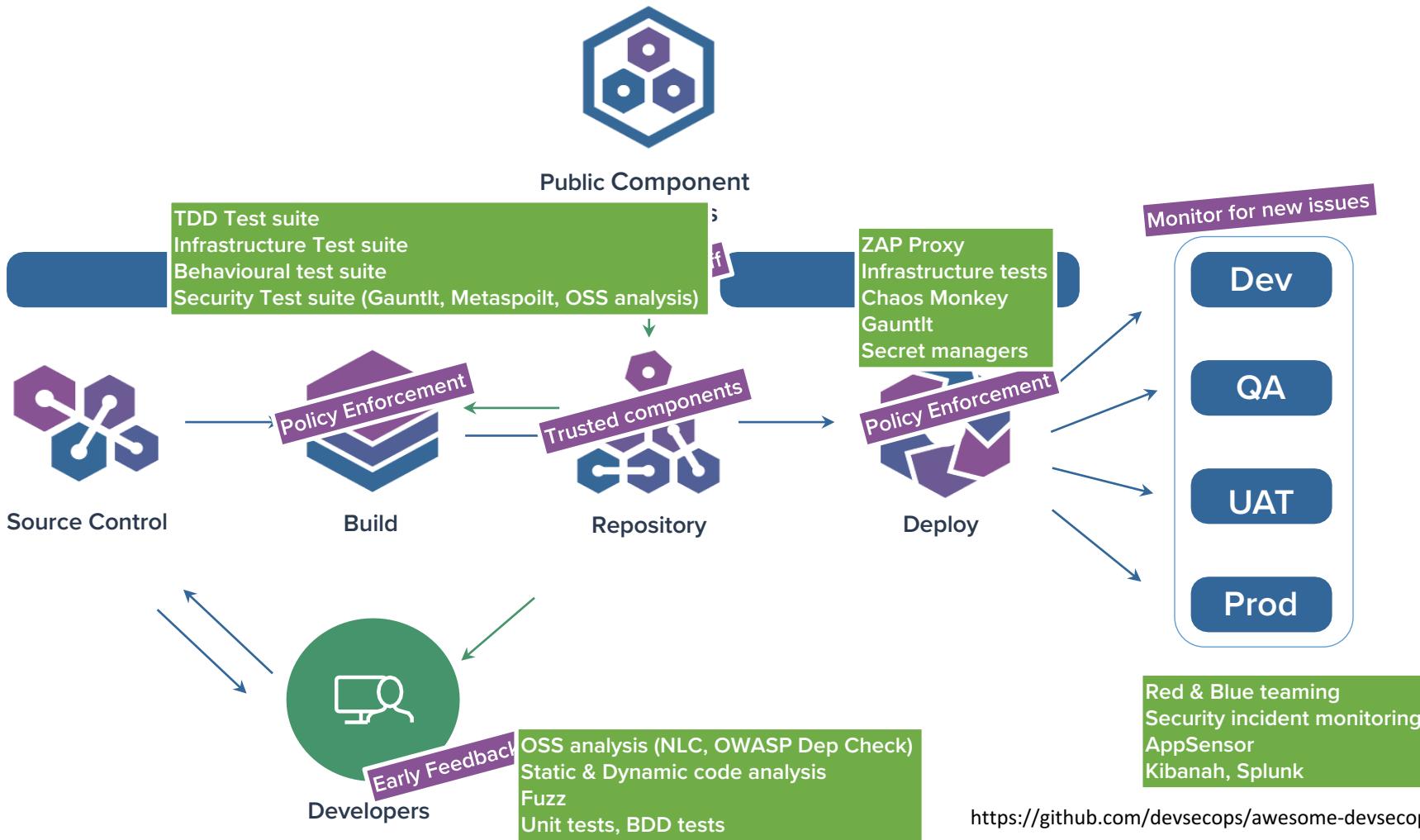
WHERE IS SECURITY BEING AUTOMATED?



The onion model of testing

SECURITY







Good Procurement Bill - US

Ingredients

Anything sold must provide a Bill of Materials of 3rd Party and Open Source Components

Hygiene & Avoidable Risk

Cannot use known vulnerable components

Remediation

Must be patchable/updateable



Exxon





Group: **org.apache.struts**

Artifact: **struts2-core**

Version: **2.3.4**

Overridden License: -

Declared License: **Apache-2.0**

Observed License: **Apache-2.0**

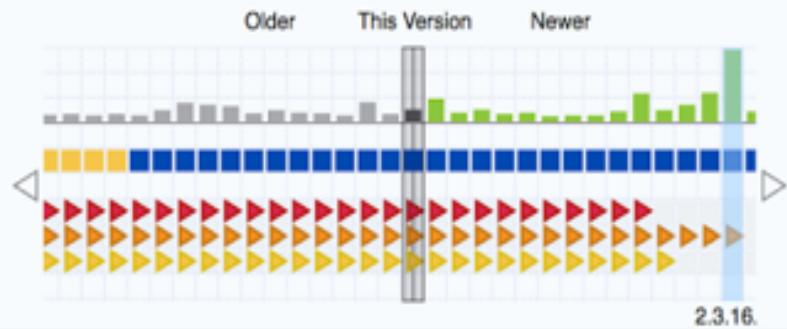
Highest Policy Threat: **9** within 2 policies

Highest Security Threat: **10** within 19 security issues

Cataloged: **1 year ago**

Match State: **exact**

Popularity



Design an approach that works *with* not *against*

The screenshot shows the Jenkins dashboard at <http://localhost:8060>. The left sidebar includes links for New Item, People, Build History, Project Relationship, Check File Fingerprint, Manage Jenkins, and Credentials. Below these are sections for Build Queue (empty) and Build Executor Status (1 Idle). The main content area displays a table of projects with columns for Name, Last Success, Last Failure, Last Duration, and Policy Violations. Each project row includes a green Jenkins icon, a red circle icon, and a dropdown menu. The Policy Violations section shows counts for various categories: Sonatype (5), Jenkins (4), and Nexus (31).

S	W	Name ↓	Last Success	Last Failure	Last Duration	Policy Violations
●	●	Enterprise App Snap with Nexus Pro Staging	2 mo 3 days - #85	25 min - #88	1 min 10 sec	5 4 31
●	●	EnterpriseApp1	3 mo 23 days - #107	21 min - #134	2 min 9 sec	10 5 33
●	●	Hadoop	N/A	3 mo 1 day - #25	2 min 41 sec	6
●	●	Ozone Widget Framework	N/A	7 days 3 hr - #10	55 sec	
●	●	WebgoatSrc	6 days 3 hr - #71	6 min 22 sec - #73	40 sec	5 29

Icon: S M L Legend:

Help us localize this page Page generated: Dec 16, 2014 1:23:31 PM REST API Jenkins ver. 1.589

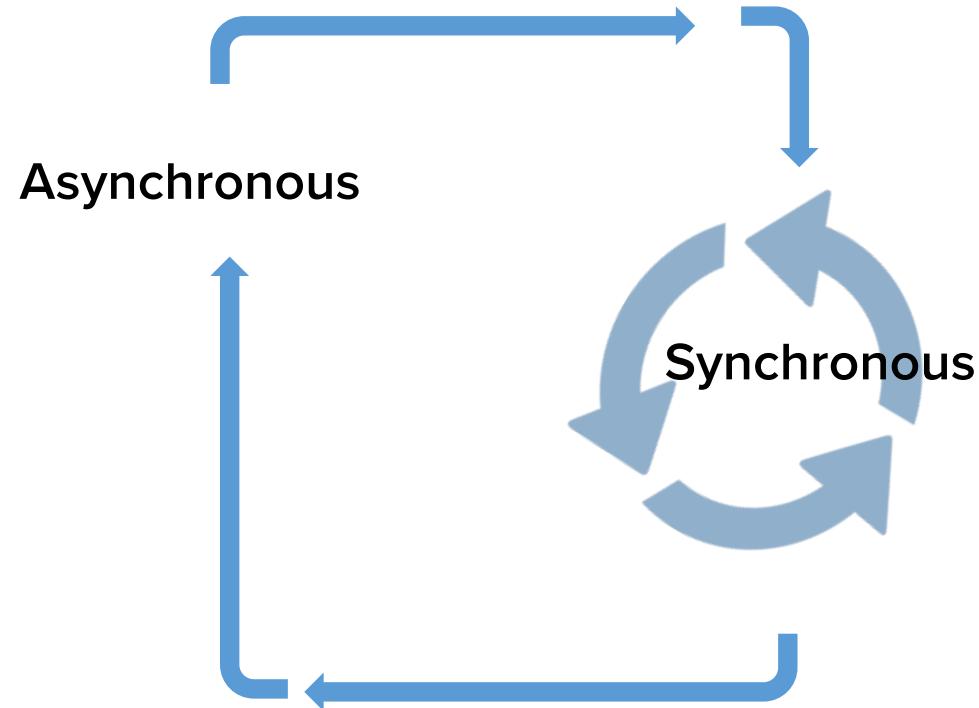
Know what
you run

Applications
OS Packages
Libraries



Policy Threat ▾	Component ▾	Popularity	Age	Release History
Search Name	Search Component			10 years
No Banned-deprecated	org.springframework : spring-context : 3.0.5.RELEASE	●	5.5 y	
	uk.ltd.getahead : dwr : 1.1.1	●	10.0 y	
Security-Critical	org.apache.struts : struts2-assembly : zip : all : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-blank : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-core : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-mailreader : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-portlet : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-rest-plugin : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-rest-showcase : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-showcase : war : 2.3.14	●	3.1 y	
Security-High	commons-collections : commons-collections : 3.1	●	10.5 y	
	commons-fileupload : commons-fileupload : 1.2.2	●	5.8 y	
	org.apache.struts : struts-core : 1.3.10	●	7.4 y	
	org.apache.struts : struts2-assembly : zip : all : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-blank : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-core : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-mailreader : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-portlet : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-rest-showcase : war : 2.3.14	●	3.1 y	
	org.apache.struts : struts2-showcase : war : 2.3.14	●	3.1 y	

Use the CI Pipeline to incrementally improve security practices



Synchronous testing occurs at every build

Policy Name: Security-High Threat Level: 9

INHERITANCE

This Policy Inherits to:

- All Applications and Repositories
- Applications of the specified Application Category

Bank X Better Payment - 2016-05-06 - *Build Report*

Summary Policy Violations Security Issues License Analysis

This report provides security and license assessments for open source components found within an application.

CONSTRAINTS

High risk CVSS score is in violation if all of the following are true:

- Security Vulnerability Severity greater than or equals
- Security Vulnerability Severity less than 10
- Security Vulnerability Status is not Not Applicable

Scope of Analysis

99 COMPONENTS IDENTIFIED
100% OF ALL COMPONENTS ARE OPEN SOURCE

16 POLICY ALERTS AFFECTING 99 COMPONENTS
56 SECURITY ALERTS AFFECTING 16 COMPONENTS
27 LICENSE ALERTS AFFECTING 162 COMPONENTS

Security Issues

How bad are the vulnerabilities and how many are there?

Critical (7-10) 118
Severe (4-6)

Threat Level: 0 10 20 30 40 50

The summary of security issues demonstrates the breakdown of vulnerabilities based on severity and the threat level it poses to your application.

The dependency depth highlights quantity and severity and distribution within the application's dependencies.

Jenkins WebGoat-Test

Back to Dashboard Status Changes Workspace Build Now Delete Maven project Configure Modules Application Management Git Polling Log

Maven project WebGoat-Test

Polls Webgoat repo, builds on new commit

Workspace Recent Changes Application Composition Report

Dependency Depth

Depth	Critical (7-10)	Severe (4-6)
1	100%	100%
2	10%	10%
3	10%	10%
4	10%	10%
5+	10%	10%

```
[INFO] Evaluating policies... (ETA 30s)
```

```
[INFO] -----  
-----
```

```
[INFO] BUILD FAILURE
```

```
[INFO] -----  
-----
```

```
[INFO] Total time: 37.210 s
```

```
[INFO] Finished at: 2015-10-21T18:38:53+01:00
```

```
[INFO] Final Memory: 17M/496M
```

```
[INFO] -----  
-----
```

```
[ERROR] Failed to execute goal com.sonatype.clm:clm-maven-plugin:2.1.1:evaluate (default-cli) on project WebGoat: Sonatype CLM reports policy failing due to
```

```
[ERROR] Policy(NO high sec vulnerabilities) [
```

```
[ERROR] Component(gav=commons-fileupload:commons-fileupload:1.2.1, hash=384faa82e193d4e4b054) [
```

```
[ERROR] Constraint(No secs) [Security Vulnerability present because: Found 4 Security Vulnerabilities, Security Vulnerability Severity >= 7 because: Found Security Vulnerability with Severity >= 7] ]]
```

Asynchronous testing – outside of Delivery Cycle

Deep dive

hp Dashboard Applications Reports Administration Search Apps & Reports Live Chat User

Issues Dashboard

Assignment Status Developer Status Auditor Status Issue Status Last Month Highlights expand all | collapse all APPLICATION TYPE

Action Priority Most Prevalent Trending

Application	Release	Last Completed	Assessment Type	Actions
Webgoats	3	2013/07/02	Static Source Code Analysis	351
Internal Portal	2.2	2013/06/28	Static Source Code Analysis	348
SOL Test	1	2013/06/25	Static Source Code Analysis	194
Webgoat Fixes	3.0 (Java)	2013/07/05	Static Source Code Analysis	128
WebGoat Demo	1	2013/06/13	Standard Dynamic Assessment	101
TestProd Oct	Version 1	2013/10/19	Premium Dynamic Assessment	97
Riches SpiDynamics	1	2013/05/30	Basic Dynamic Assessment	21
FPR Test	v1	2014/05/21	Standard Dynamic Assessment	14

Hotspots Reviews SQA LE QA Time Machine My Components Violations Drilldown Clouds Design Libraries sonar

Violations 1,148 ▼ Rules compliance 96.7% Blocker 0 Critical 0 Major 637 ▼ Minor 178 ▼ Info 333 ▲

Alerts : Skipped unit tests > 0.

Code coverage 68.7% Unit test success 100.0% 69.3% line coverage 0 failures 67.0% branch coverage 0 errors 2,597 tests ▲ 0 skipped 4:08 min ▲

Lines of code 62,406 ▲ Classes 1,300 ▲ 110,305 lines ▲ 171 packages 23,838 statements ▲ 7,029 methods ▲ 1,195 files ▲ 1,348 accessors ▲

Comments 7.7% Duplications 0.8% 5,208 lines ▲ 924 lines ▼ 26.9% docu. API 49 blocks 4,272 undocu. API ▲ 35 files

Package tangle index 10.1% Dependencies to cut 35 between packages ▲ > 56 cycles 51 between files

LCOM4 1.1 /class Response for Class 15 /class 3.8% files having LCOM4>1

Complexity 1.9 /method 10.5 /class 11.4 /file Total: 13,592 ▲ Methods Files

Events All

12 Apr 2012	Version	2.16-SNAPSHOT
06 Apr 2012	Version	2.15-SNAPSHOT
27 Mar 2012	Profile	Sonar for Sonar version 7
02 Mar 2012	Profile	Sonar for Sonar version 6

Tags 325 0 mandatory 325 optional 48 nosonar TODO FIXME @deprecate

The dashboard provides a comprehensive overview of software quality and testing status. It includes sections for Assignment Status, Developer Status, Auditor Status, and Issue Status. Key metrics displayed include the total number of violations (1,148), rules compliance (96.7%), and code coverage (68.7%). The dashboard also tracks comments, duplications, and package tangle index. A timeline shows recent events like version updates and profile changes. A sidebar navigation menu includes Home, Sonar, Dashboard, Hotspots, Reviews, SQA LE, QA, Time Machine, My Components, Violations Drilldown, Clouds, Design, and Libraries. A Sonar logo is present in the center of the dashboard area.

Results

View ▾

! VIOLATIONS

COMPONENTS

APPLICATIONS

NAME	FFECTED APPS	TOTAL RISK	Critical	Severe	Moderate	Low	
commons-httpclient : commons-httpclient : 3.1	11	205	81	118	6	0	▶
org.apache.struts : struts2-assembly : zip : all : 2.3.14	4	150	96	48	6	0	▶
org.apache.struts : struts2-blank : war : 2.3.14	4	130	76	48	6	0	▶
org.apache.struts : struts2-showcase : war : 2.3.14	4	130	76	48	6	0	▶
org.apache.struts : struts2-portlet : war : 2.3.14	4	130	76	48	6	0	▶
org.apache.struts : struts2-rest-showcase : war : 2.3.14	4	130	76	48	6	0	▶
org.apache.struts : struts2-mailreader : war : 2.3.14	4	125	76	43	6	0	▶
commons-collections : commons-collections : 3.1	9	124	97	24	3	0	▶
org.apache.struts : struts2-core : 2.3.14	4	122	76	43	3	0	▶
axis : axis : 1.2	5	116	53	60	3	0	▶
commons-collections : commons-collections : 3.2.1	9	99	81	18	0	0	▶
org.apache.struts.xwork : xwork-core : 2.3.14	4	99	66	33	0	0	▶
org.springframework : spring-web : 2.5.6.SEC03	6	99	36	57	6	0	▶
org.springframework : spring-context : 2.5.6.SEC03	6	94	36	58	0	0	▶

Be
transparent
with
information

*Wall of
shame = yay*

Get involved!



devsecops / awesome-devsecops

Code Issues 1 Pull requests 1 Projects 0 Wiki Insights ▾

An authoritative list of awesome devsecops tools with the help from community experiments and contributions.
<http://devsecops.org>

devsecops threat-intelligence devops podcast

80 commits 1 branch 0 releases 7 contributors CC0-1.0

Branch: master New pull request Create new file Upload files Find file Clone or download ▾

slietz committed on GitHub New persona images Latest commit 19009c9 23 days ago

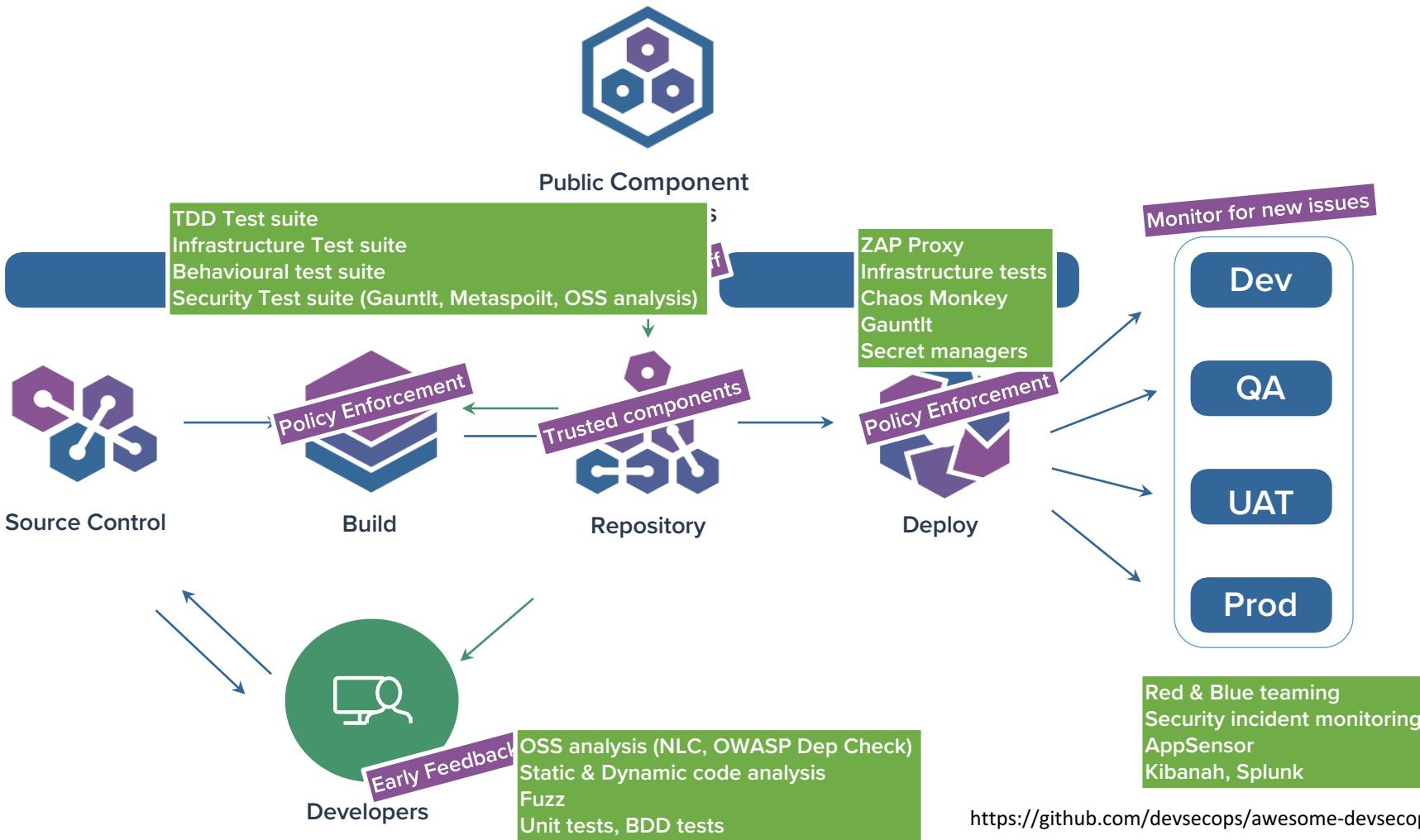
File	Description	Time Ago
.gitignore	Initial commit	2 years ago
CONTRIBUTING.md	initial upload	2 years ago
LICENSE	Create LICENSE	2 years ago
README.md	Additions from pbenjamin	a month ago
dso-dev.png	New persona images	23 days ago
dso-ops.png	New persona images	23 days ago
dso-sec.png	New persona images	23 days ago
p-bluestream.md	Create p-bluestream.md	26 days ago
p-developer.md	Create p-developer.md	26 days ago
p-operations.md	Create p-operations.md	26 days ago
p-redteam.md	Create p-redteam.md	26 days ago
p-security.md	Create p-security.md	26 days ago

README.md

Awesome DevSecOps

Inspired by the awesome-* trend on GitHub. This is a collection of documents, presentations, videos, training materials, tools, services and general leadership that support the DevSecOps mission. These are the essential building blocks and tidbits that can help you to arrange for a DevSecOps experiment or to help you build out your own DevSecOps program.





Thanks - References

- **Wired Article – Hackers remotely kill Jeep on Highway:** <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- https://www.theregister.co.uk/2016/03/30/bmw_complies_with_gpl/
- **State of Devops 2015:** <https://puppetlabs.com/2015-devops-report>
- **Rugged Devops Book:** <http://devops.com/2015/04/20/the-rugged-devops-ebook/>
- **Rugged Software:** <http://www.ruggedsoftware.org/>
- **DevSecOps:** <http://devsecops.org>
- **“The Phoenix Project” by Gene Kim:** <http://itrevolution.com/books/phoenix-project-devops-book/>
- **State of Software Supply Chain 2015:** <https://www.sonatype.com/state-of-the-software-supply-chain>
- **7 Habits of Rugged Devops:** <https://www.forrester.com/report/The+Seven+Habits+Of+Rugged+DevOps/-/E-RES126542>
- **Verizon Data Breach Report:** <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>
- **CodeCentric CI Example:** <https://blog.codecentric.de/en/2015/10/continuous-integration-platform-using-docker-container-jenkins-sonarqube-nexus-gitlab/>
- **FS-ISAC:** <https://www.sonatype.com/software-security-control-white-paper>
- **IEC-62304:** http://www.iso.org/iso/catalogue_detail.htm?csnumber=38421
- **PCI-DSS:** https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss
- **Reflections on NPMGate:** <http://blog.npmjs.org/post/141577284765/kik-left-pad-and-npm>
- **Lessons learnt again from NPMGate:** <http://www.sonatype.org/nexus/2016/03/25/npm-gate-lessons-learned-again/>
- **DevSecOps toolkit:** <https://github.com/devsecops/awesome-devsecops>