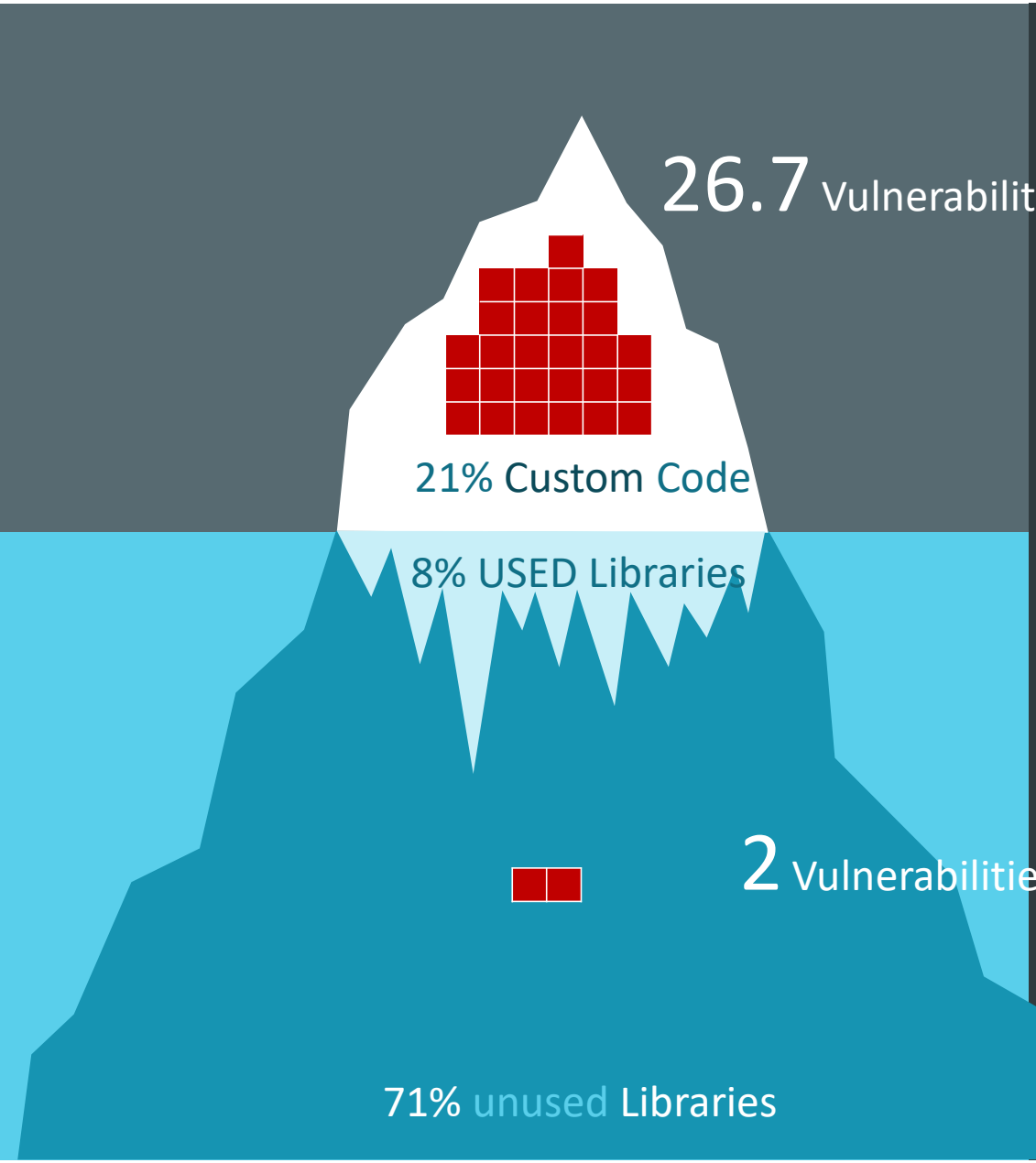
# The Three ways of DevSECOps:

## Building a security pipeline with free tools

OWASP SINGAPORE

Jeff Williams – @planetlevel
CTO and Co-FOUNDER – Contrast

CONTRAST SECURITY

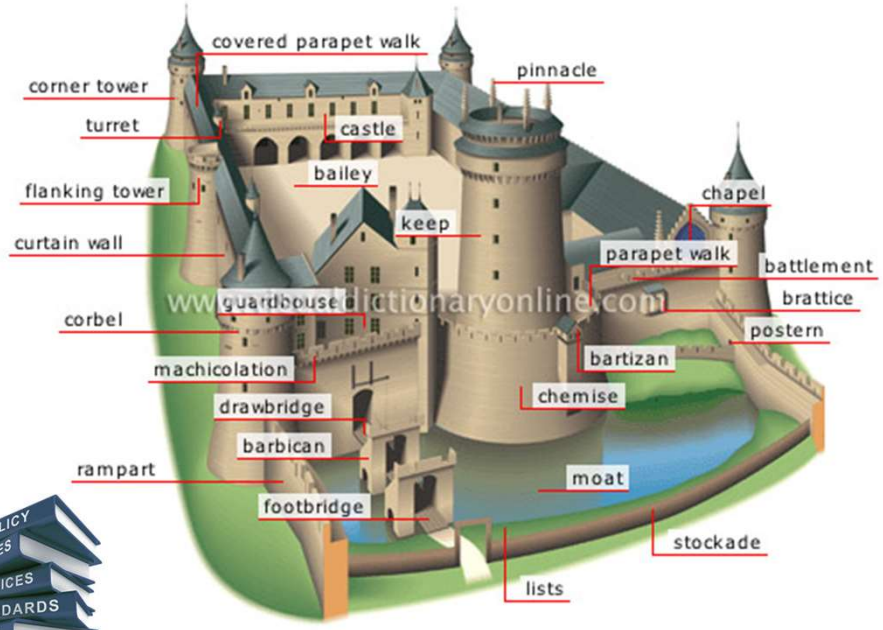


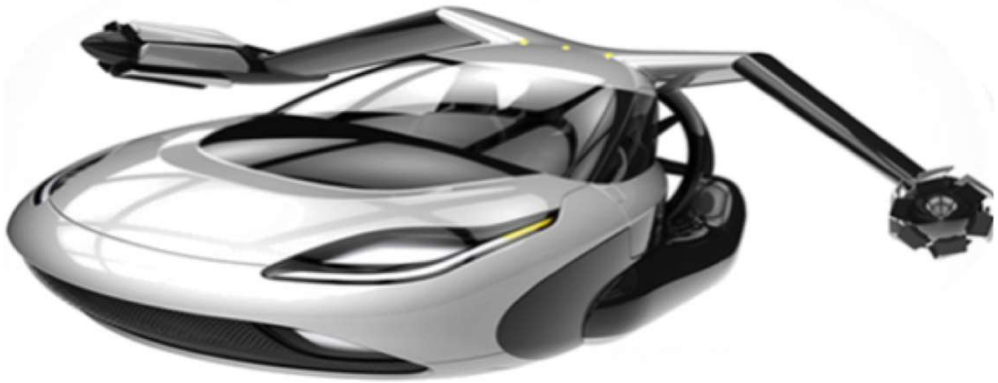

# The Average application is extremely vulnerable

# You are Under AttacK

| | | |
|---|---|---|
| reflected-xss | 58.6% | -8.1% |
| path-traversal | 57.9% | -21.3% |
| sql-injection | 53.8% | -11.6% |
| method-tampering | 50.9% | 23.8% |
| cve-2017-5638 | 27.2% | 4.9% |
| cmd-injection | 24.9% | -24.3% |
| csrf | 17.1% | 14.7% |
| cve-2017-9791 | 16.7% | -8.3% |
| cve-2017-12616 | 12.8% | 0.3% |
| cve-2016-4438 | 8.3% | 0.0% |
| ognl-injection | 8.2% | -8.5% |
| cve-2013-2251 | 8.0% | -4.5% |
| padding-oracle | 4.3% | 4.3% |
| VP: patch forJBoss Remote Exploit | 4.1% | 0.1% |
| cve-2016-3081 | 1.0% | -3.2% |
| cve-2014-0112 | 0.0% | -8.3% |

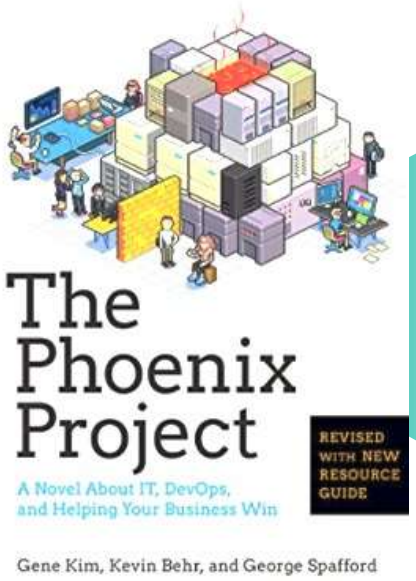
# Please, Don’t let anyone Blame Velocity




**SECURING FAST-CHANGING THINGS IS DIFFERENT**

# DevSecOps is very promising...

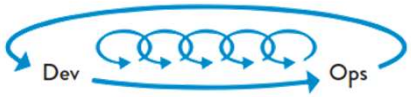



## DEVOPS

**1.Establish work flow**


**2.Ensure instant feedback**


**3.Culture of experimentation**

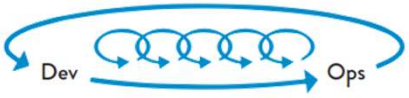



## DEVSECOPS

**1.Establish security work flow**

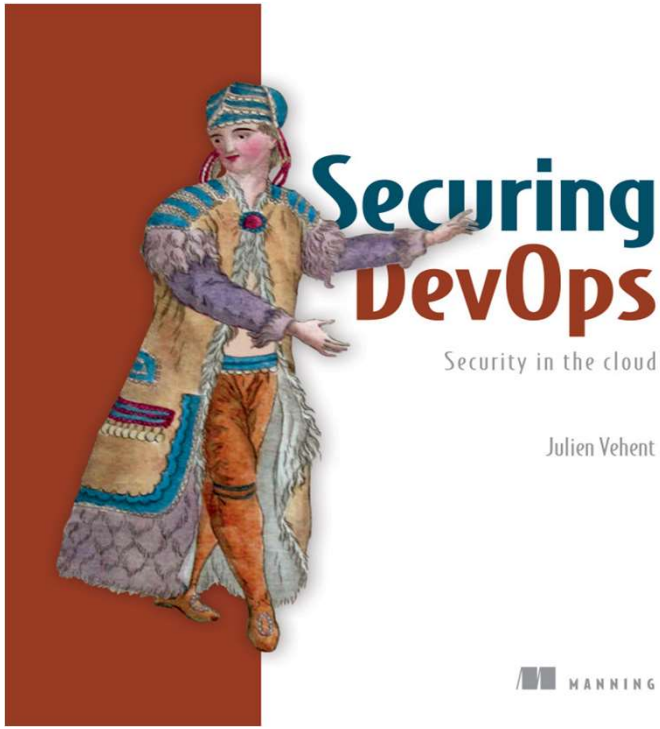

**2.Ensure instant security feedback**


**3.Build a security culture**

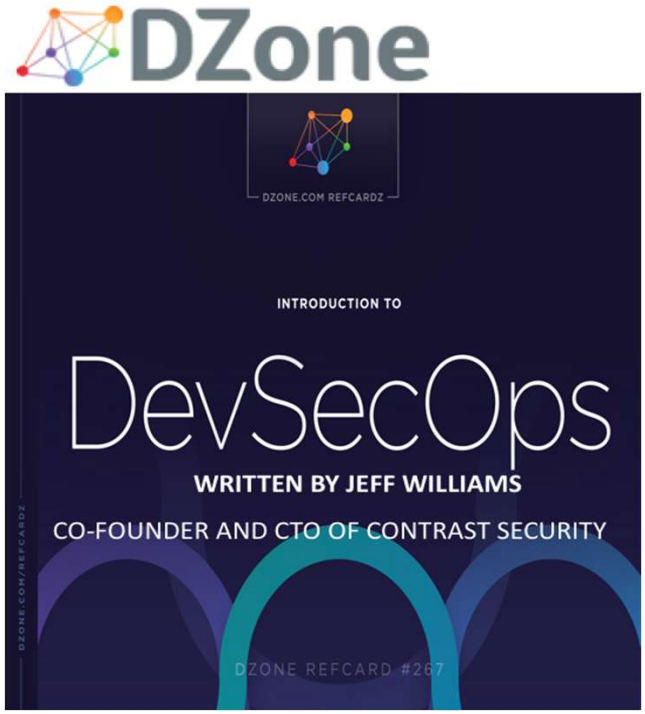



https://itrevolution.com/the-three-ways-principles-underpinning-devops/

# Recommended resources

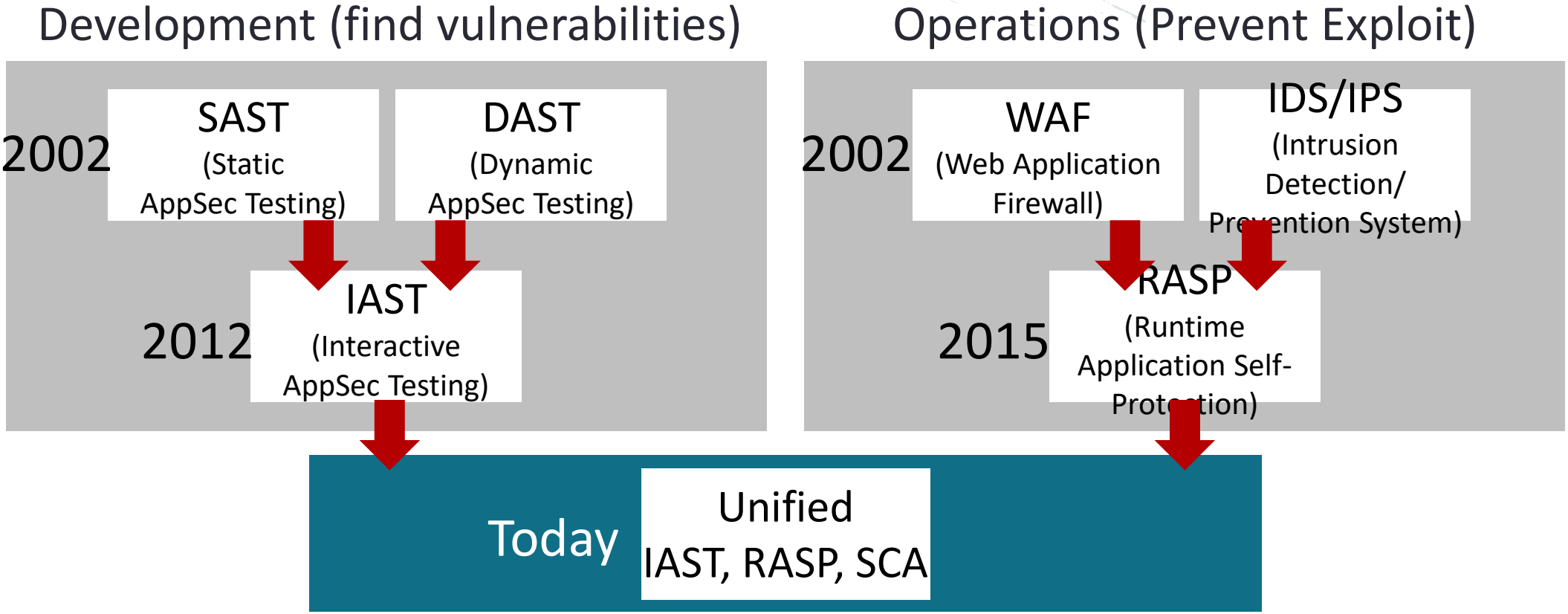



https://www.manning.com/books/securing-devops




https://dzone.com/refcardz/introduction-to-devsecops

# Evolution of appsec Automation



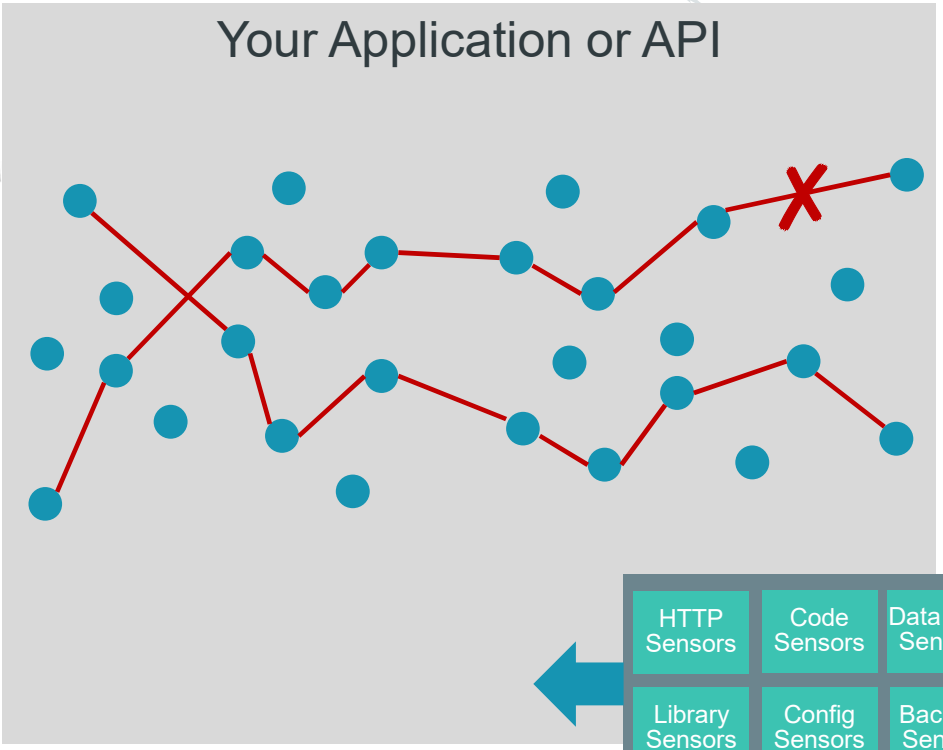
# How IAST and RASP WOrk

**IAST** Interactive Application Security Testing

- Detects vulnerabilities in both custom code and libraries during normal use

**RASP** Runtime Application Self- Protection

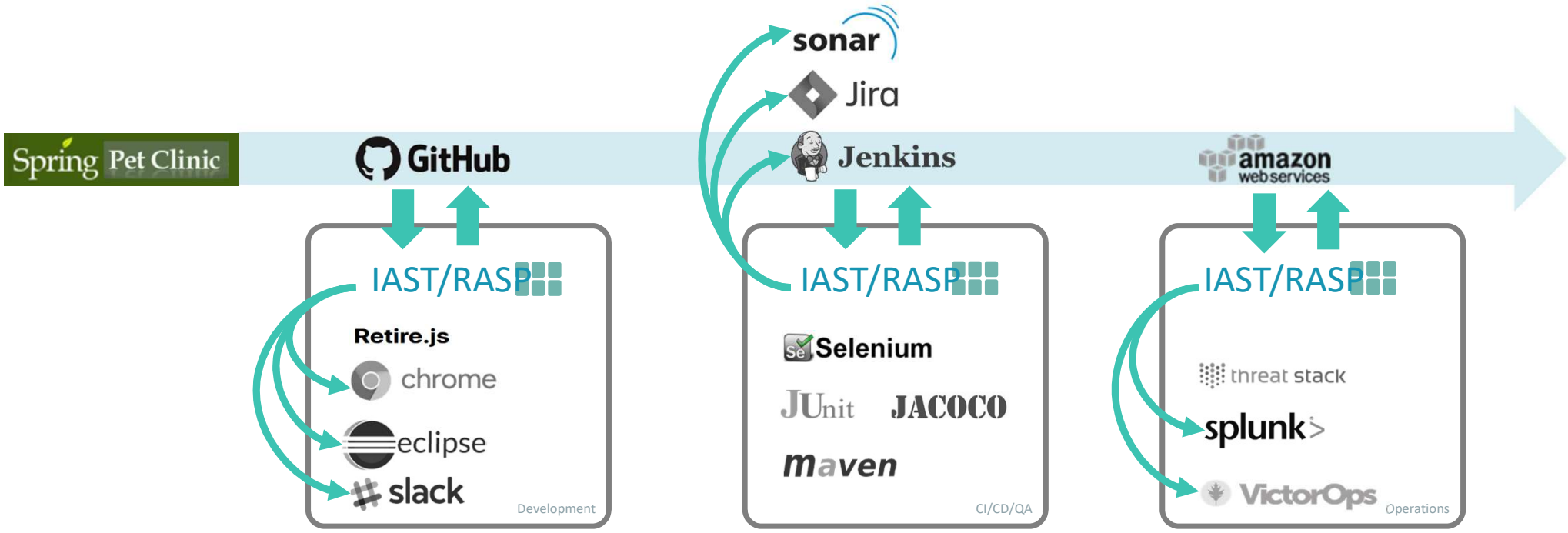
- Prevents vulnerabilities from being exploited in both custom code and libraries




Exploit Prevented

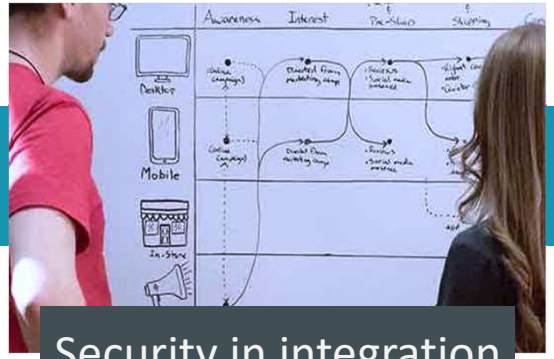
Vulnerability Confirmed

# A DevSECOPS enhanced pipeline



# Shift left, right, and everywhere!

Security in development




Security in integration

Security in operations

**EMPOWER**

- Test my custom code and libraries
- Realtime feedback through my tools
- Don’t slow me down

**ASSURE**

- Don’t slow down my builds
- Integrate with my testing tools
- Real vulns break my build

**PROTECT**

- Tell me who is attacking and how
- Stop vulns from being exploited
- Don’t create alert fatigue

# Security in Development

## Test my custom code AND libraries

- Must be extremely accurate
- Must work on modern apps with APIs and OSS

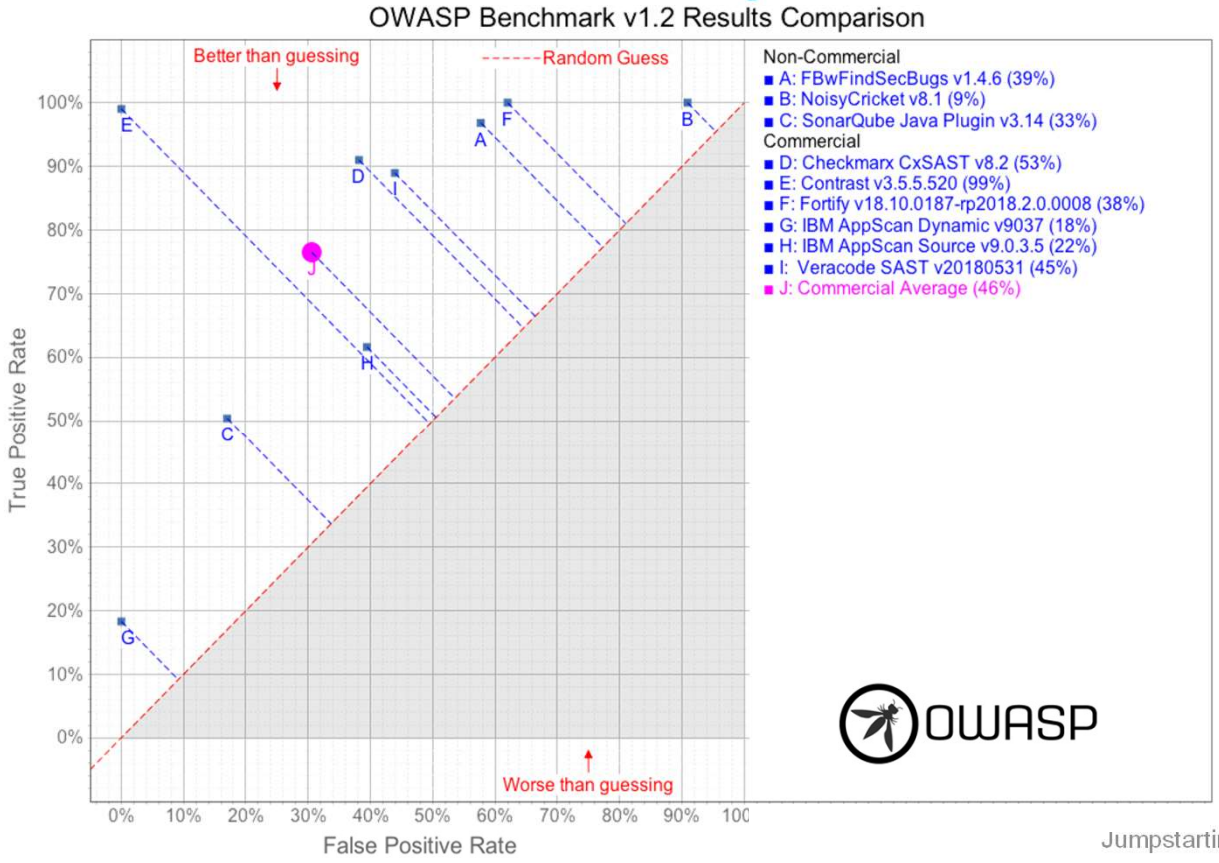
## Realtime feedback through my tools

- Must integrate with tools I'm already using – NO PDF!

## Don't slow me down

- Must not create bottleneck – NO SCANNING!

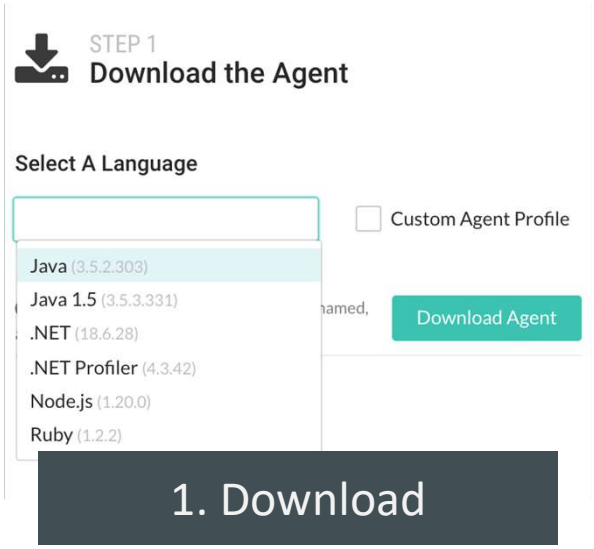
# Automation is all about speed, accuracy, and ease-of-use



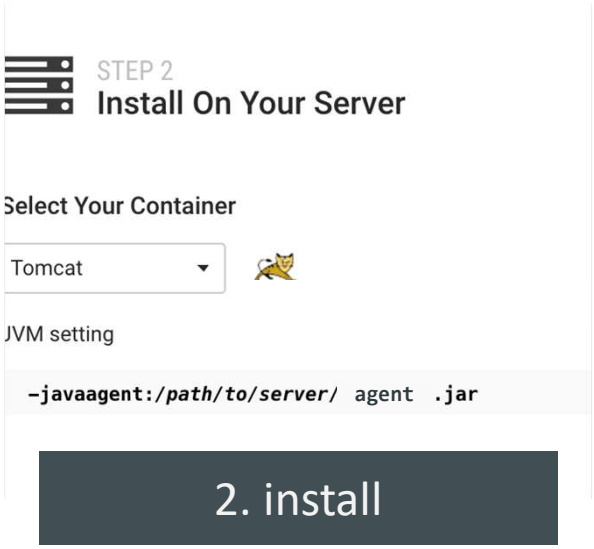

**OWASP Benchmark**

**Free and open application benchmark with thousands of security test cases**

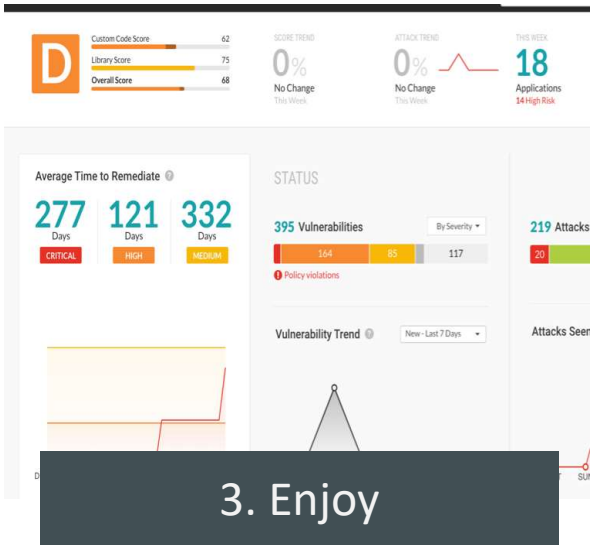
# DOWNLOAD an fast IAST agent



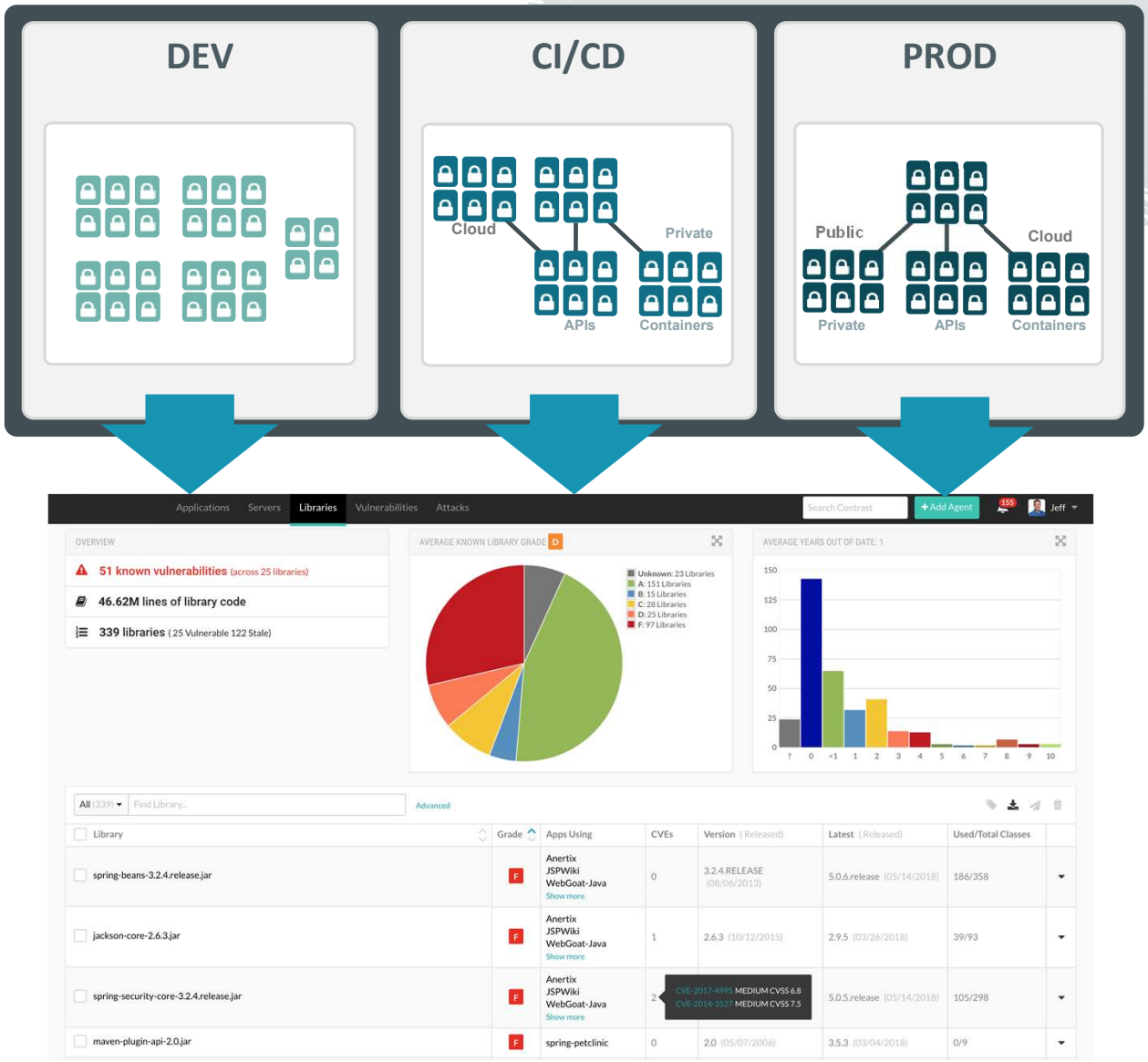

1. Download




2. install



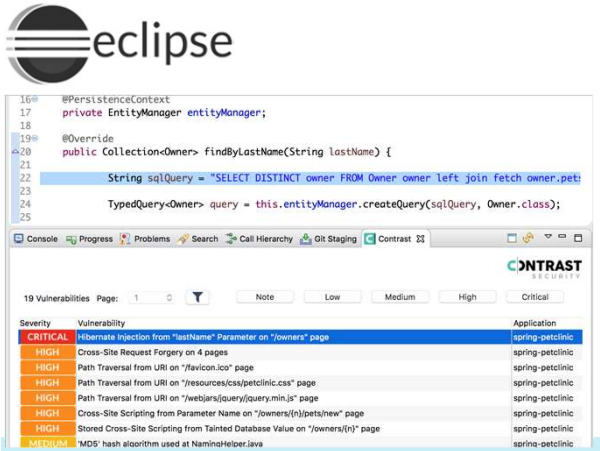

3. Enjoy



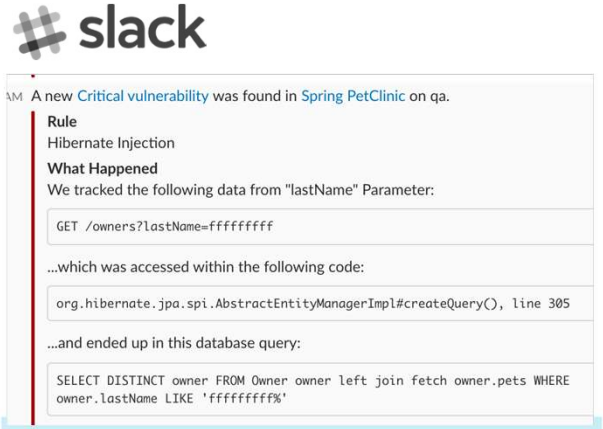

# Empower developers to assess their own security!

Custom code
- and -
Open Source

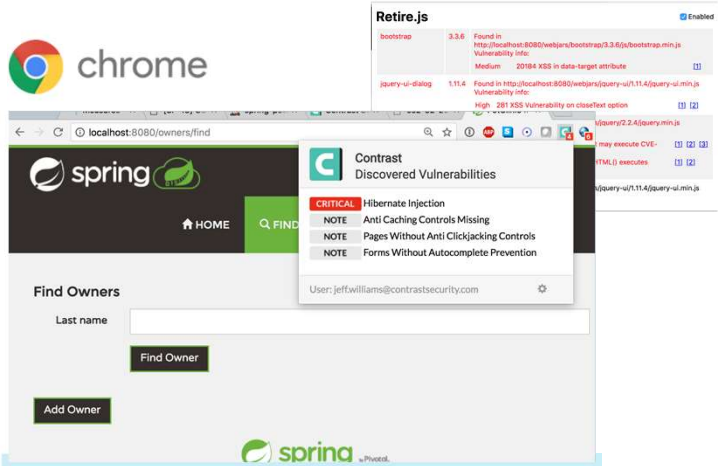
# Security in Everyday environment




## IDE




## Chatops




## Browser

## OTHERS

eclipse
Visual Studio
IntelliJ IDEA
slack
HipChat

Jira
Visual Studio Team Foundation Server
GitHub
Bugzilla
SERENA

Jenkins
Bamboo
maven
gradle

JUnit
nunit
Selenium
webhooks

splunk>
AlienVault
LogRhythm
ArcSight
VictorOps

IBM Bluemix
amazon web services
Microsoft Azure
Pivotal
pagerduty

# Security In Integration

## Don’t slow down my builds

- Fully automated security testing with every build

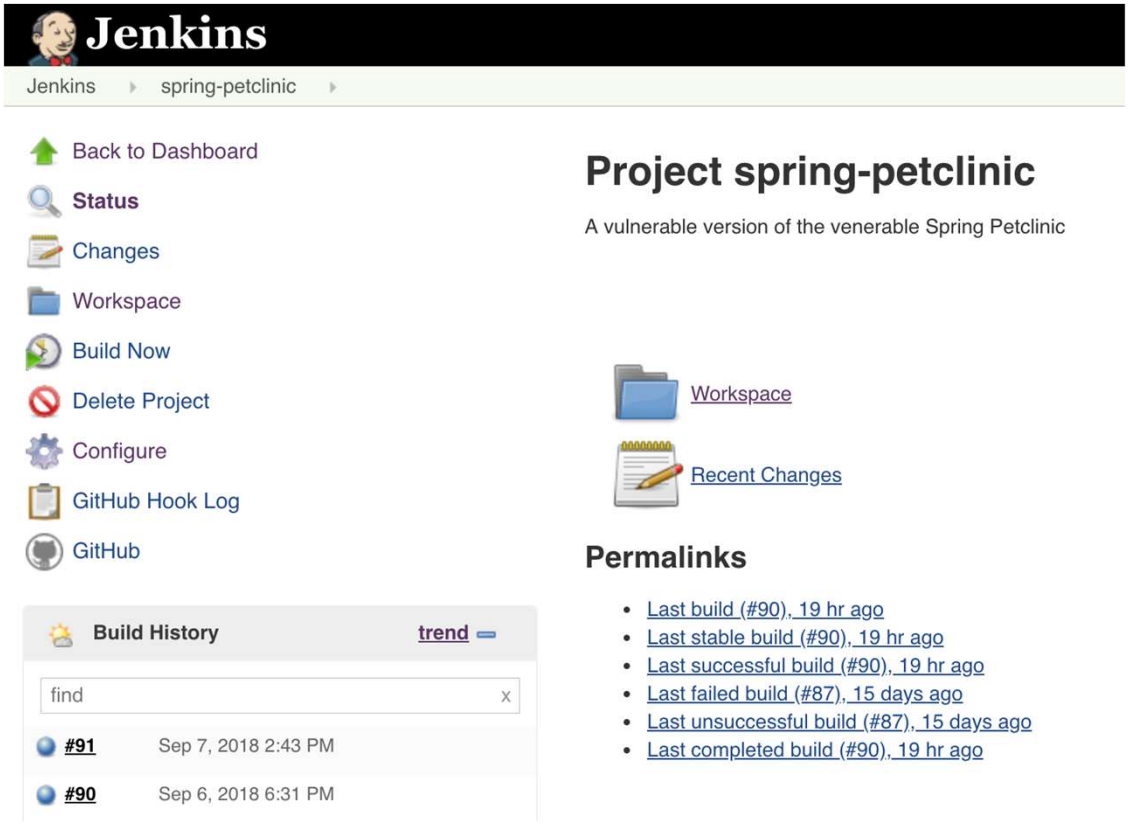
## Integrate with my testing tools

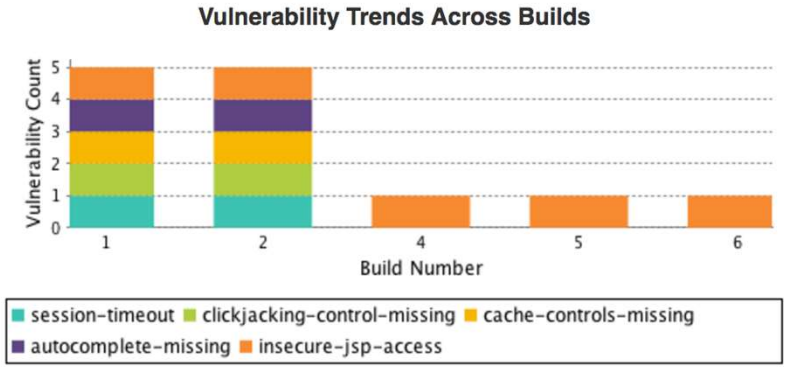
- Plugins, integrations, webhooks, and FULL REST API

## Break my build… but only for real issues

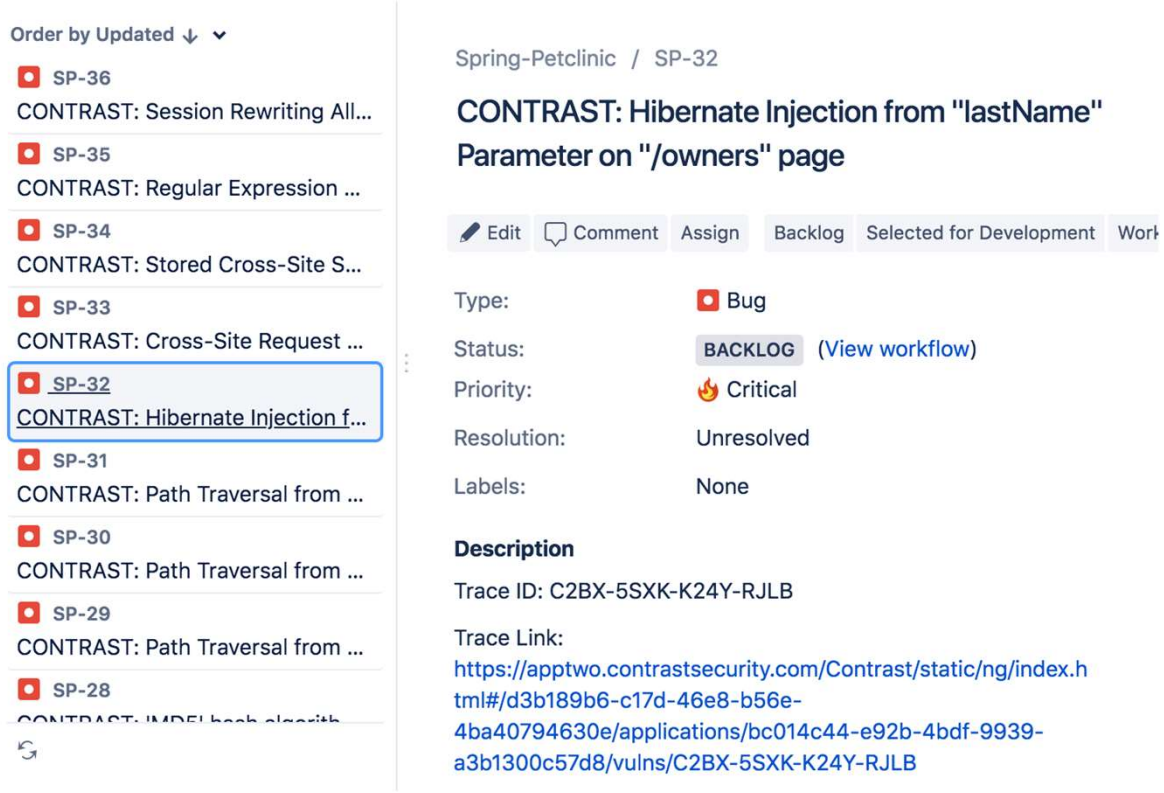
- Set criteria for when to break the build

# Fail the build

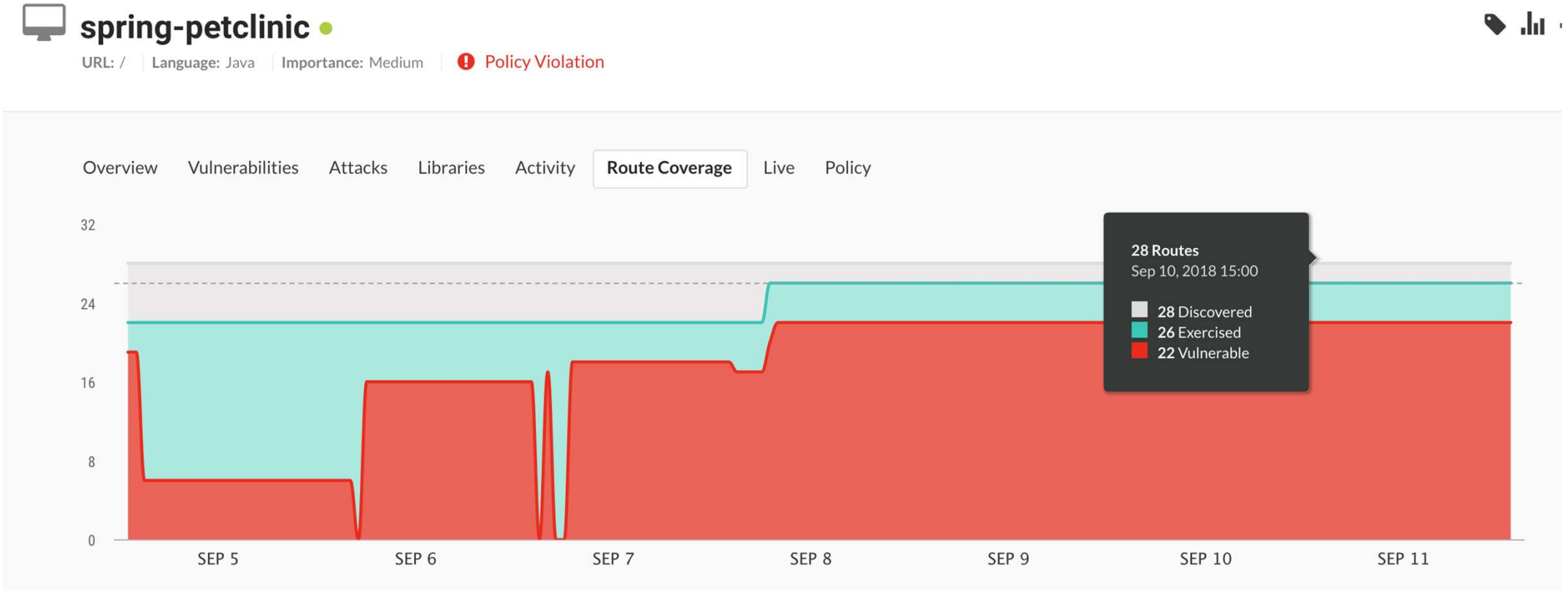


# Automatic bugtracking integration



# Measuring attack surface



# Measuring security testing Coverage

Projects Issues Rules Quality Profiles Quality Gates

Search for projects, sub-projects and files...

Log in

petclinic master

June 7, 2016 9:49 PM Version 1.5.1

Overview Issues Measures Code Activity

Overview

On new code

| | |
|---|---|
| Coverage | 41.7% |
| Lines to Cover | 30 |
| Uncovered Lines | 17 |
| Line Coverage | 43.3% |
| Conditions to Cover | 6 |
| Uncovered Conditions | 4 |
| Condition Coverage | 33.3% |

Overall

| | |
|---|---|
| Coverage | 84.4% |
| Lines to Cover | 267 |
| Uncovered Lines | 33 |
| Line Coverage | 87.6% |
| Conditions to Cover | 60 |
| Uncovered Conditions | 18 |
| Condition Coverage | 70.0% |

Tests

| | |
|---|---|
| Unit Tests | 40 |
| Errors | 0 |
| Failures | 0 |
| Skipped | 1 |
| Success | 100% |
| Duration | 4s |

petclinic

**40 / 40** files


See missing test coverage's long-term risks. Bubble size indicates the volume of uncovered lines, and each bubble's vertical position reflects the volume of missing coverage. Small bubbles on the bottom edge are best.

# Security in operations

## Tell me who is attacking and how

- I need actionable threat intelligence

## Stop vulnerabilities from being exploited

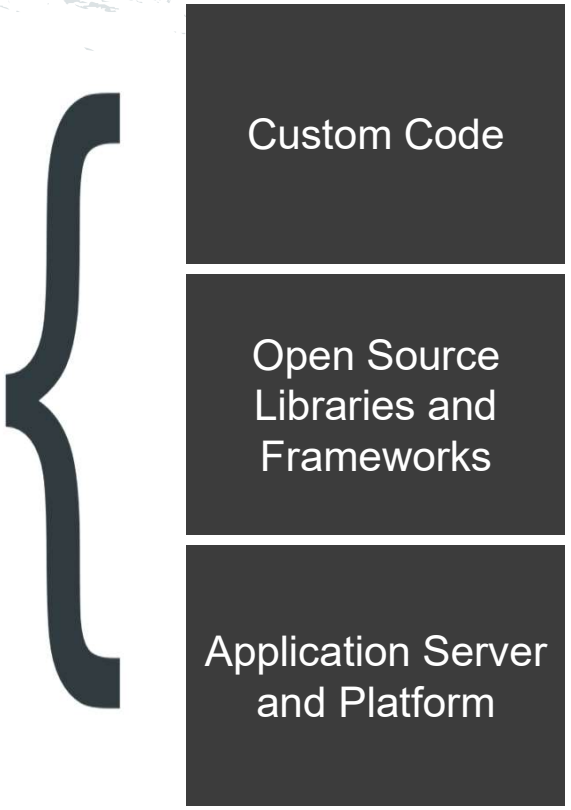
- Must not overblock (FP) or underblock (FN)

## Don’t create alert fatigue

- Don’t warn me about meaningless probes

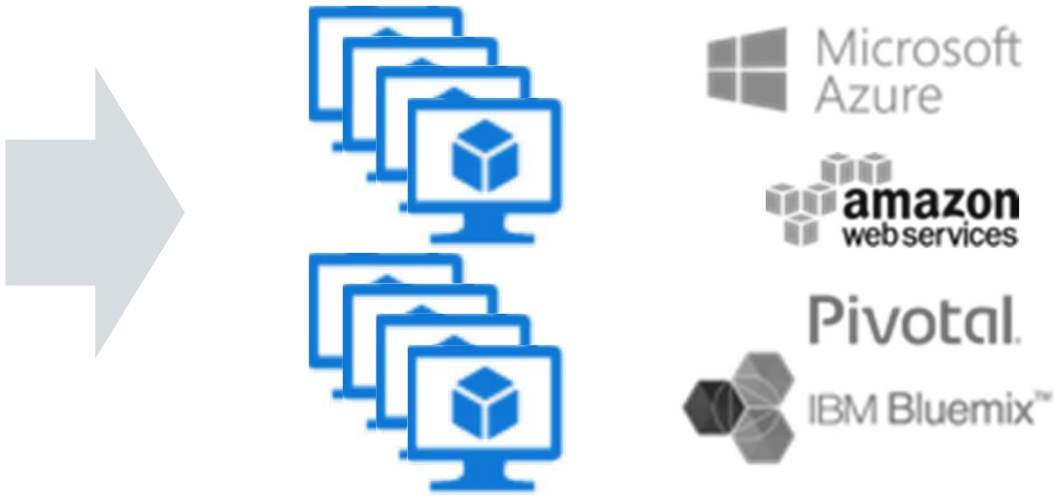
# PROTECT Applications and APIs WITH R

- PREVENTS Known Vulnerabilities from exploit
- Prevents LATENT Vulnerabilities from exploit
- Fast response to prevent NOVEL vulnerabilities from exploit



# RASP deploys with your application

- Ansible
- Puppet
- Docker
- Kubernetes
- Whatever…

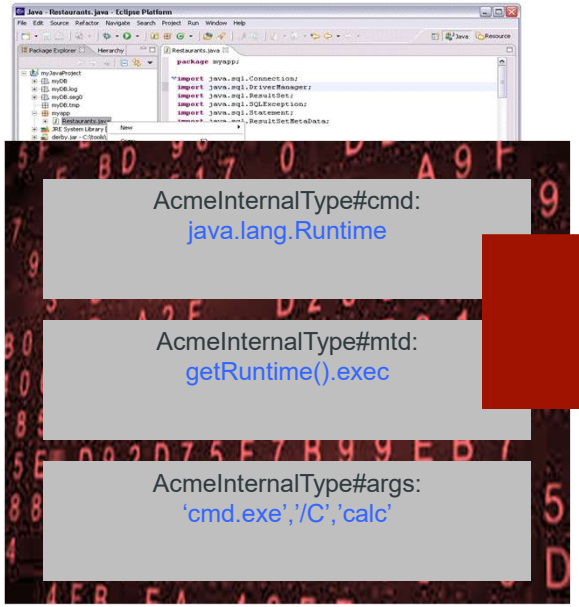


# Protect against latent vulnerabilities


You must have infrastructure to respond within hours.

# RASP supports complex protocols

Bad Guy



AcmeInternalType#cmd:
java.lang.Runtime

AcmeInternalType#mtd:
getRuntime().exec

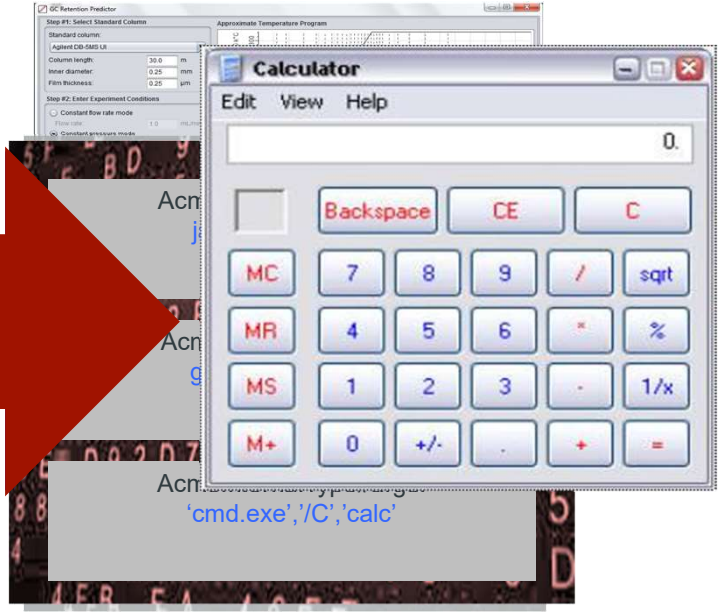
AcmeInternalType#args:
'cmd.exe','/C','calc'

Untrusted deserialization

Attacker sends malicious object

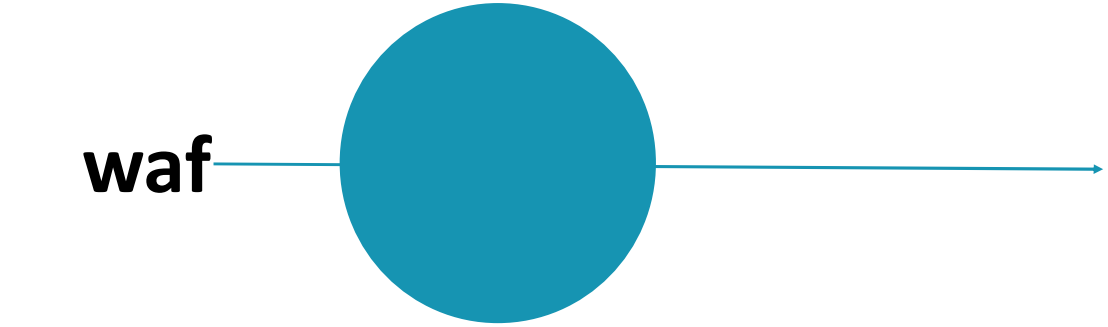
```
POST / HTTP/1.1
User-Agent: Java/1.8.0_74
Host: localhost
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-type: application/x-www-form-urlencoded
Content-Length: 1876
Connection: close

rO0ABXNyADJzdW4ucmVmbGVjdC5hbm5vdGF0aW9uLkFubm90YXRpb25JbnZvY2F0aW9uSGFuZ
GxlclXK9Q8Vy36lAgACTAAMbWVtYmVyVmFsdWVzdAAPTGphdmEvdXRpbC9NYXA7TAAEdHlwZX
QAEUxqYXZhL2xhbmcvQ2xhc3M7eHBzfQAAAAEADWphdmEudXRpbC5NYXB4cgAXamF2YS5sYW5
```

Application

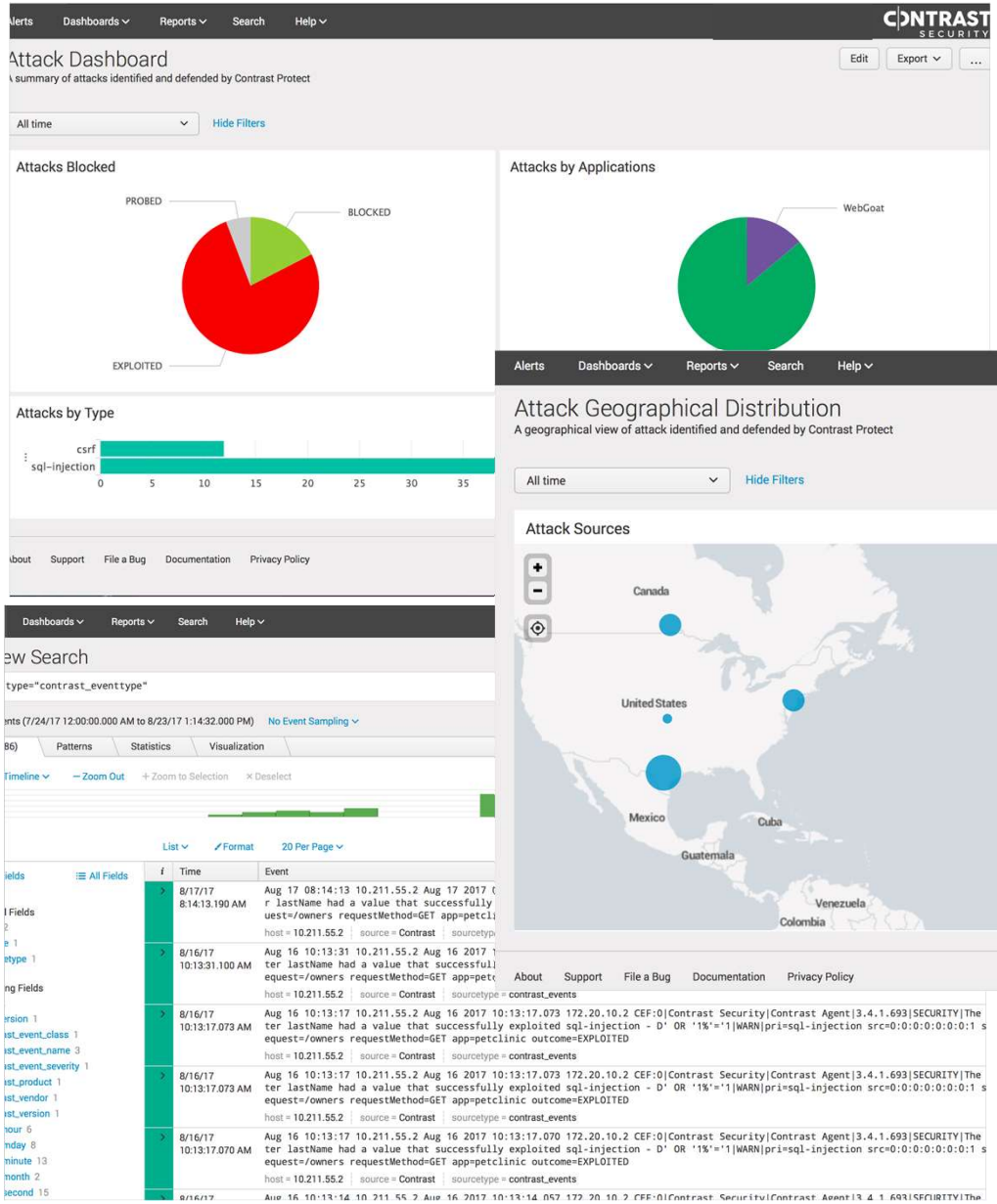



'cmd.exe','/C','calc'

# RASP IS FAST

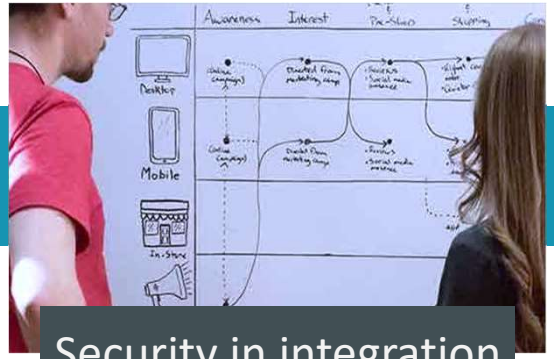


# appsec Threat intelligence



# DevSecOps Pipeline

Security in development




Security in integration

Security in operations

## EMPOWER

- Test my custom code and libraries
- Realtime feedback through my tools
- Don't slow me down

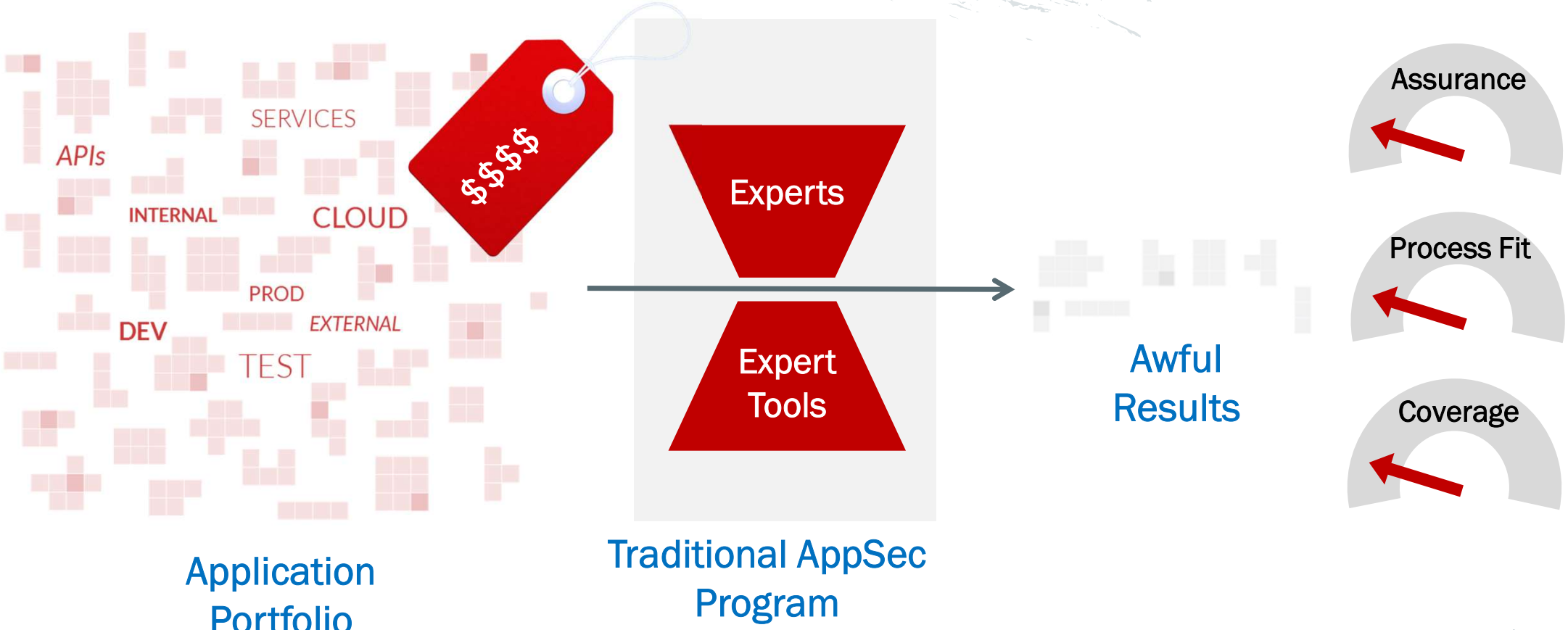
## ASSURE

- Don't slow down my builds
- Integrate with my testing tools
- Real vulns break my build

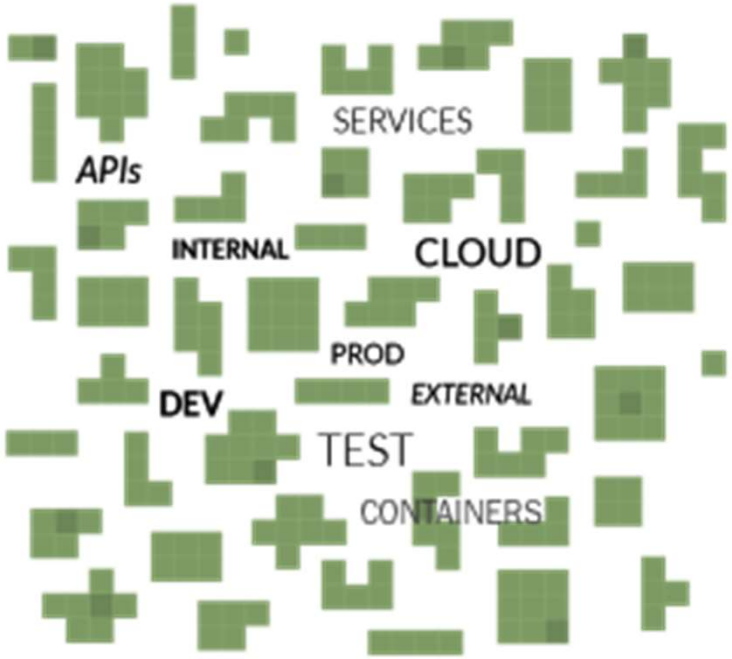
## PROTECT

- Tell me who is attacking and how
- Stop vulns from being exploited
- Don't create alert fatigue

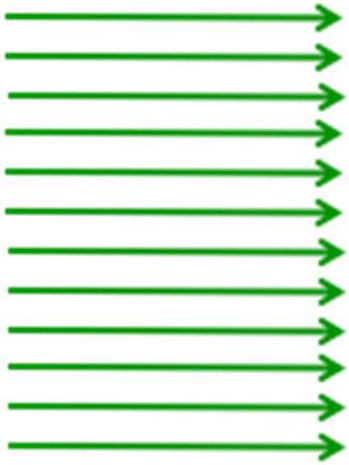
# SUMMARY: Scanners and Firewalls don't Scale



# Summary: devops + security works at scale




Enable application portfolio with IAST/RASP agents




Continuous assessment and protection in parallel

# Free DevSecOps Tools

## OWASP Dependency check

- Free SCA tool to scan for known vulnerabilities in libraries.
- **https://www.owasp.org/index.php/OWASP_Dependency_Check**

## Retire.js

- Free SCA tool to scan for known vulnerabilities in javascript libraries
- **https://retirejs.github.io/retire.js**

## Contrast CE

- Free and full-strength IAST, RASP, and SCA for Java applications and APIs.
- **http://contrastsecurity.com/ce**

OWASP
SINGAPORE

# THANK YOU!

## Ask me anything

Jumpstarting Your DevSecOps Pipeline with IAST and RASP

Jeff Williams @planetlevel

CONTRAST
SECURITY