



# JUMPSTARTING YOUR DEVSECOPS PIPELINE WITH IAST AND RASP

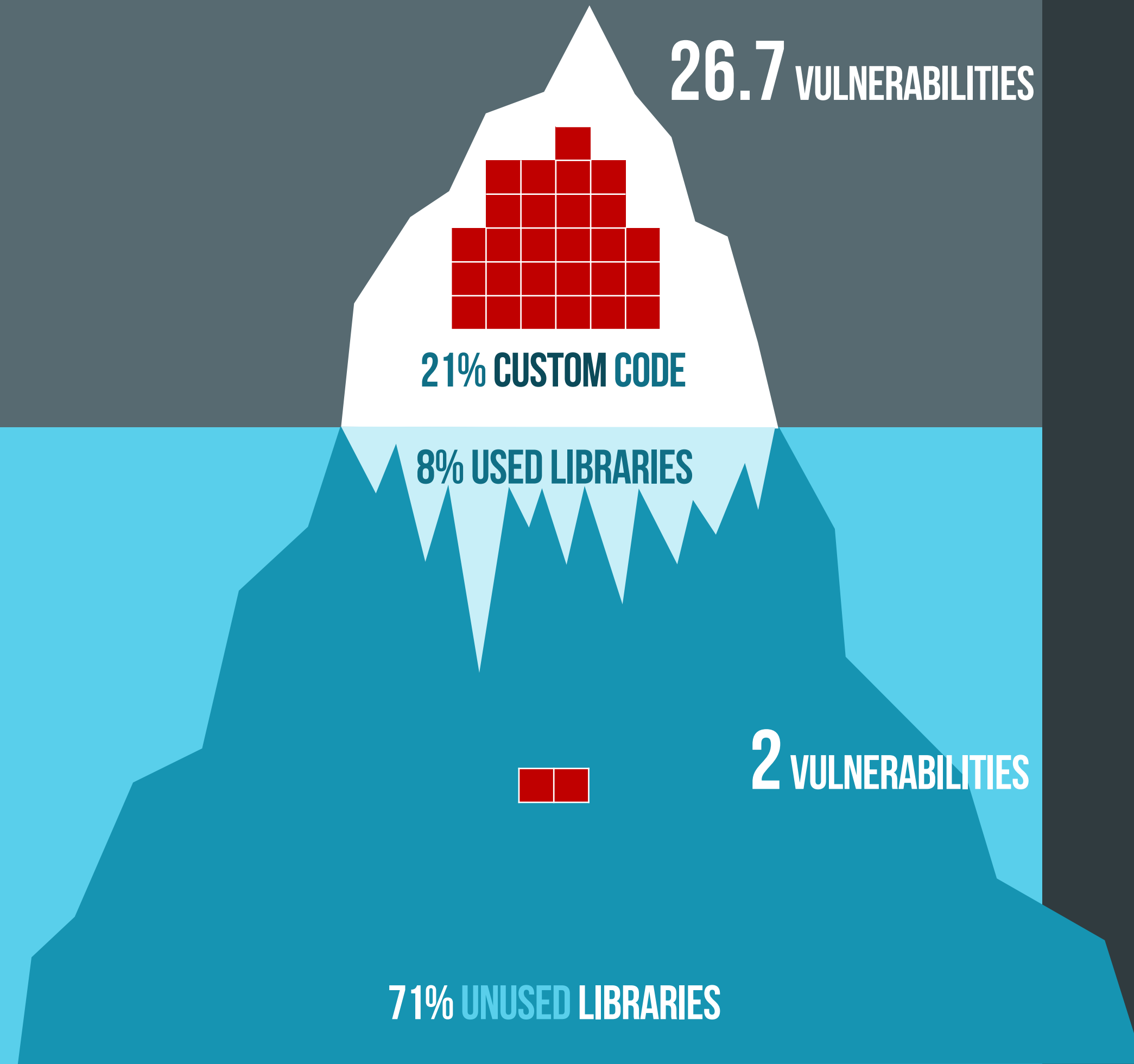


OWASP  
AppSec Europe  
London 2nd-6th June 2018

JEFF WILLIAMS — @PLANETLEVEL  
CTO AND CO-FOUNDER — CONTRAST SECURITY



# THE AVERAGE APPLICATION IS EXTREMELY VULNERABLE



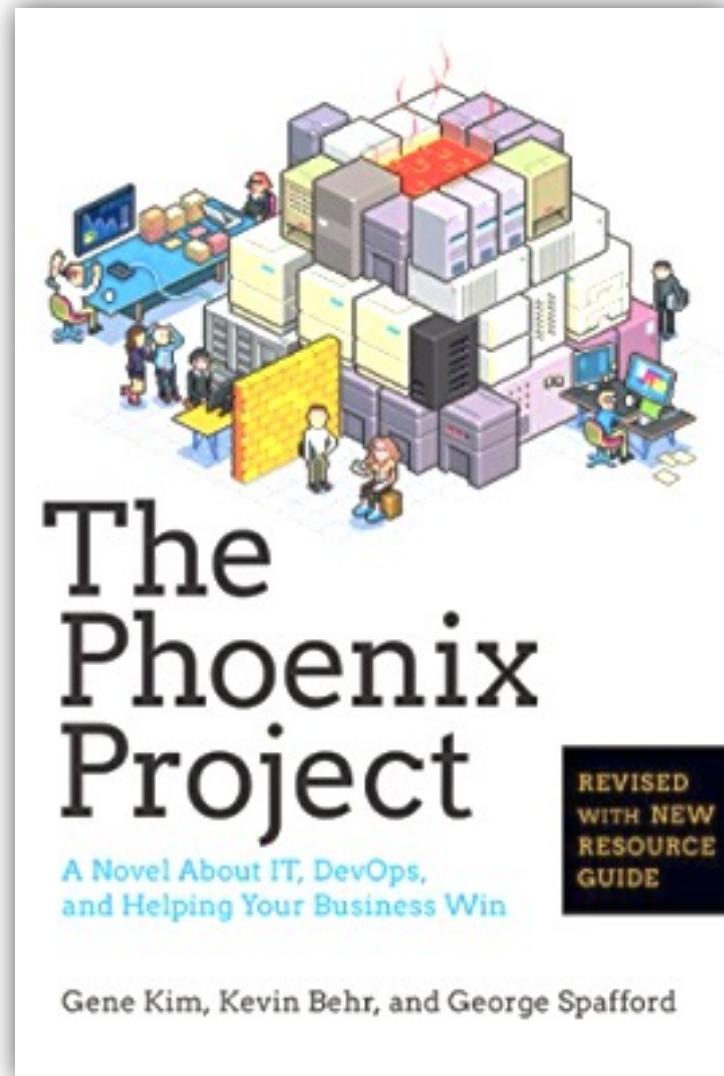
# YOU ARE UNDER ATTACK

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%

# DEVSECOPS IS VERY PROMISING...

## DEVOPS

## DEVSECOPS



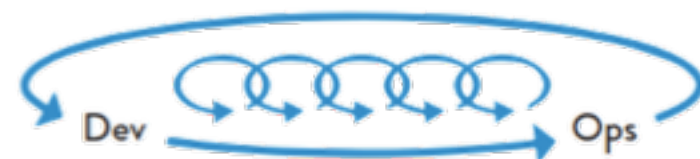
### 1. Establish work flow



### 2. Ensure instant feedback



### 3. Culture of experimentation



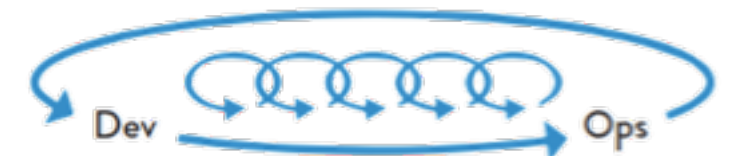
### 1. Establish **security** work flow



### 2. Ensure instant **security** feedback



### 3. Build a **security** culture



# DZONE DEVSECOPS REFCARD

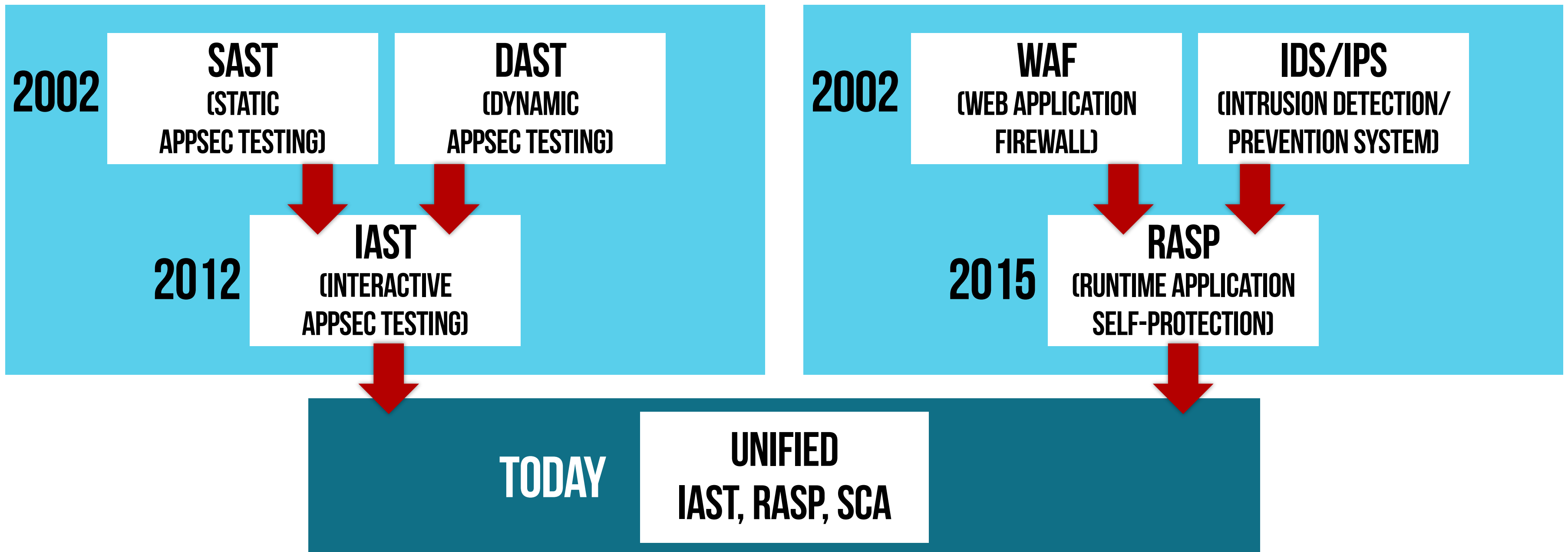


<https://dzone.com/refcardz/introduction-to-devsecops>

# EVOLUTION OF APPSEC AUTOMATION

## DEVELOPMENT (FIND VULNERABILITIES)

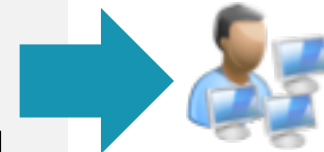
## OPERATIONS (PREVENT EXPLOIT)



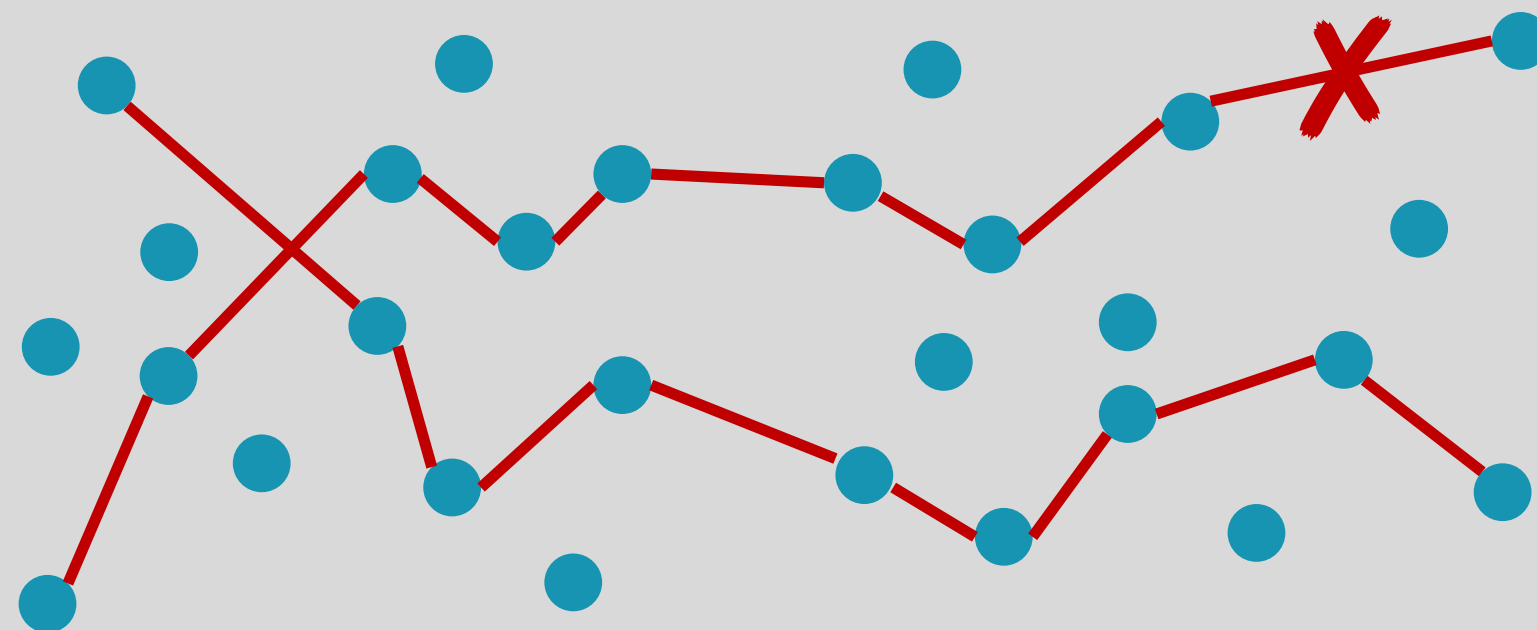
# HOW IAST AND RASP WORK

## IAST INTERACTIVE APPLICATION SECURITY TESTING

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



Your Application or API

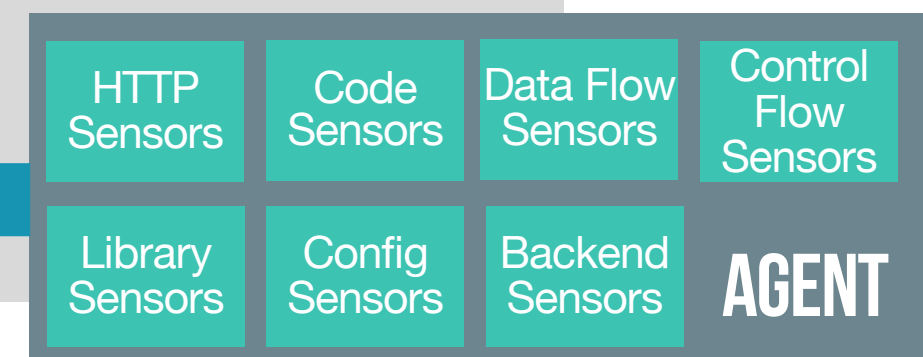


EXPLOIT PREVENTED

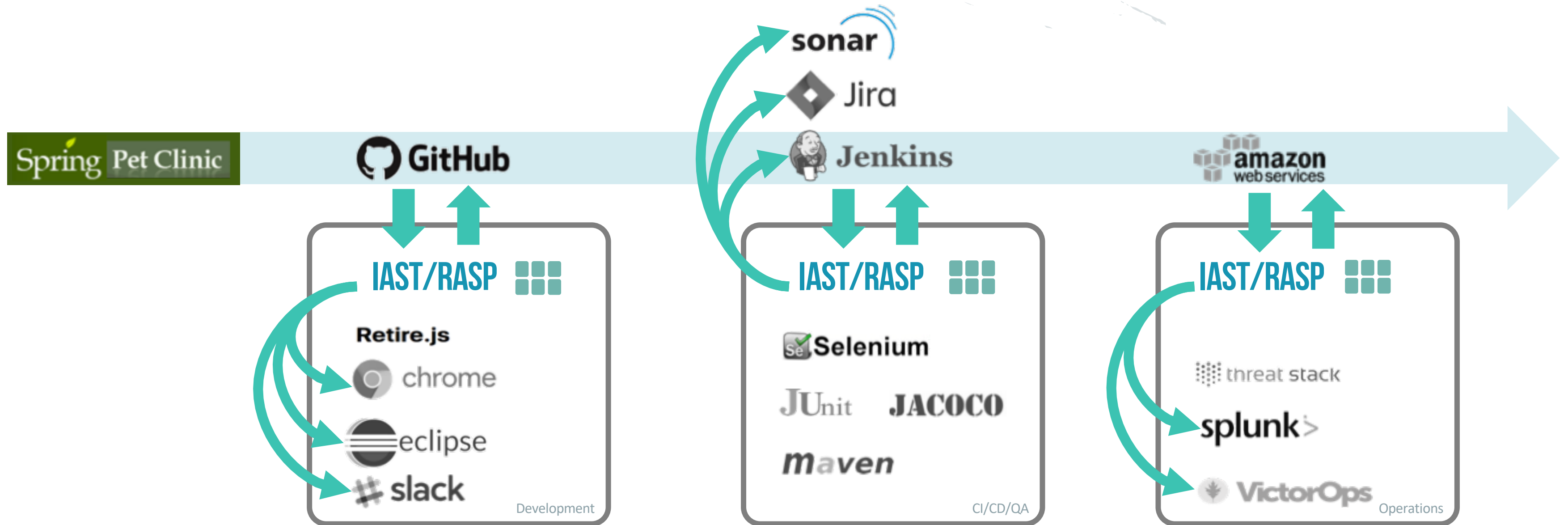
VULNERABILITY CONFIRMED

## RASP RUNTIME APPLICATION SELF-PROTECTION

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



# TURNING DEVOPS INTO DEVSECOPS





# TODAY'S MISSION...



**1. ADD SECURITY TO DEVELOPMENT**



**2. LOCK DOWN OPEN SOURCE LIBRARIES**



**3. ENABLE AUTOMATIC SECURITY TESTING**



**4. PREVENT EXPLOITS IN OPERATION**

# DEVSECOPS GOALS:

## DEV

### SECURITY

- Must cover policies/rules I care about
- Must have minimal false positives/false negatives

### SPEED

- Must integrate in tools I'm already using – NOT PDF
- Must notify with ChatOps!

### SCALE

- Must not create bottleneck – NO SCANNING
- Must work on my portfolio including APIs!

# GET AN IAST/RASP AGENT

<https://www.contrastsecurity.com/ce>

**STEP 1**  
**Download the Agent**

Select A Language

Custom Agent Profile

Download Agent

**1. DOWNLOAD**

**STEP 2**  
**Install On Your Server**

Select Your Container

Tomcat

Enable Contrast. Add the following

JVM setting

```
-javaagent:/path/to/server/contrast.jar
```

**2. INSTALL**

Custom Code Score 62  
Library Score 75  
Overall Score 68

SCORE TREND  
0% No Change This Week

ATTACK TREND  
0% No Change This Week

THIS WEEK  
18 Applications  
14 High Risk

Average Time to Remediate

277 Days CRITICAL  
121 Days HIGH  
332 Days MEDIUM

STATUS  
395 Vulnerabilities  
219 Attacks

**3. ENJOY**

# USING IAST FROM WITHIN MAVEN

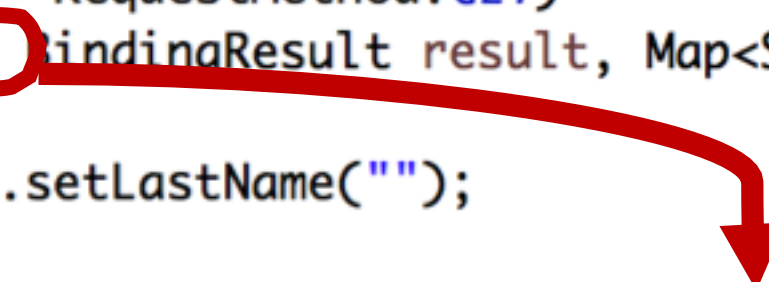
```
<plugin>
  <groupId>org.springframework.boot</groupId>
  <artifactId>spring-boot-maven-plugin</artifactId>
  <configuration>
    <!-- Verify security and coverage during normal use -->
    <jvmArguments>
      -javaagent:${project.basedir}/jacocoagent.jar=destfile=${project.basedir}/target/jacoco.exec
      -javaagent:${project.basedir}/contrast.jar
      -Dcontrast.dir=${project.basedir}/working
      -Dcontrast.log.daily=true
    </jvmArguments>
  </configuration>
</executions>
```

# HQL INJECTION

```
@RequestMapping(value = "/owners", method = RequestMethod.GET)
public String processFindForm(Owner owner, BindingResult result, Map<String, Object> model) {

    if (owner.getLastName() == null) owner.setLastName("");

    Collection<Owner> results = this.owners.findByLastName(owner.getLastName());
}
```




```
@Override
public Collection<Owner> findByLastName(String lastName) {

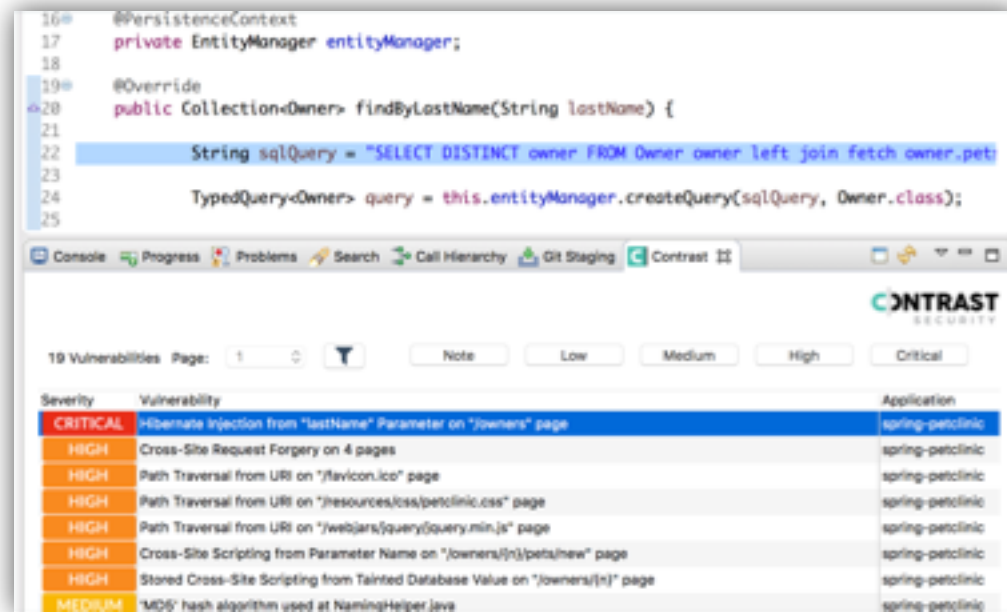
    String sqlQuery = "SELECT DISTINCT owner FROM Owner owner left join fetch owner.pets WHERE owner.lastName = '" + lastName + "'";

    TypedQuery<Owner> query = this.entityManager.createQuery(sqlQuery, Owner.class);

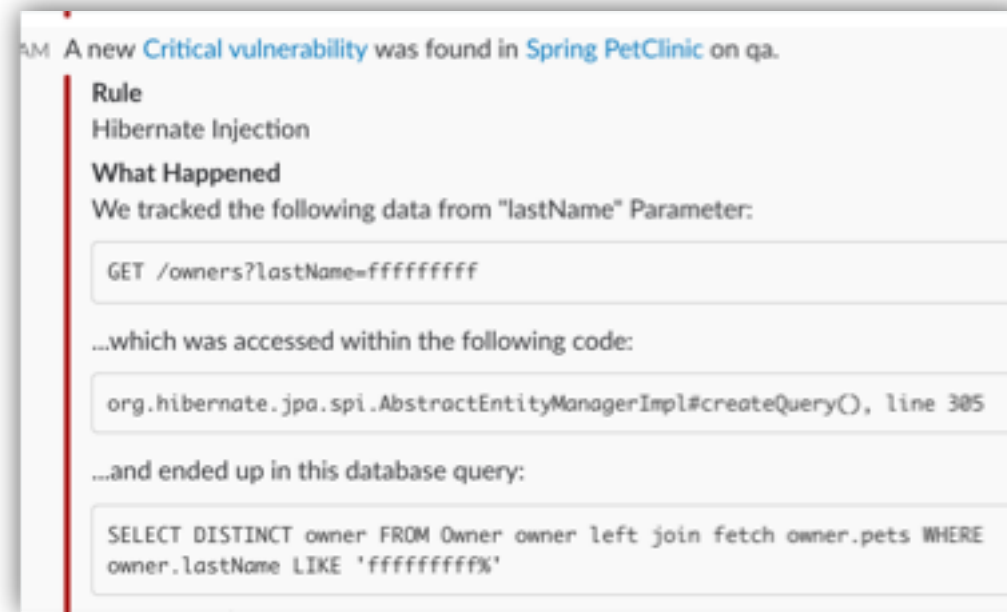
    return query.getResultList();
}
```



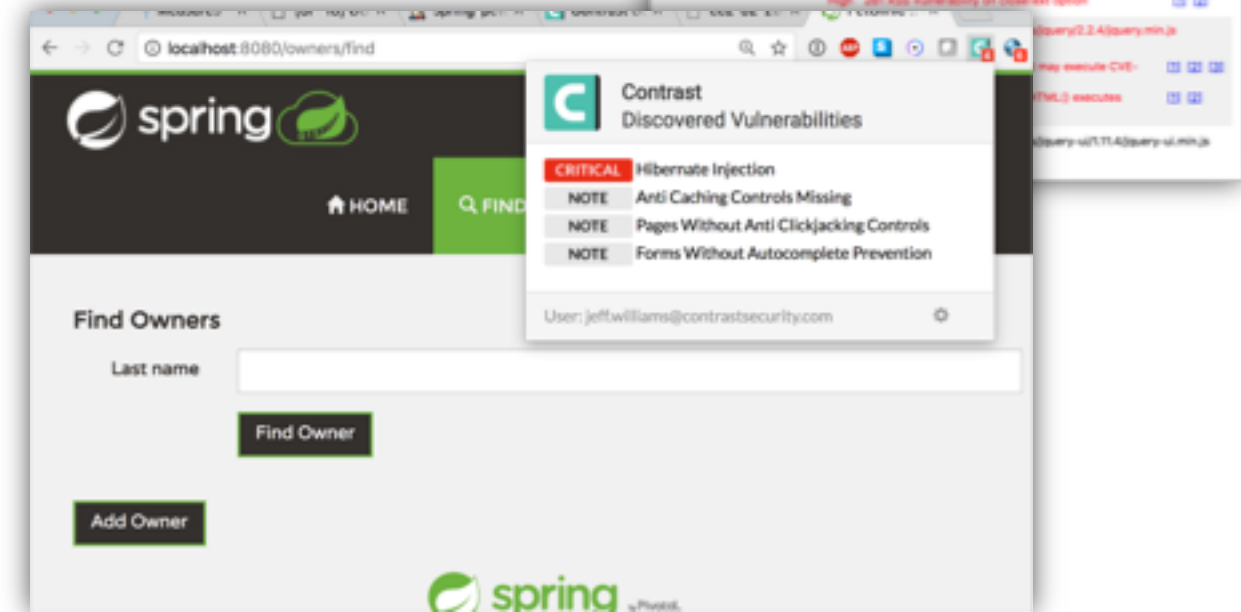
# HOW DO YOU WANT YOUR SECURITY?



IDE

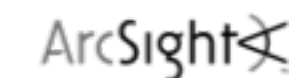


CHATOPS



BROWSER

OTHERS:



# TODAY'S MISSION...



- Security
- Speed
- Scale



1. ADD SECURITY TO DEVELOPMENT



2. LOCK DOWN OPEN SOURCE LIBRARIES



3. ENABLE AUTOMATIC SECURITY TESTING



4. PREVENT EXPLOITS IN OPERATION

# DEVSECOPS GOALS: OPEN SOURCE

## INVENTORY

- Must identify all components everywhere
- Must show libraries that are actually used (72% unused)

## ASSESS

- Must pinpoint apps and servers with vulnerable libraries
- Must identify both known and unknown vulnerabilities

## PROTECT

- Detection isn't enough
- Protect against both known and unknown flaws



All (121) Find Event 03/08/2017 02:19 pm - 04/07/2017 02:19 pm Advanced You have filters set. Clear

### CVE-2017-5638 Event from 222.186.34.77

PROBED When: 04/04/2017 02:03 AM URL: /Contrast/error/404.html

+ Add Exclusion

Overview Request Discussion 0

We observed an attack against CVE-2017-5638 enter the application through the HTTP Request Header "content-type":

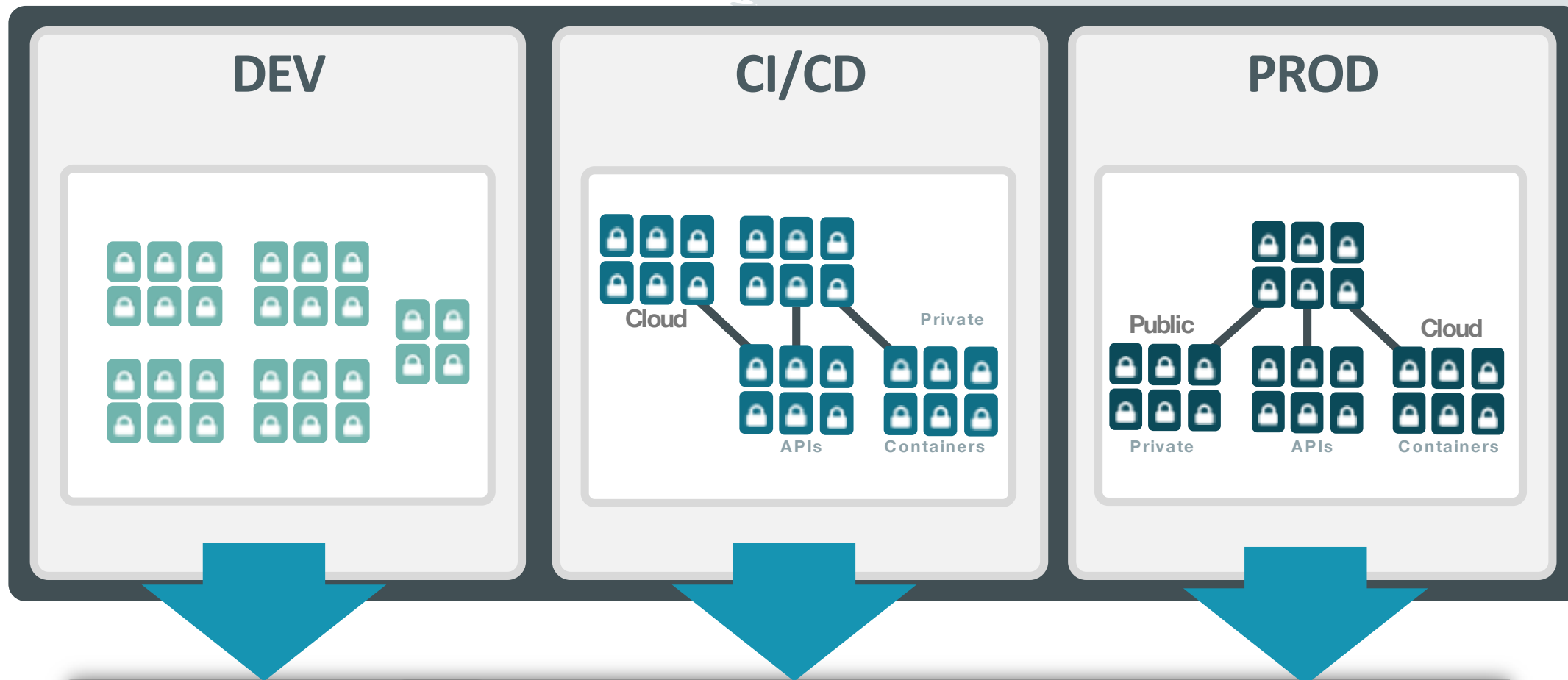
```
GET /Contrast/error/404.html HTTP/1.0
Accept: */*
Accept-Language: zh-cn
Connection: close
Content-Type: %({(#_memberAccess=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#wmres=#context['com.opensymphony.xwork2.dispatcher.HttpServletResponse']).(#wmres.getWriter().print("S2-045 dir--***")).(#wmreq=#context.get('com.opensymphony.xwork2.dispatcher.HttpServletRequest')).(#wmres.getWriter().println(#wmreq.getSession().getServletContext().getRealPath("/"))).(#wmres.getWriter().flush()).(#wmres.getWriter().close()))).multipart/form-data
Cookie: AWSELB=539F750F10478D4E063589242269EA3B38F3BDF0DC18B0F7A35AA369BDF525DBE006E8DA108F4FC48572AD541F9C37F85D9F6382CF8E20CC1054089C7766B93FCB079E28F15EF3BAF264DDEB64E0691CC65B16F00F;JSESSIONID=821ABF417420EEE1EEEE9AA7F0BA4640
Host: 127.0.0.1:8080
Referer: http://54.86.199.1
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)
X-Forwarded-For: 222.186.34.77
X-Forwarded-Host: app.contrastsecurity.com
X-Forwarded-Port: 443
X-Forwarded-Proto: https
X-Forwarded-Server: app.contrastsecurity.com
```

# ACTUAL ATTACK ON CVE-2017-5638

# HOW FAST CAN YOU RESPOND?



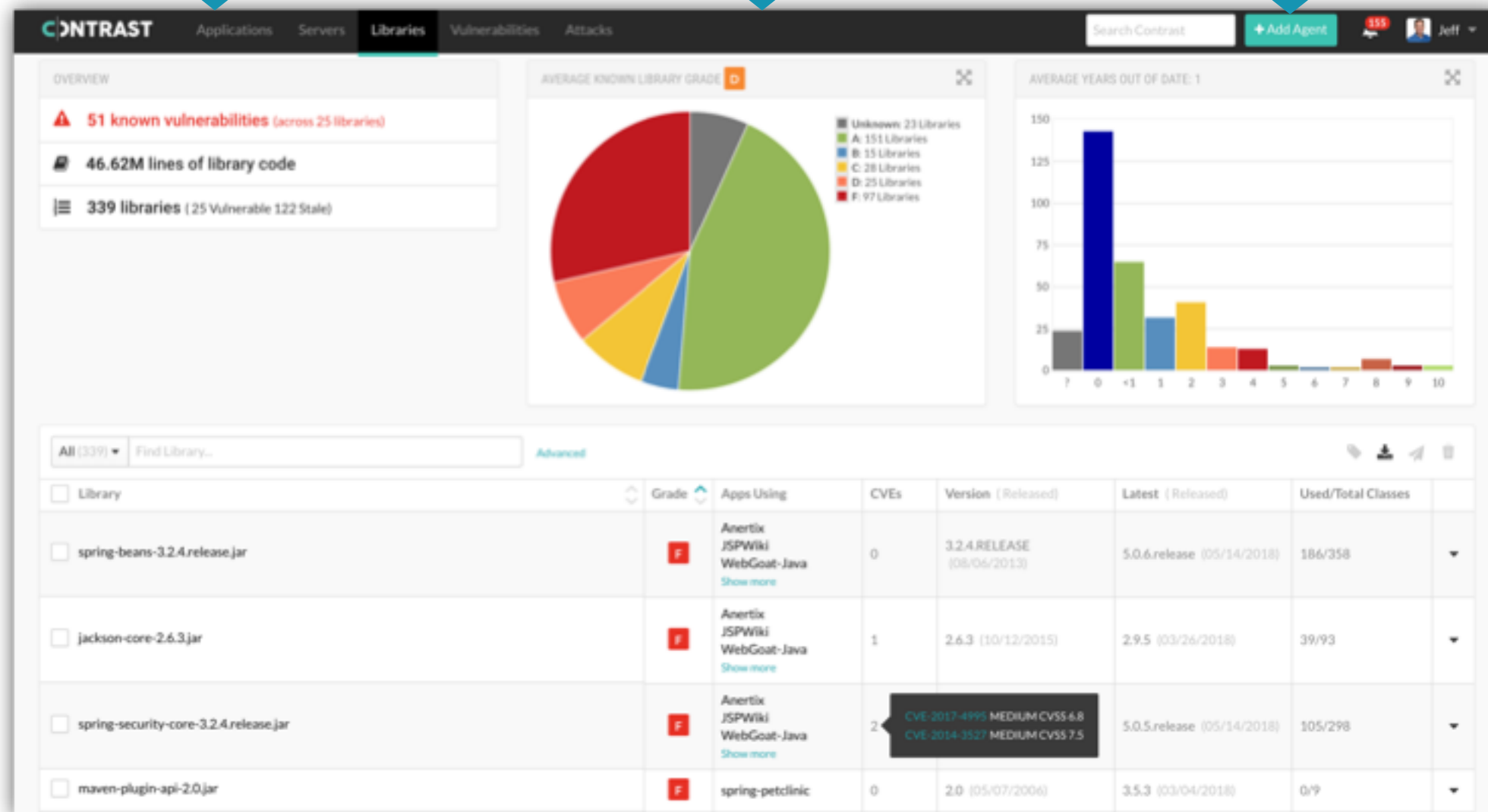
**YOU MUST HAVE THE  
INFRASTRUCTURE IN PLACE TO  
RESPOND WITHIN HOURS.**



# ASSESS OSS WITH IAST

1. CONTINUOUSLY  
INVENTORY ALL OSS

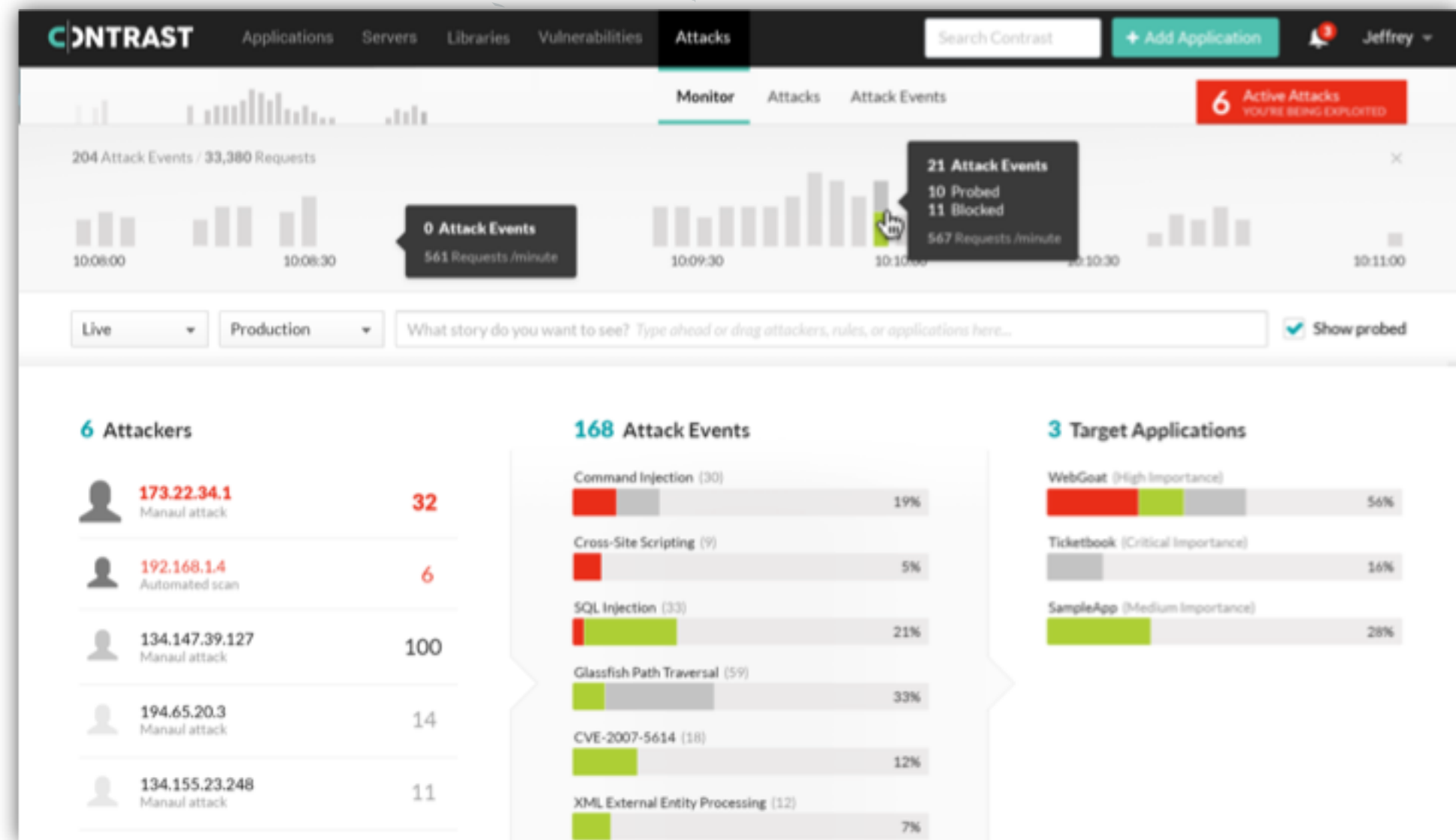
2. AUTOMATICALLY DETECT  
VULNERABILITIES IN OSS



# PROTECT OSS WITH RASP

1. PREVENT **KNOWN** OSS VULNERABILITIES FROM BEING EXPLOITED

2. DEFEND APPLICATIONS FROM ATTACKS ON **UNKNOWN** OSS VULNERABILITIES



# TODAY'S MISSION...



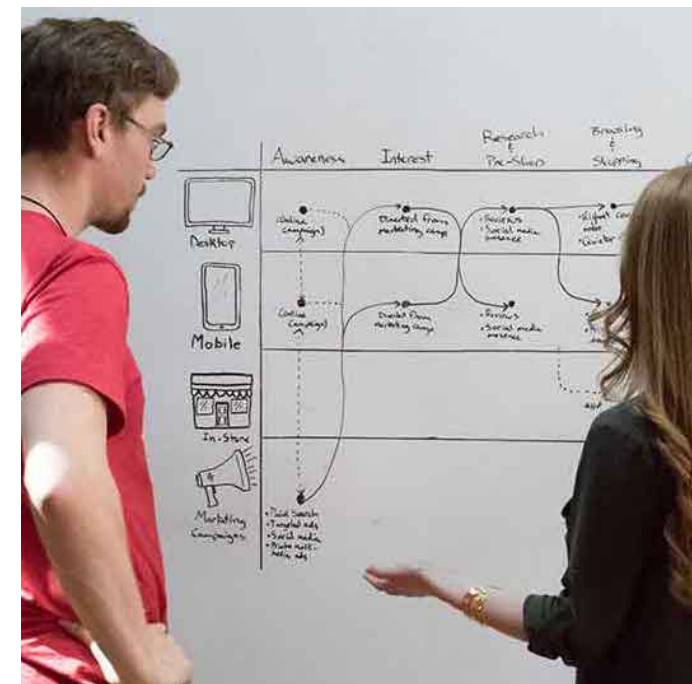
- Security
- Speed
- Scale

1. ADD SECURITY TO DEVELOPMENT

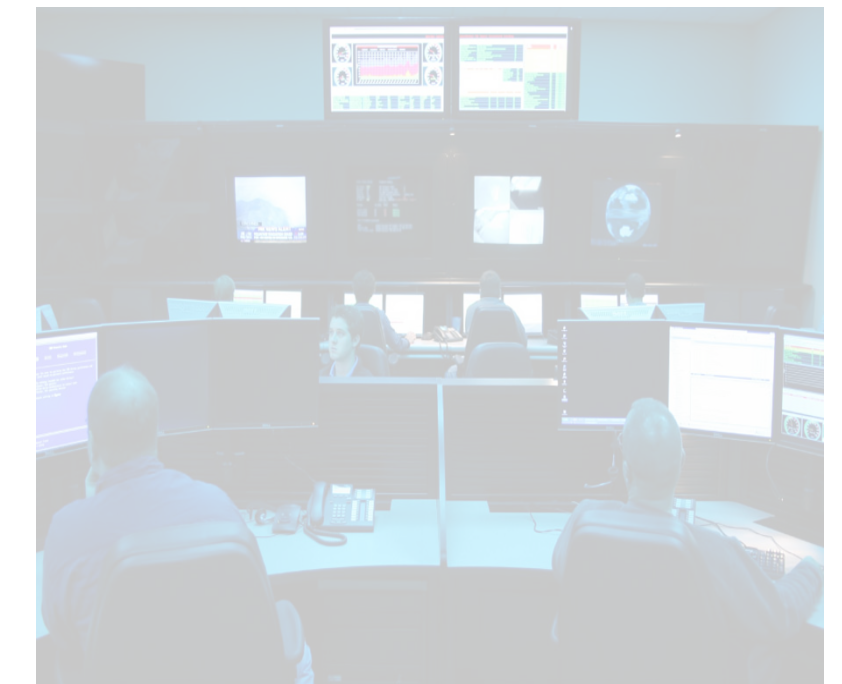


- Inventory
- Assess
- Protect

2. LOCK DOWN OPEN SOURCE LIBRARIES



3. ENABLE AUTOMATIC SECURITY TESTING



4. PREVENT EXPLOITS IN OPERATION

# DEVSECOPS GOALS:

## CI / CD

### CONTINUOUS

- Security testing automatically with every build
- Works without extensive test cases

### INTEGRATED

- Open vulnerability tickets automatically
- Plugins, integrations, webhooks, and full REST API

### FEEDBACK

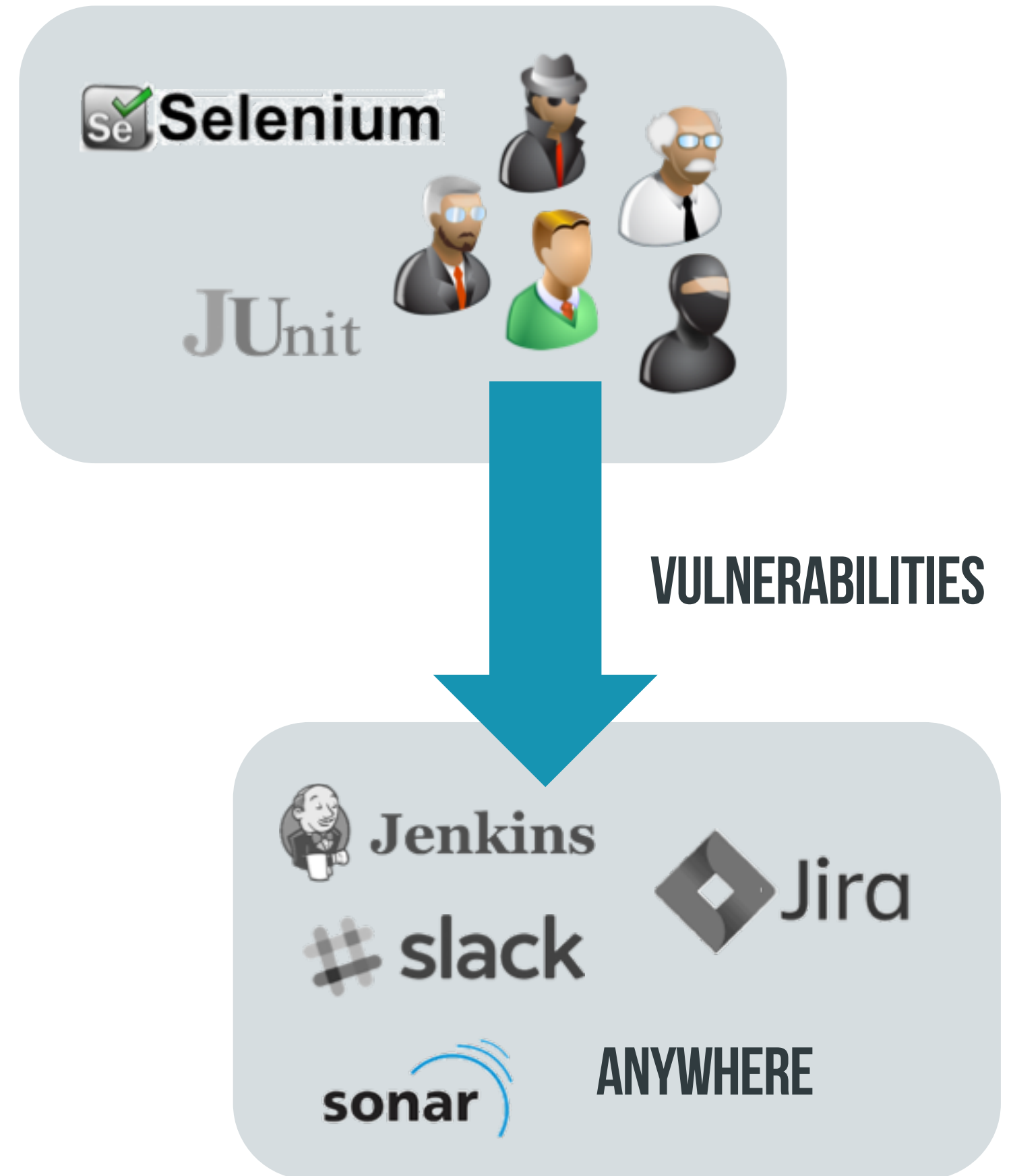
- Set criteria for when to break the build
- Manage appsec policy across application portfolio

# IAST WORKS THE SAME IN CI/CD

```
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-surefire-plugin</artifactId>
  <configuration>
    <!-- Verify security and coverage during automated tests. -->
    <argLine>
      -javaagent:${project.basedir}/jacocoagent.jar=destfile=${project.basedir}/target/jacoco.exec
      -javaagent:${project.basedir}/contrast.jar
      -Dcontrast.dir=${project.basedir}/working
      -Dcontrast.log.daily=true
    </argLine>
  </configuration>
</plugin>
```

**IAST WORKS WITH  
ALL TYPES OF  
TESTING...**

**...EVEN PRODUCTION**





Overview

On new code

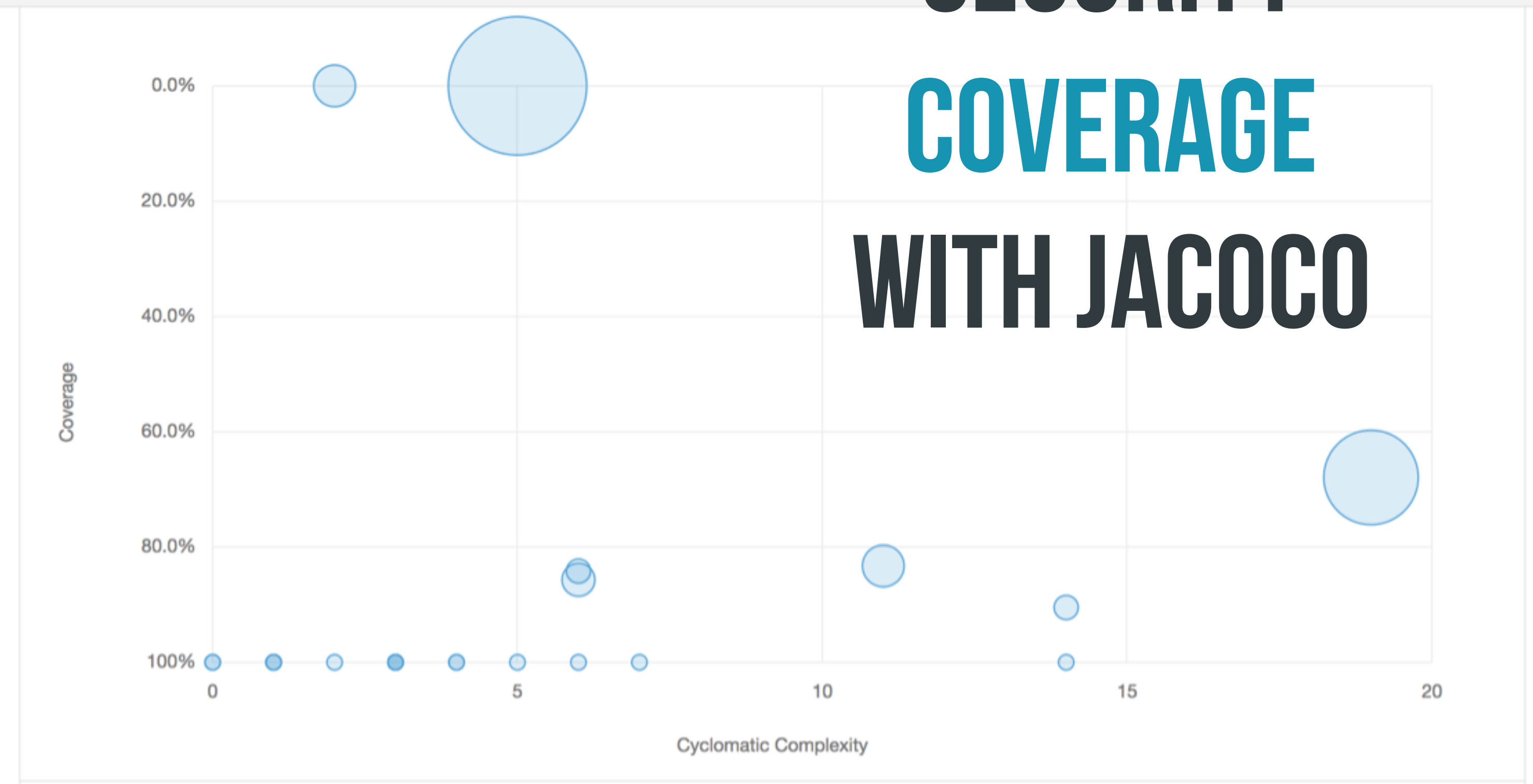
Coverage	41.7%
Lines to Cover	30
Uncovered Lines	17
Line Coverage	43.3%
Conditions to Cover	6
Uncovered Conditions	4
Condition Coverage	33.3%

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



# SECURITY COVERAGE WITH JACOOCO

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.

# TODAY'S MISSION...



✓

- Security
- Speed
- Scale


1. ADD SECURITY TO DEVELOPMENT



✓

- Inventory
- Assess
- Protect

2. LOCK DOWN OPEN SOURCE LIBRARIES



✓

- Continuous
- Integrated
- Feedback

3. ENABLE AUTOMATIC SECURITY TESTING



4. PREVENT EXPLOITS IN OPERATION

# DEVSECOPS GOALS:

## OPS

### VISIBILITY

- Who is attacking? What attack vectors?
- What applications and vulnerabilities are they targeting?

### PROTECT

- Must not overblock (FP) or underblock (FN)
- No tailoring or “learn mode”

### CONTROL

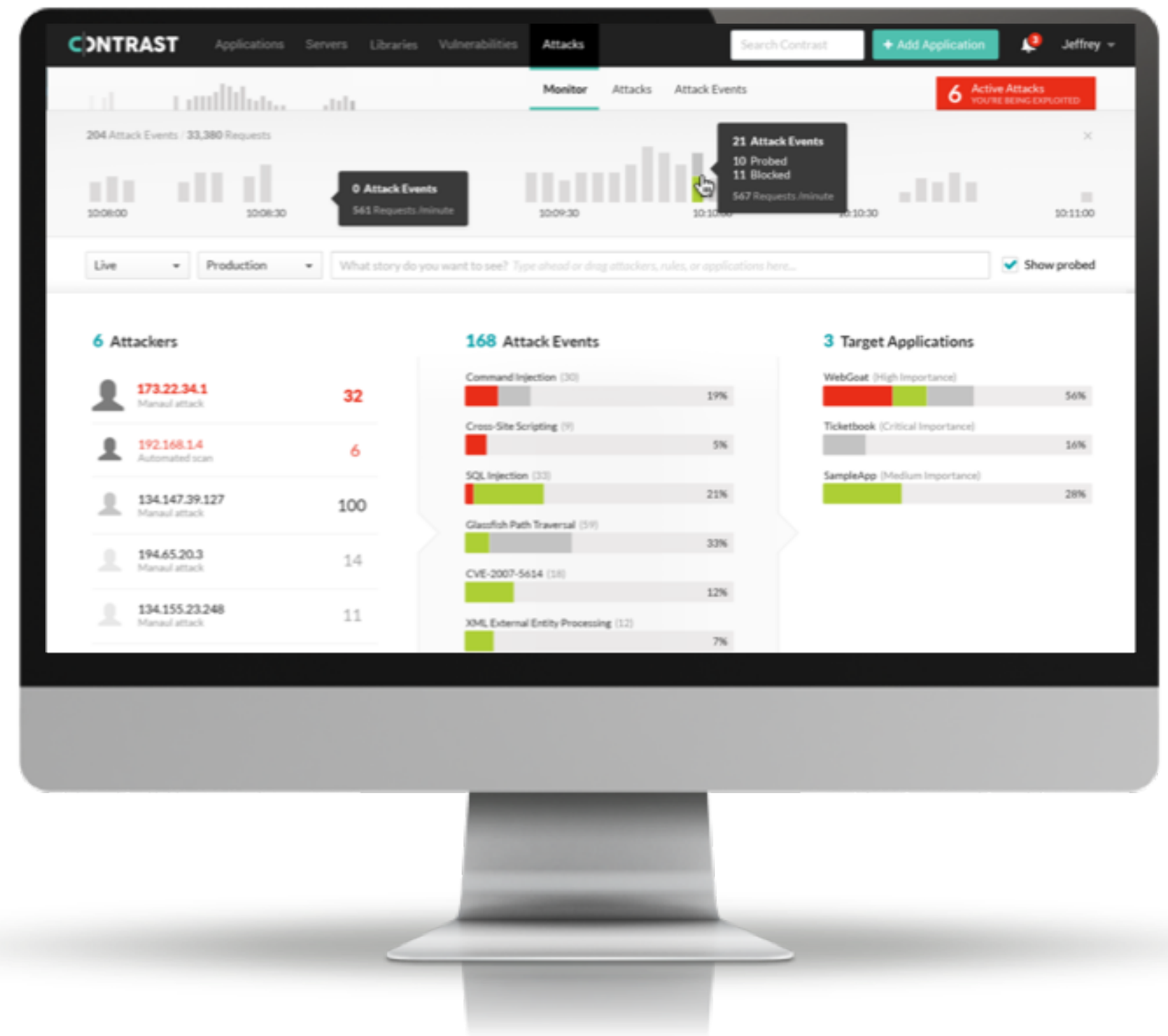
- Change rules centrally, enforce from within apps
- Automatic updates

# RASP PROTECTS FROM WITHIN

WHO IS ATTACKING?

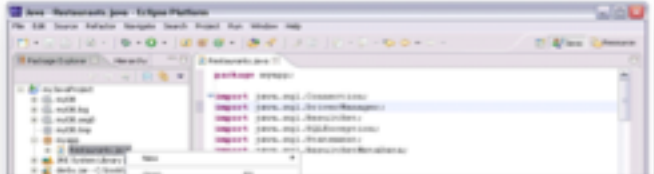
WHAT TECHNIQUES ARE THEY USING?

WHICH APPS AND APIS ARE THEY TARGETING?



# RASP IS ACCURATE

**BAD GUY**



AcmeInternalType#cmd:  
java.lang.Runtime

AcmeInternalType#mtd:  
getRuntime().exec

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

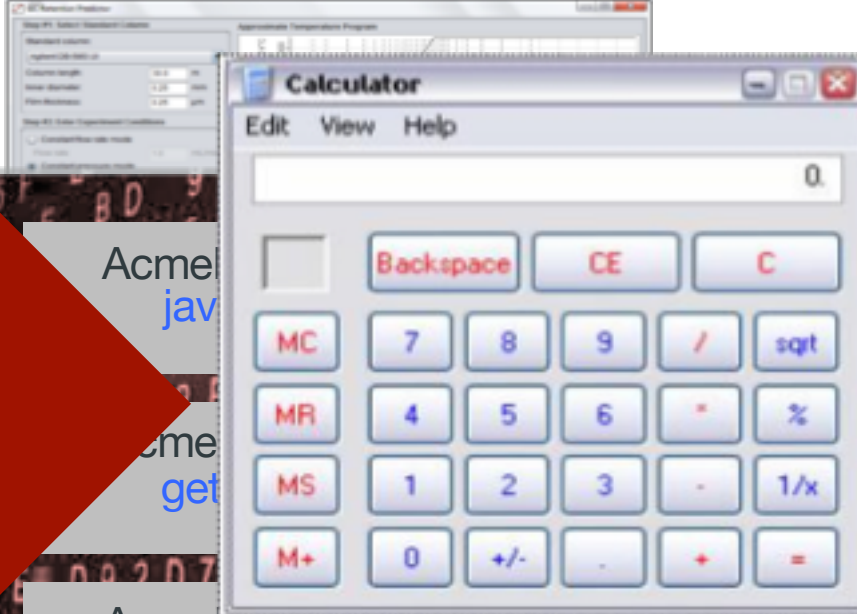
**UNTRUSTED DESERIALIZATION**

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
```

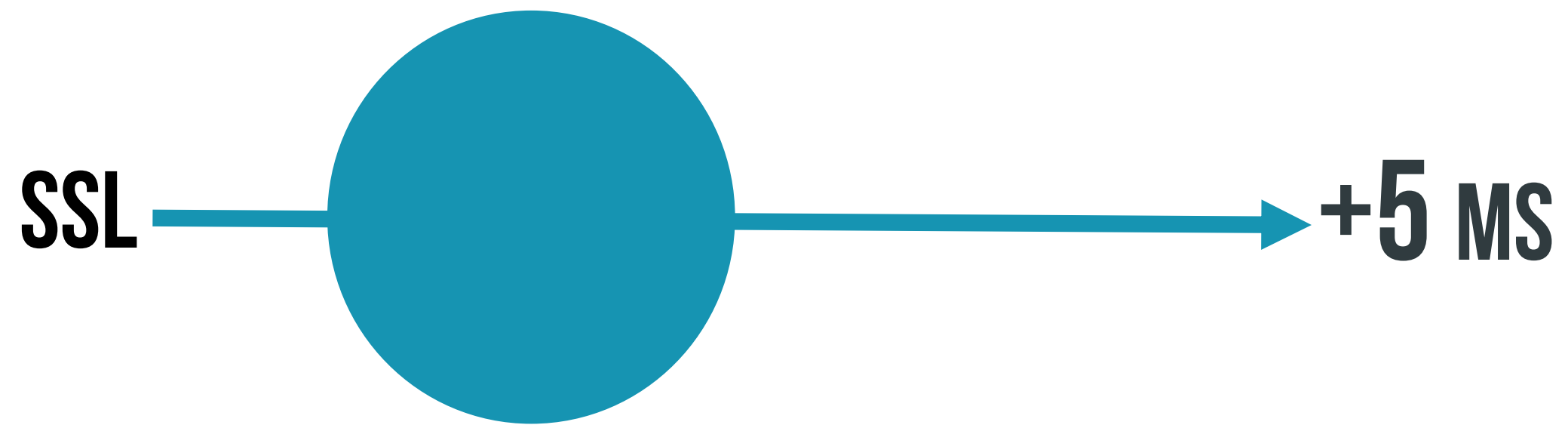
```
r00ABX0fyADJzdW4ucmVmbGVjdc5hbm5vdGF0aW9uLkFubm90YXRpb25JbnZvY2FOaW9uSGFuZ
Gxlc1lK9Q8Vy36iAgACTAAMBWVtYmVmfmdVVzdAAPTGphdmEvdXRpbC5NYXA7TAAEdHlwZX
QAEUxqYXZlL2xhbmcvQ2xhc3N7eHBzfQAAAAEADVphdmEudXRpbC5NYXB4cgAXamF2YS50eX
V5
```

**APPLICATION**



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

# RASP IS FAST



**CONTRAST  
PROTECT**



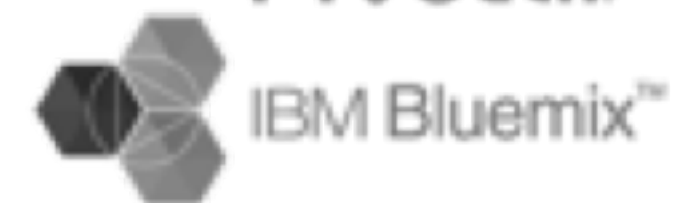
**100X FASTER THAN SSL**

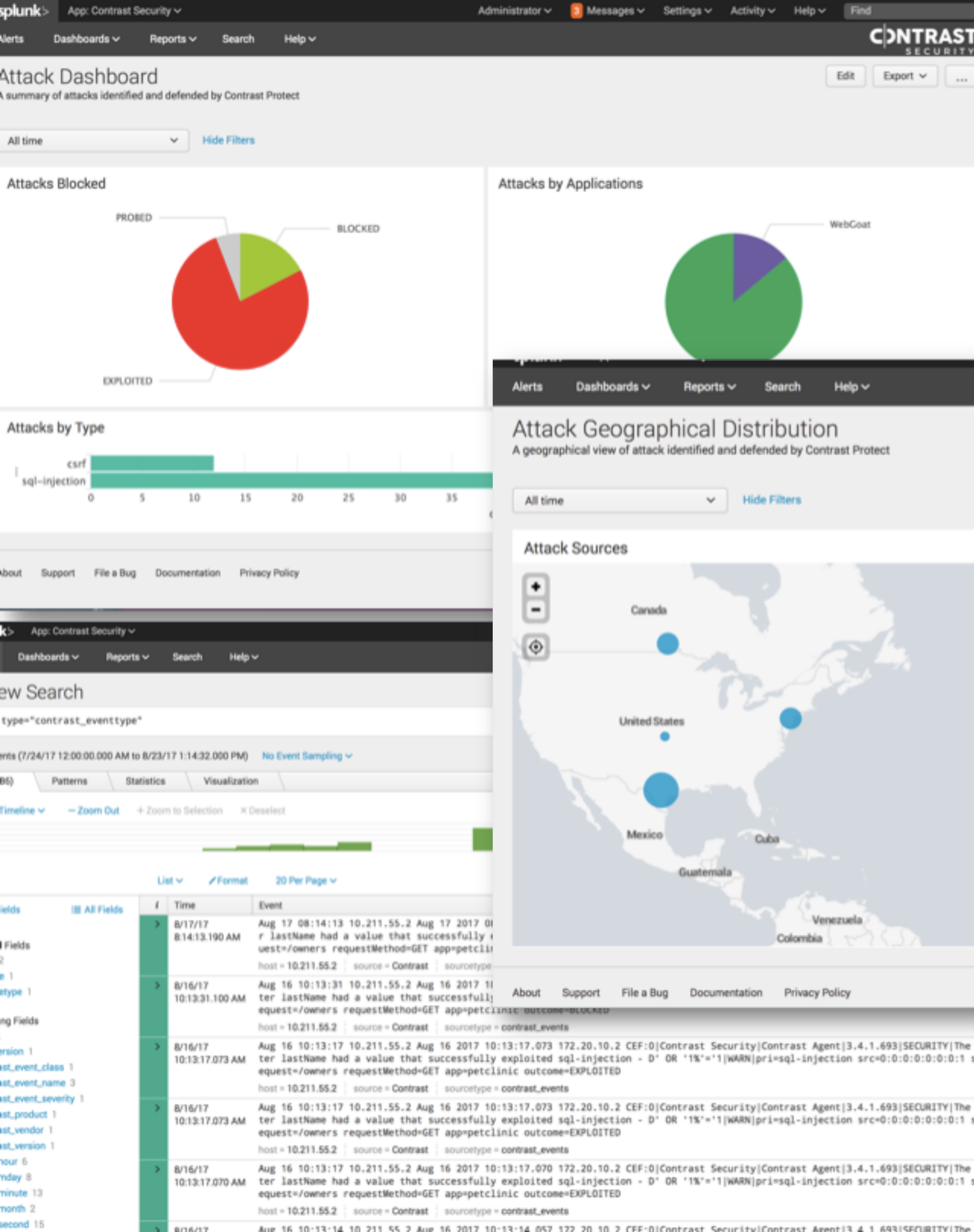
# **RASP** DEPLOYS AUTOMATICALLY WITH YOUR APPLICATION

- **ANSIBLE**
- **PUPPET**
- **DOCKER**
- **KUBERNETES**
- **WHATEVER...**



Pivotal.





# IS YOUR SOC **BLIND** TO APPSEC?





# YOU CAN START TODAY!



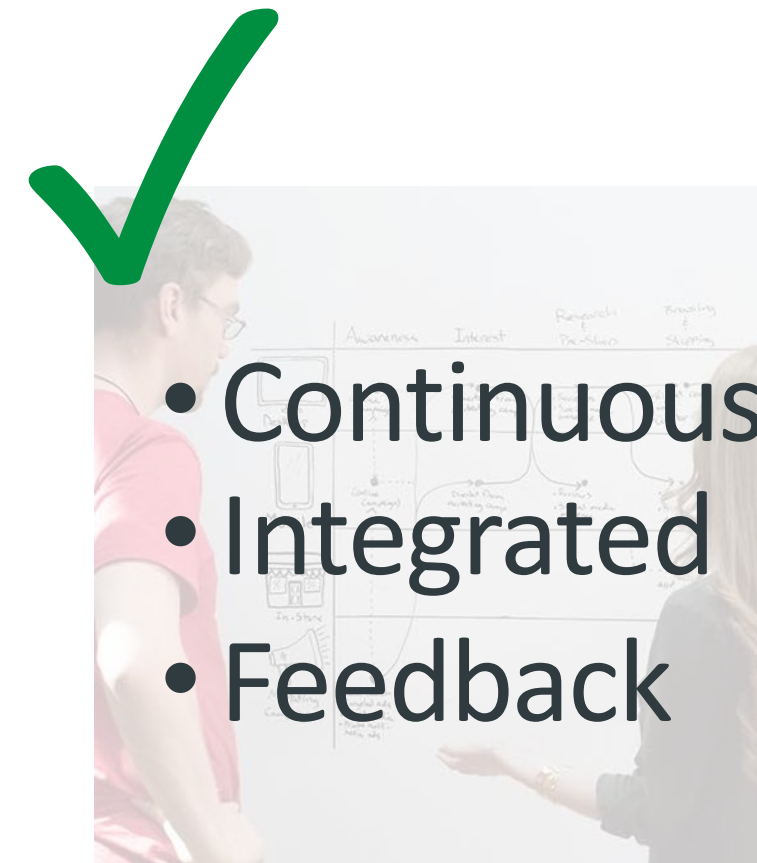
- Security
- Speed
- Scale

1. ADD SECURITY TO  
**DEVELOPMENT**



- Inventory
- Assess
- Protect

2. LOCK DOWN OPEN  
SOURCE **LIBRARIES**



- Continuous
- Integrated
- Feedback

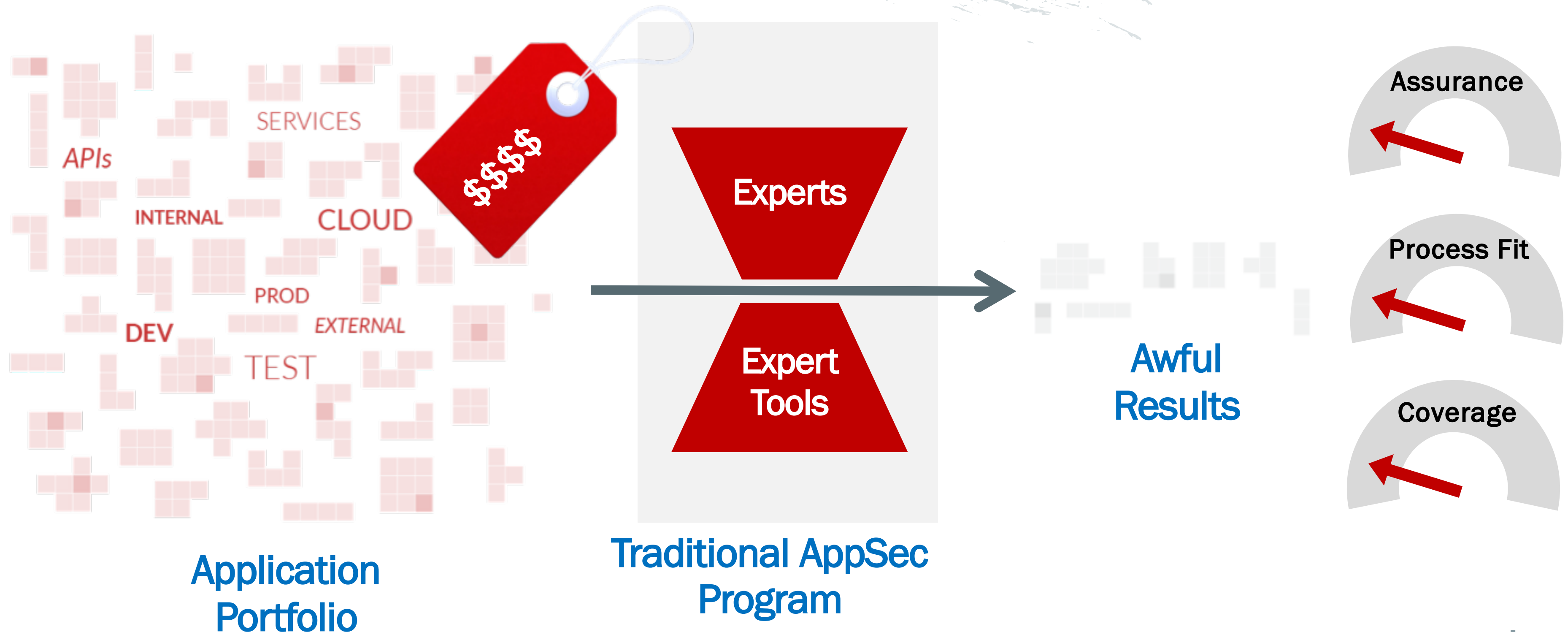
3. ENABLE AUTOMATIC  
SECURITY **TESTING**



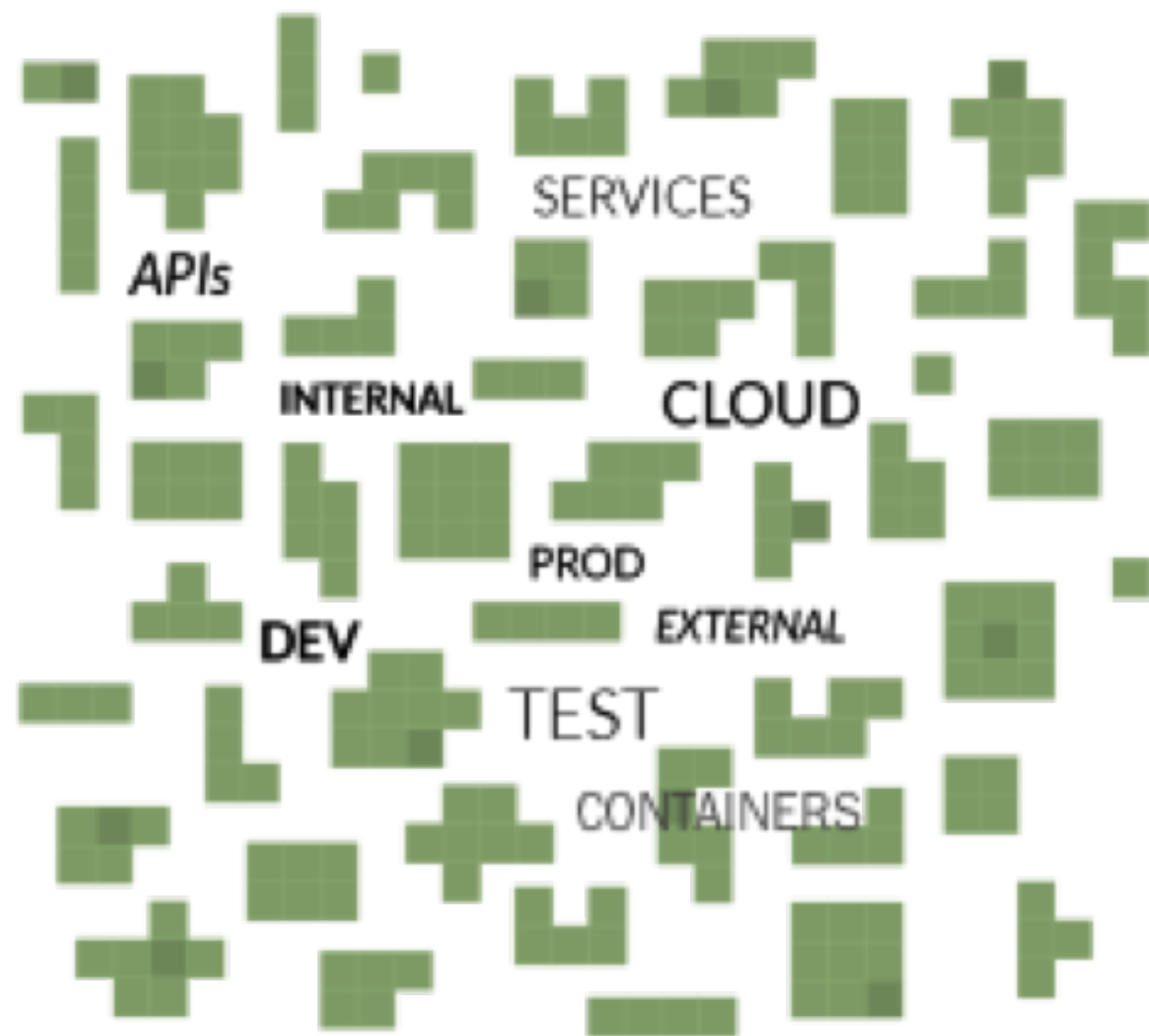
- **Visibility**
- **Protect**
- **Control**

4. PREVENT EXPLOITS  
**IN OPERATION**

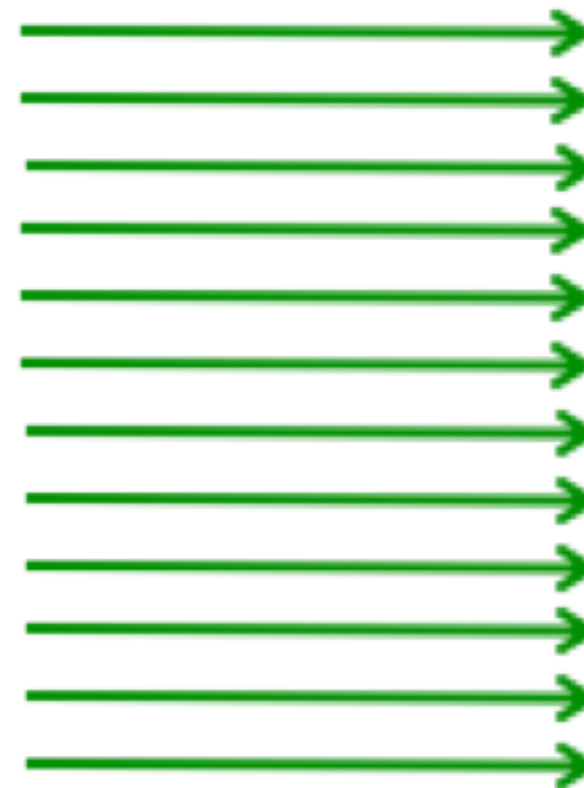
# SCANNERS AND FIREWALLS DON'T SCALE



# IAST/RASP – FULLY DISTRIBUTED APPROACH



Enable application portfolio  
with IAST/RASP agents



Continuous assessment  
and protection in parallel

# APPSEC EU EARLY ACCESS

## CONTRAST COMMUNITY EDITION — FREE

Contrast CE provides full-featured IAST and RASP for Java applications and APIs.



Finally, you can replace your SAST, DAST, SCA and WAF with something better...

Just some of the Contrast CE integrations...



<http://contrastsecurity.com/ce>



OWASP  
**AppSec Europe**  
London 2nd-6th June 2018

**THANK YOU!**  
ASK ME ANYTHING

Jumpstarting Your DevSecOps Pipeline with IAST and RASP

Jeff Williams @planetlevel

