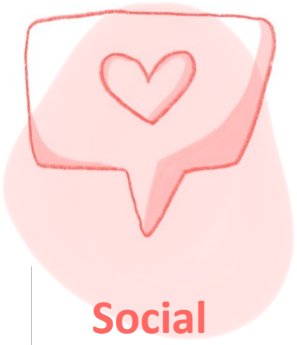
Using IAST to Unlock the Benefits of DevSecOps

Jeff Williams, Founder and CTO
Contrast Security
@planetlevel
November 2022

YOW! LONDON

Contrast SECURITY

We all blindly trust software with the most important things in life



Social

Elections

Business

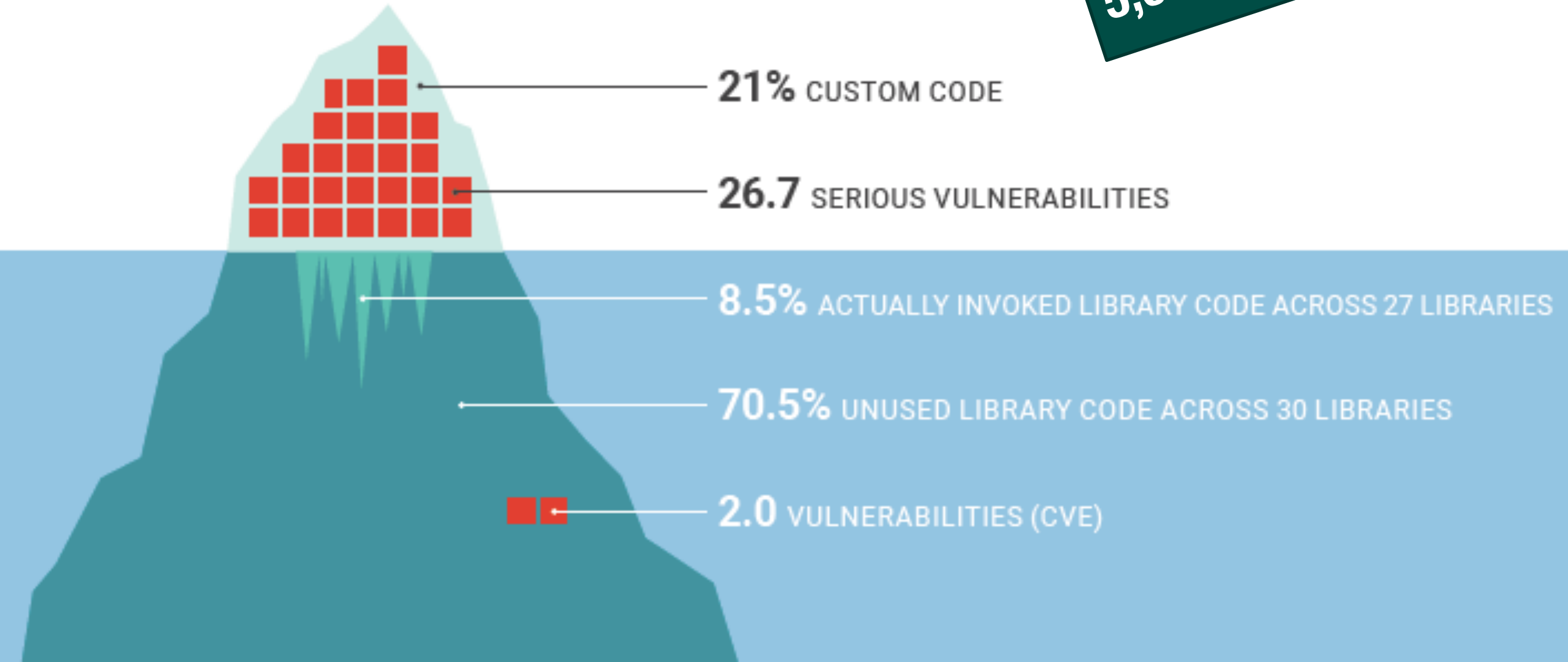
Power Grid

Money

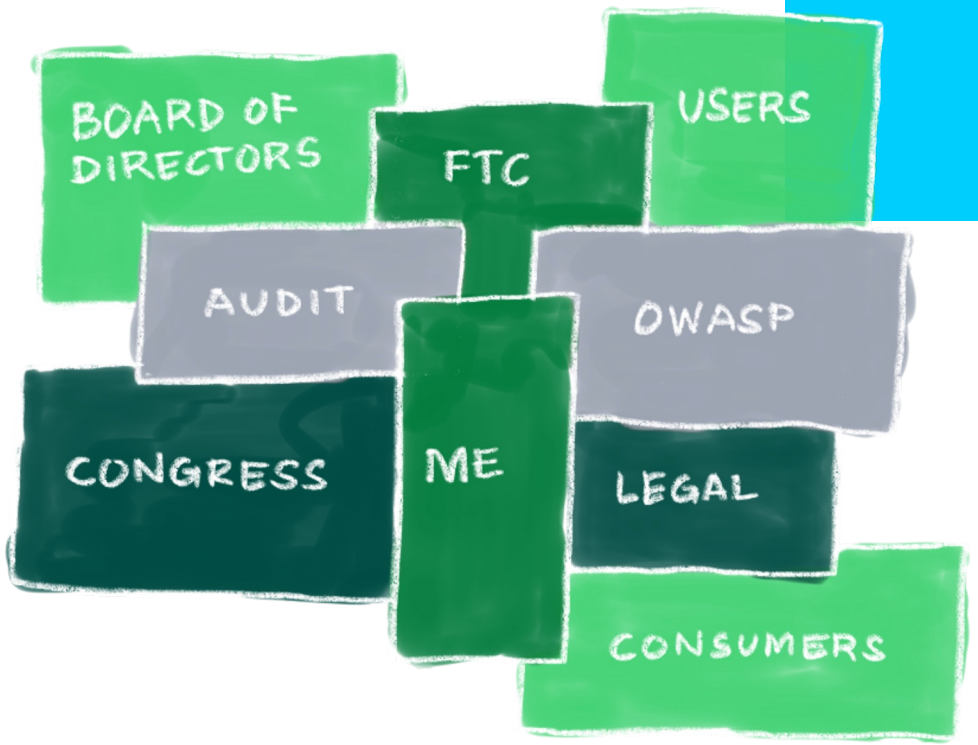
Government

The Average Application Has Serious Security Issues

5,000+ ATTACKS PER MONTH



Public expectations don't match reality



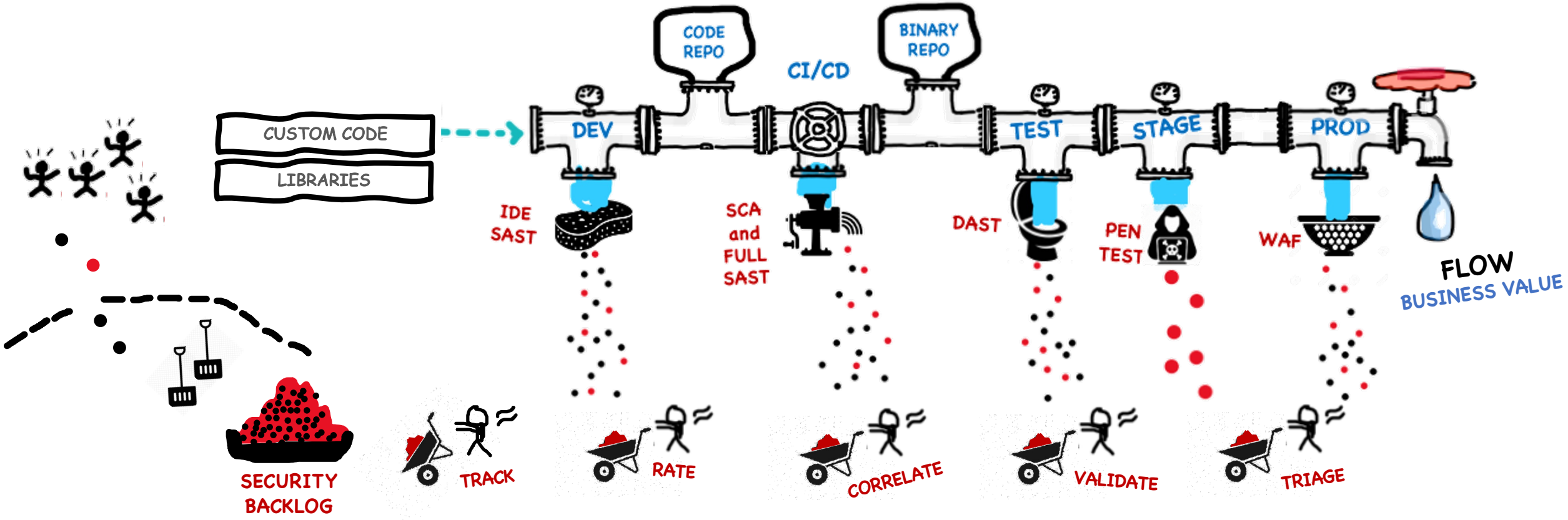

SECURITY
TRANSPARENCY
IS COMING

DevSecOps Will Fix Everything! /s

- **Problem**: **software** was poor quality, late, slow, and doesn't provide business value.
- **Approach**: DevOps
- **Results**:
  - 200x more deploys
  - 24x faster service recovery
  - 3x less change failures
  - 22% less unplanned work

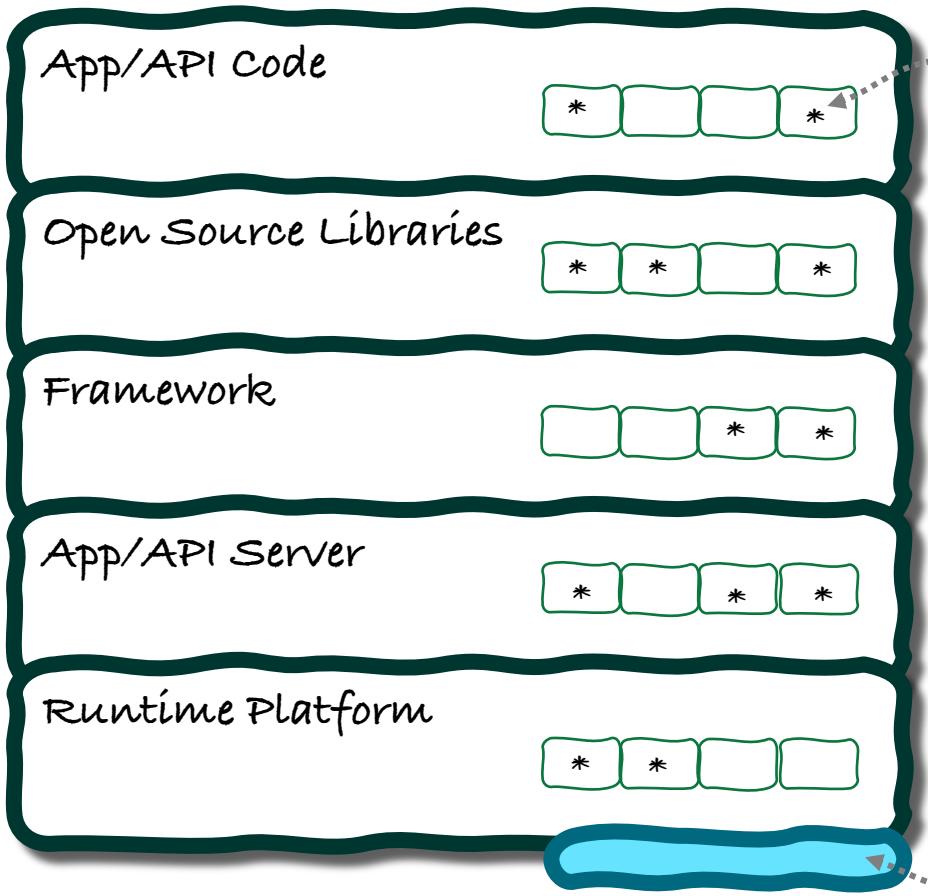
- **Problem**: **security** is poor quality, late, slow, and doesn't provide business value.
- **Approach**: DevSecOps
- **Results**?
  - 10x faster security results?
  - 80% less vulnerabilities in prod?
  - 0x increase in time to market?
  - No log4j-style firedrills?

So Why Does DevSecOps Feel Awful?



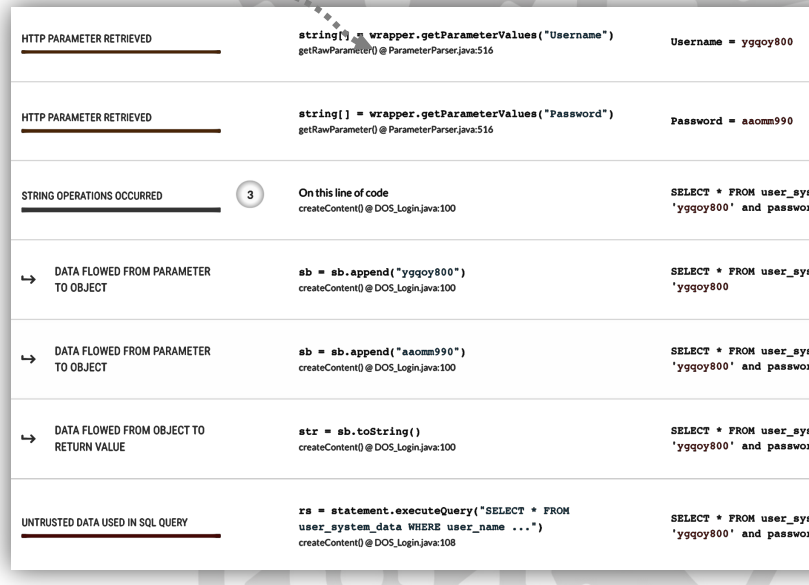
INSTRUMENTATION CHANGES EVERYTHING

Security Instrumentation!



Sensors

Vulnerability Trace



Install Runtime Security module and perform normal QA

Full App/API Workload

Example: Detecting SQL Injection

No escaping or parameterization!

```
String name=request.getParameter("Username");
String pass=request.getParameter("Password");
String query="select * from user_system_data   \
      where user='" + name + "' and user='" + pass + "'";
Statement statement = connection.createStatement(...);
ResultSet results = statement.executeQuery( query );
```

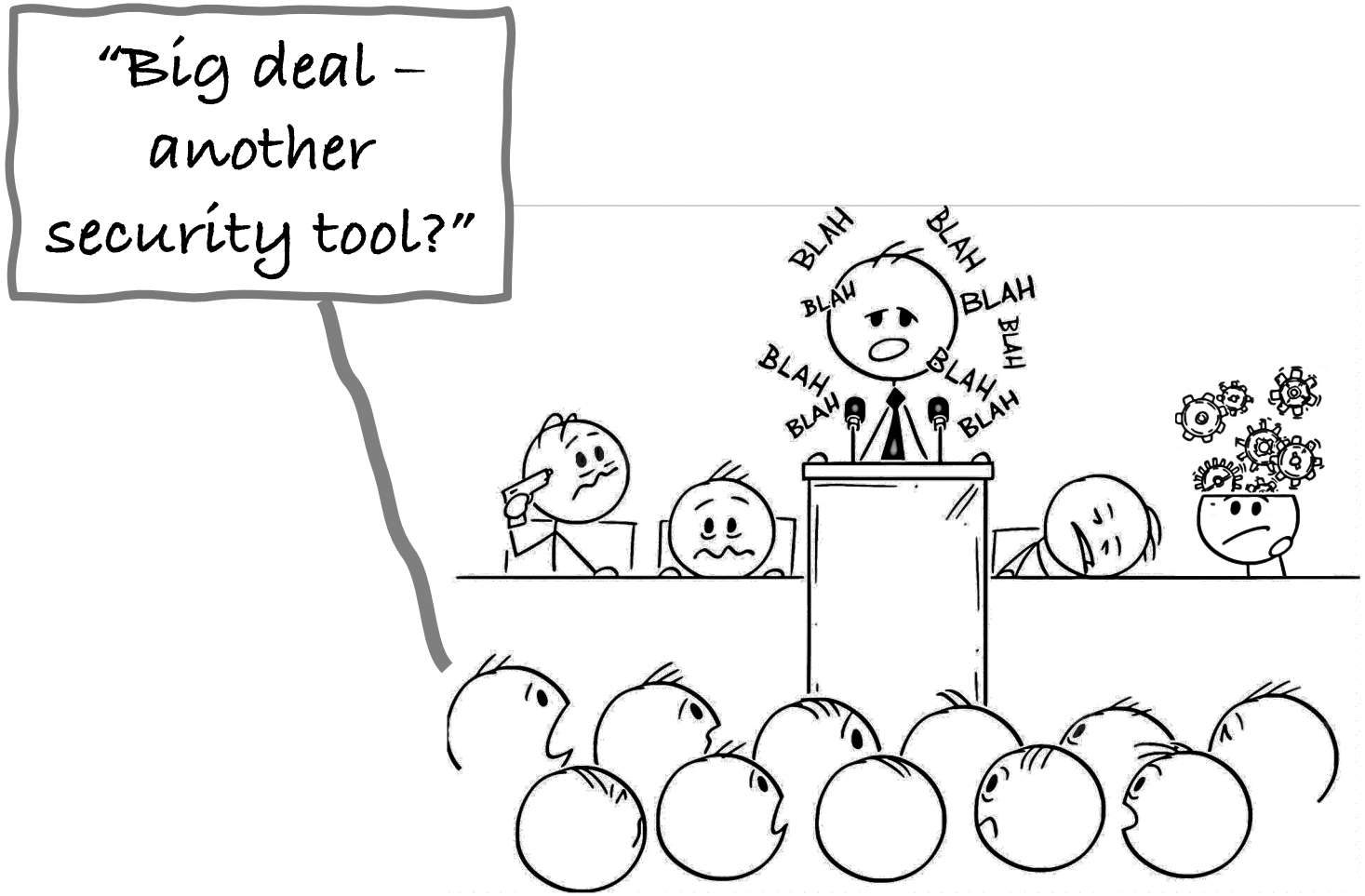
?name=ygqoy800 &
pass=aaomm990

select * from users where
user='ygqoy800' and pass='aaomm990!'

Contrast SECURITY

HTTP PARAMETER RETRIEVED		`string[] = wrapper.getParameterValues("Username")` getRawParameter() @ ParameterParser.java:516	`Username = ygqoy800`
HTTP PARAMETER RETRIEVED		`string[] = wrapper.getParameterValues("Password"` getRawParameter() @ ParameterParser.java:516	`Password = aaomm90`
STRING OPERATIONS OCCURRED	3	On this line of code createContent() @ DOS_Login.java:100	`SELECT * FROM user_system_data WHERE user_name = 'ygqoy800' and password = 'aaomm990'`
↪ DATA FLOWED FROM PARAMETER TO OBJECT		`sb = sb.append("ygqoy800")` createContent() @ DOS_Login.java:100	`SELECT * FROM user_system_data WHERE user_name = 'ygqoy800`
↪ DATA FLOWED FROM PARAMETER TO OBJECT		`sb = sb.append("aaomm990")` createContent() @ DOS_Login.java:100	`SELECT * FROM user_system_data WHERE user_name = 'ygqoy800' and password = 'aaomm990`
↪ DATA FLOWED FROM OBJECT TO RETURN VALUE		`str = sb.toString()` createContent() @ DOS_Login.java:100	`SELECT * FROM user_system_data WHERE user_name = 'ygqoy800' and password = 'aaomm990'`
UNTRUSTED DATA USED IN SQL QUERY		`rs = statement.executeQuery("SELECT * FROM user_system_data WHERE user_name ...")` createContent() @ DOS_Login.java:108	`SELECT * FROM user_system_data WHERE user_name = 'ygqoy800' and password = 'aaomm990'`

Security trace – data flow events

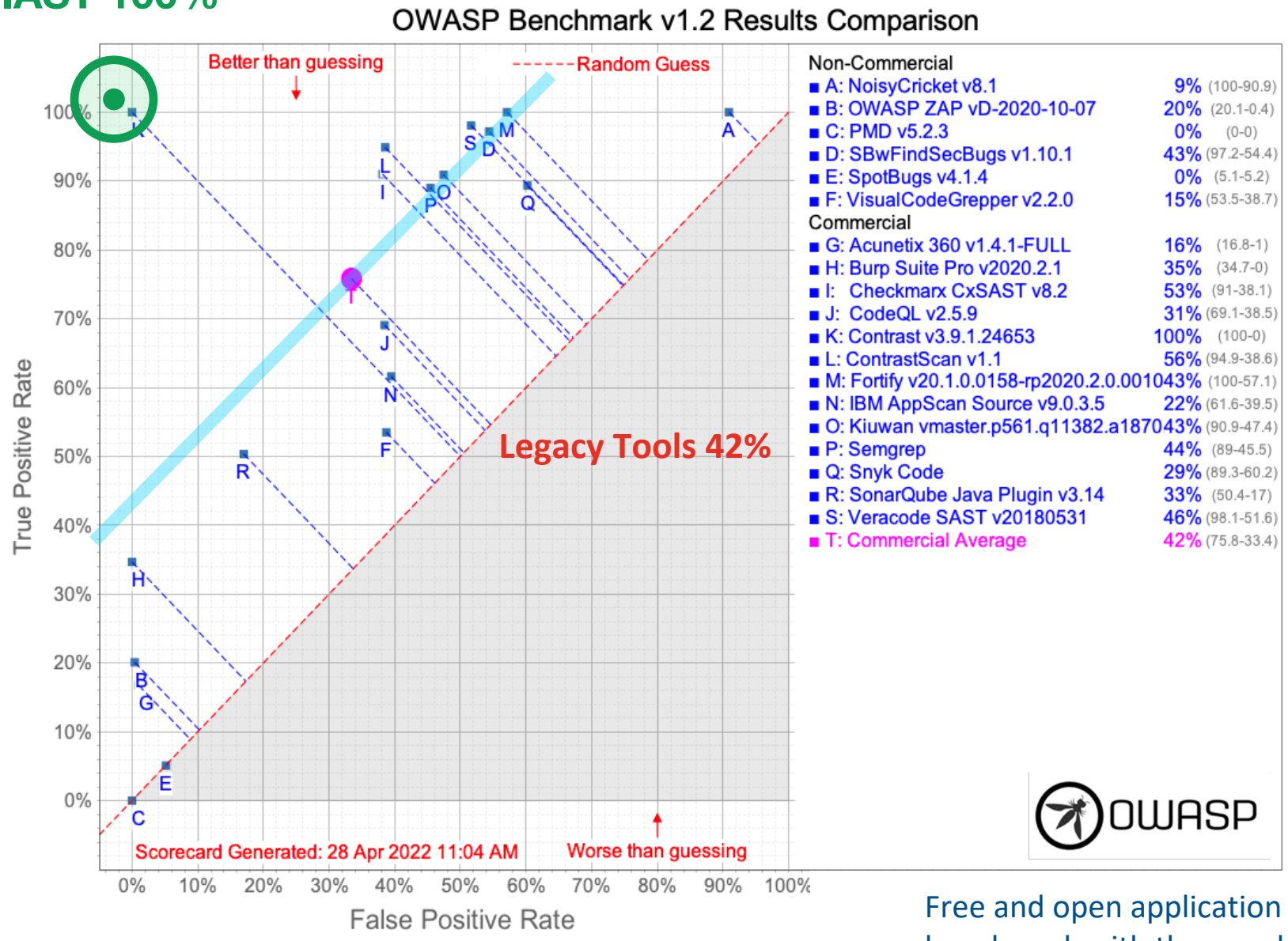


With IAST…

ANYONE can get instant, detailed, and accurate security feedback on their projects without ANY extra work.

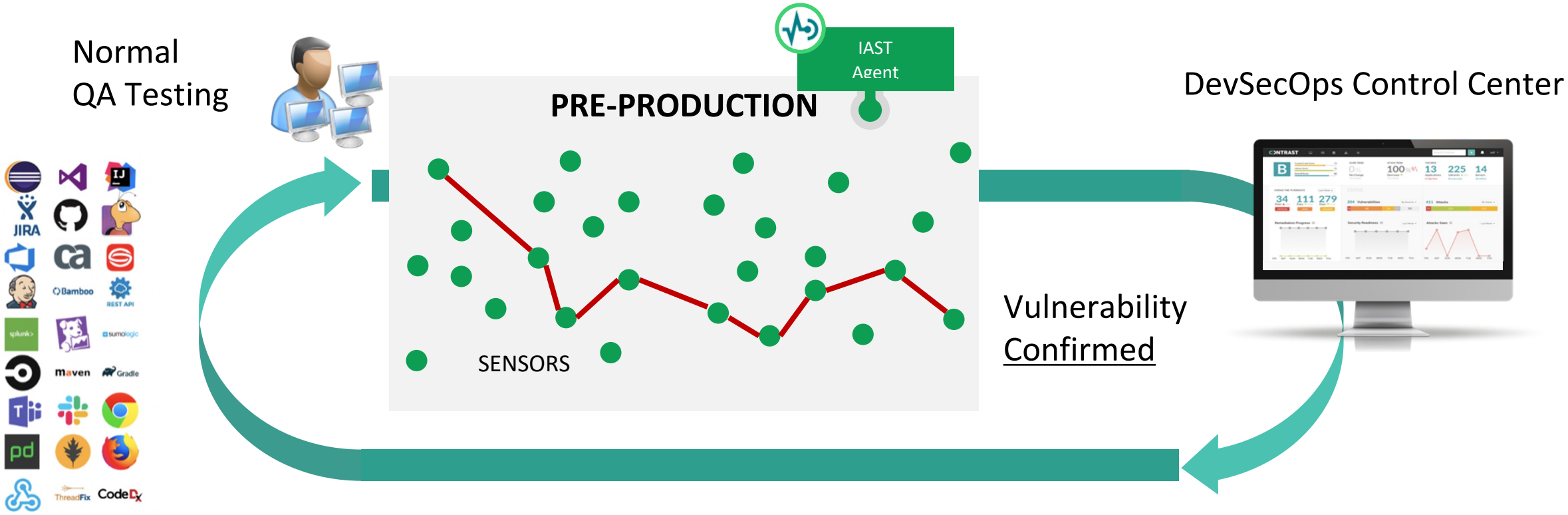
Accuracy is the most developer-friendly feature in a security tool

IAST 100%



Free and open application benchmark with thousands of security test cases

Interactive Application Security Testing (IAST)
-- using instrumentation to detect vulnerabilities during normal QA



Runtime vulnerability snapshots

What happened?

We tracked the following data from "lastName" Parameter:

```
GET /owners?lastName=Yow%21+LONDON

lastName=Yow! LONDON
```

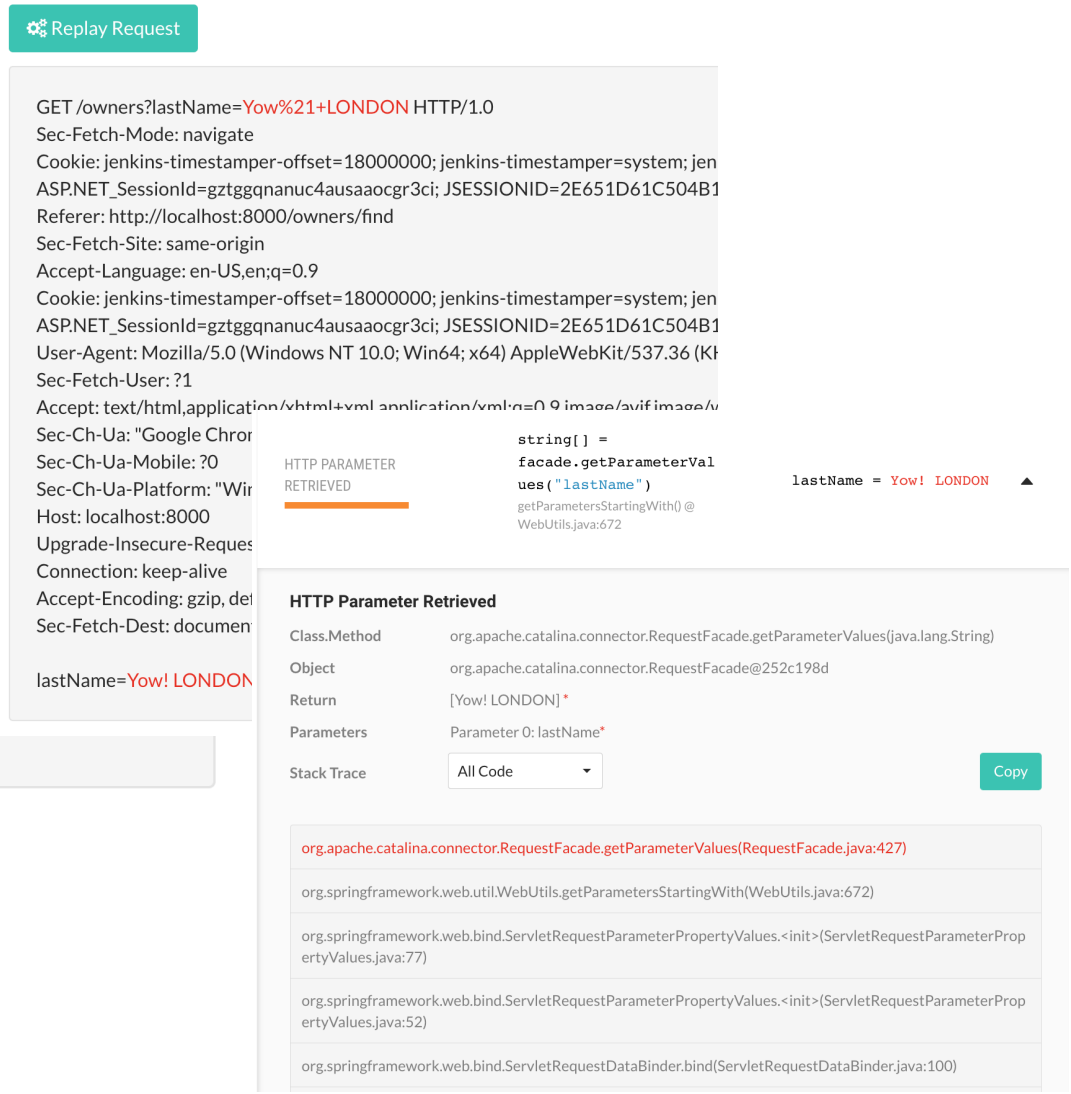
...which was accessed within the following code:

```
org.hibernate.jpa.spi.AbstractEntityManagerImpl#createQuery(), line 305
```

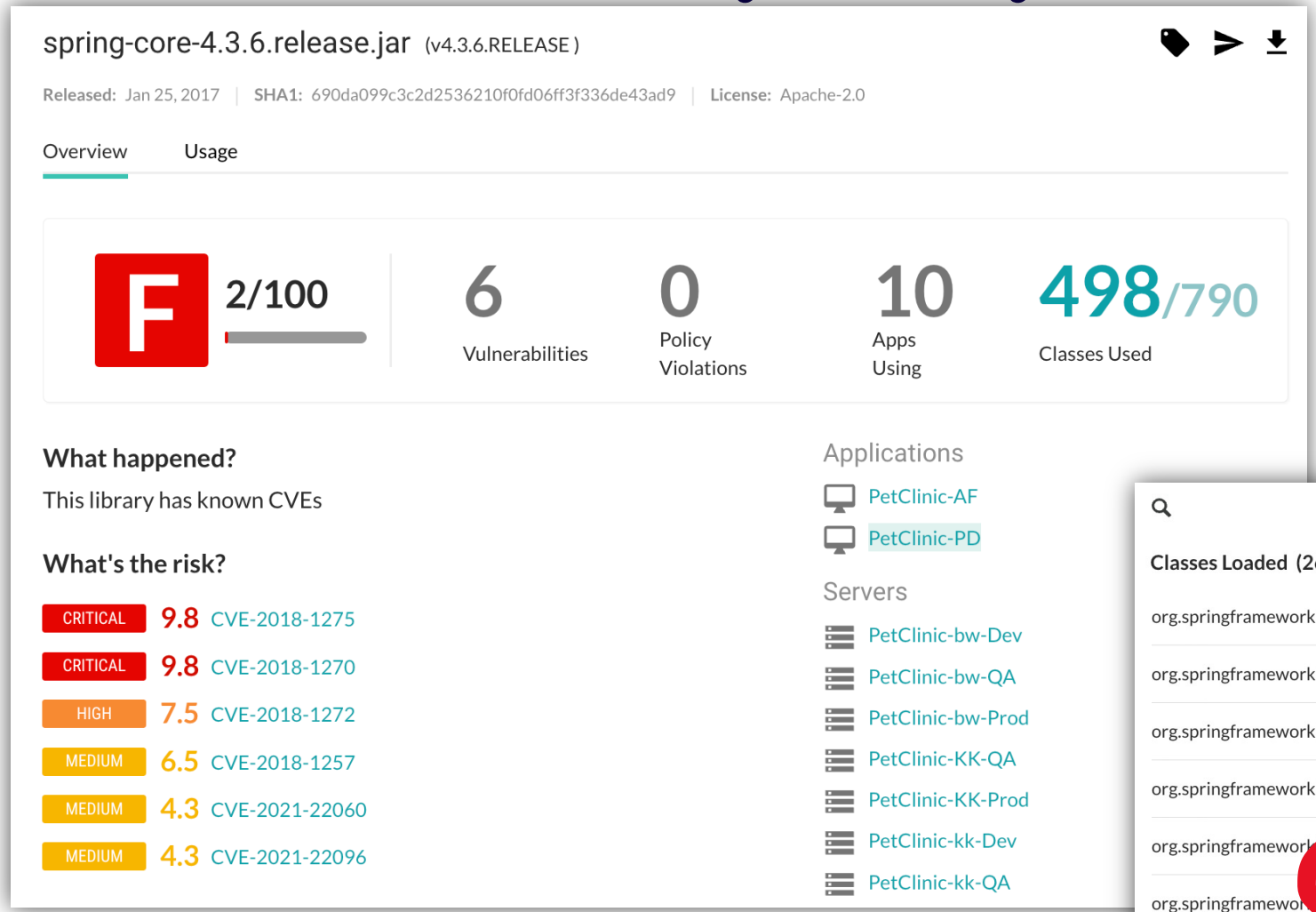
...and ended up in this database query:

```
SELECT DISTINCT owner FROM Owner owner left join fetch owner.pets WHERE owner.la
'Yow! LONDON%'
```

HTTP view, Code view,
and Data view – FULL CONTEXT



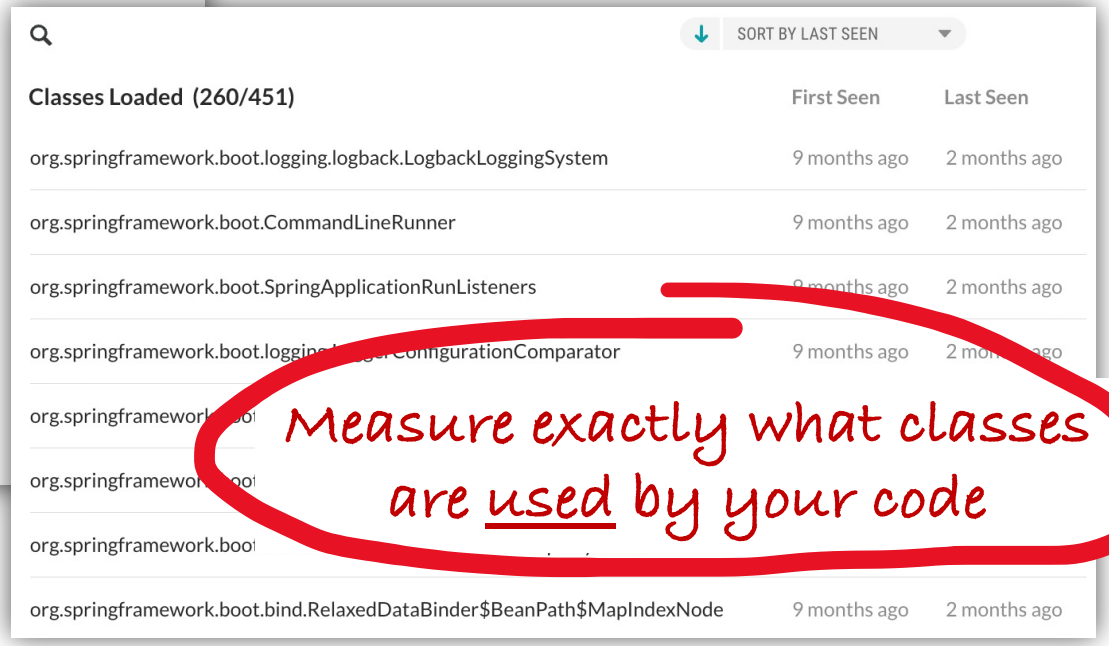
Runtime library analysis



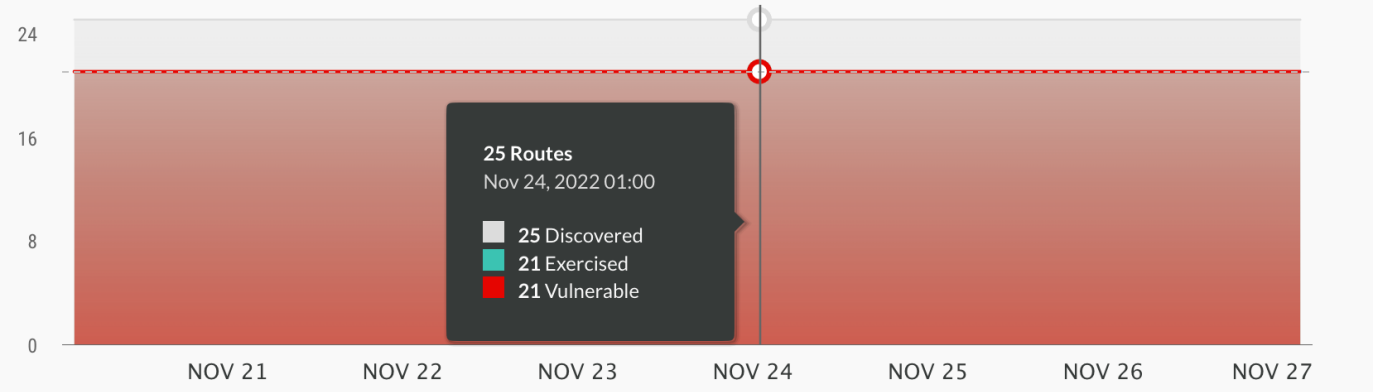
Find both known and unknown vulnerabilities in libraries

AST and SCA are one thing

... and should always be performed by one tool



Runtime route coverage



Route	Environment	Server	Vulnerabilities	Application	Last Activity
org.sprin...	Development QA	PetClinic-JW... PetClinic-JW...	3	PetClinic-JW	1 hour ago
org.sprin...	Development QA	PetClinic-JW... PetClinic-JW...	5 1	PetClinic-JW	1 hour ago
org.sprin...	Development QA	PetClinic-JW... PetClinic-JW...	3	PetClinic-JW	3 days ago
org.sprin...	Development QA	PetClinic-JW... PetClinic-JW...	4	PetClinic-JW	3 days ago

Route URLs

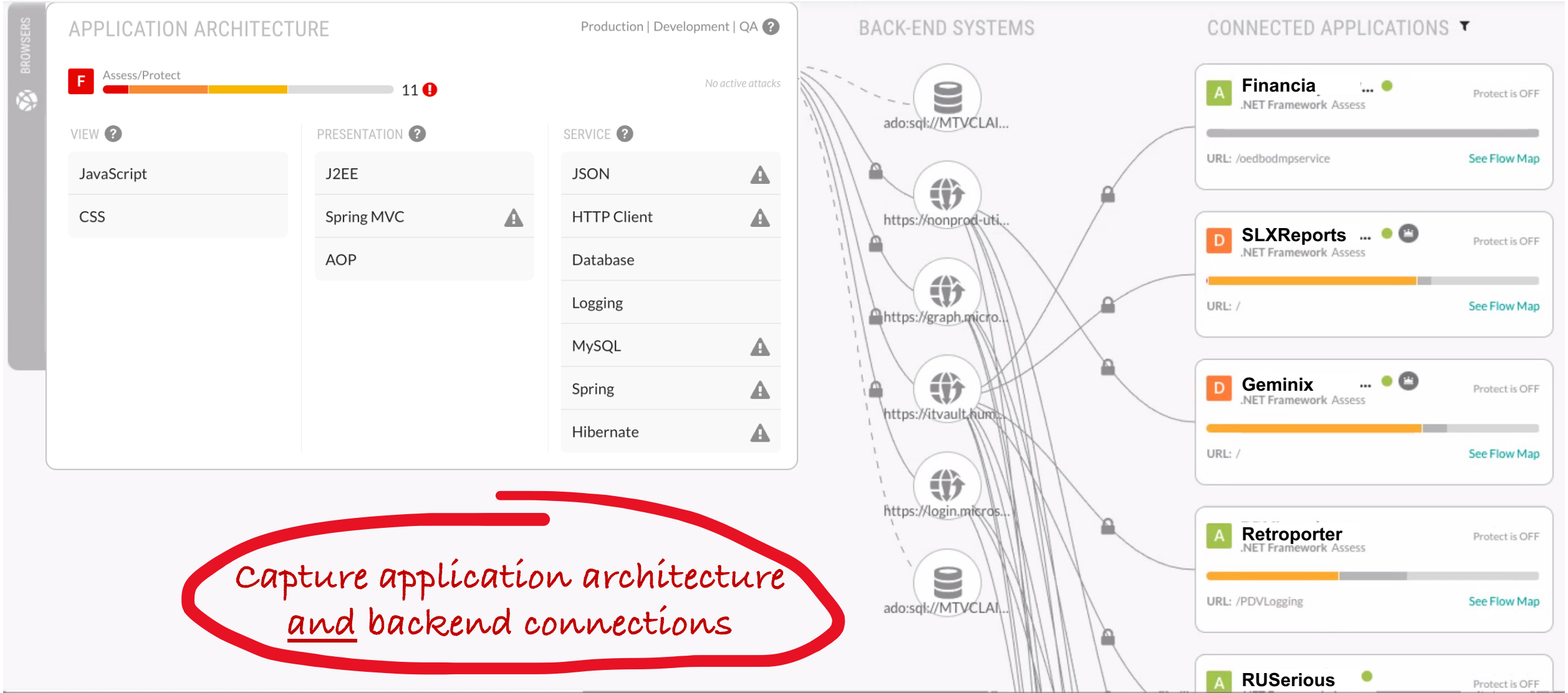
- POST /owners/new

Close

Ensure all exposed endpoints are security tested

Discover unknown routes from frameworks, plugins, old code, etc...

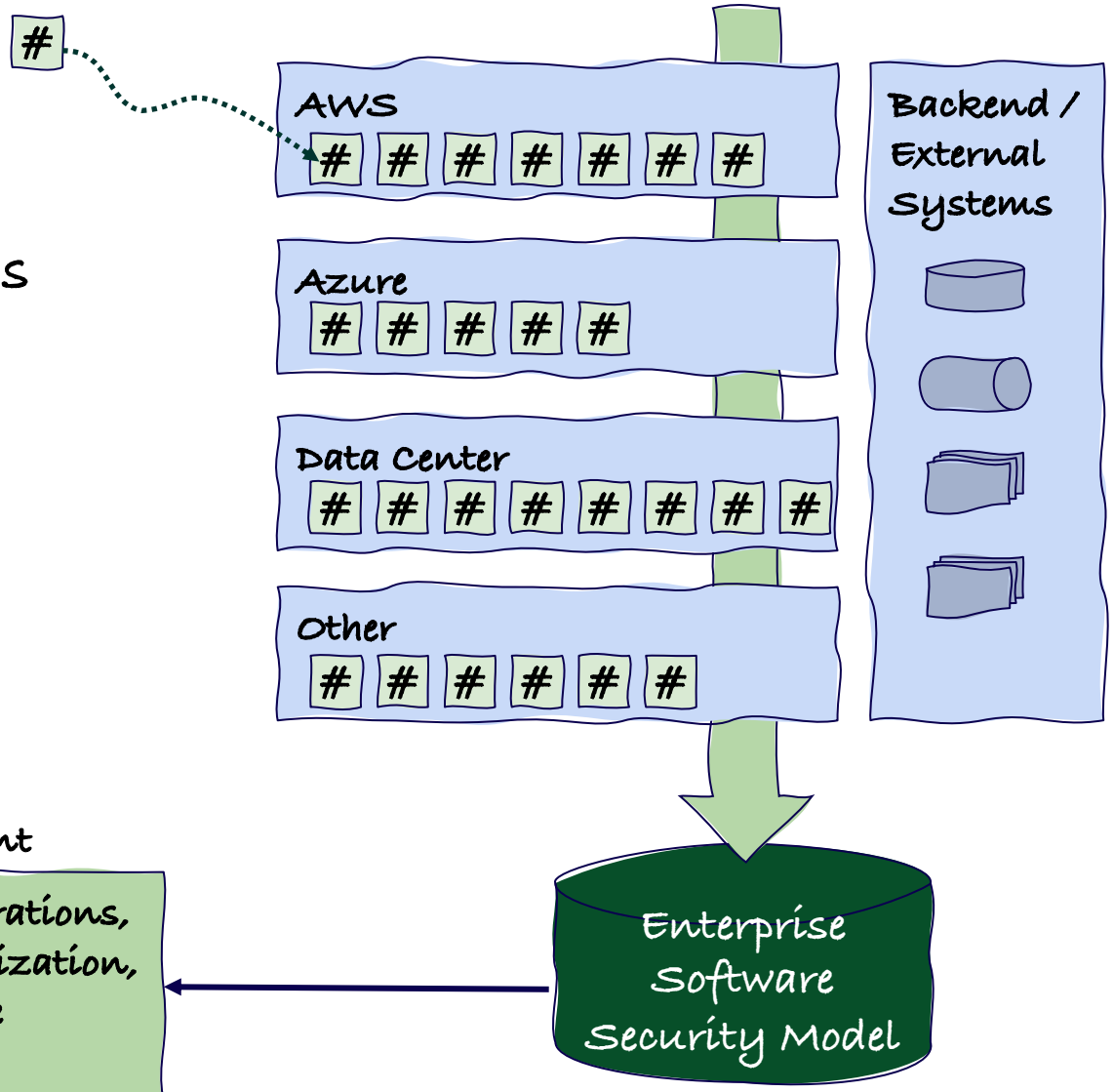
Runtime architecture diagrams



Capture application architecture and backend connections

Deploying IAST at Scale

Fully distributed. Analyze all your apps/APIs in parallel.

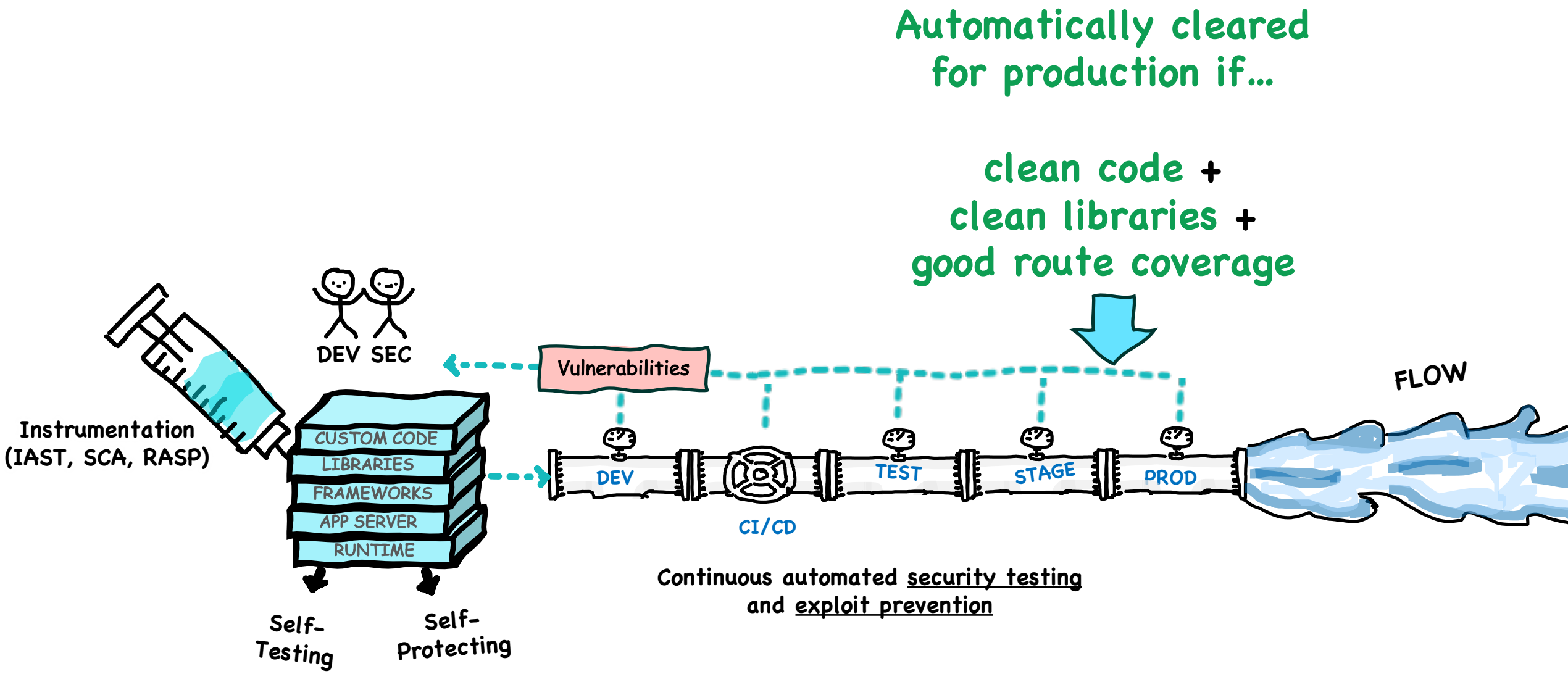


Deploy IAST automatically to all your servers via:

- Kubernetes operator
- Platform engineering
- Gold Server
- Container build
- Etc…

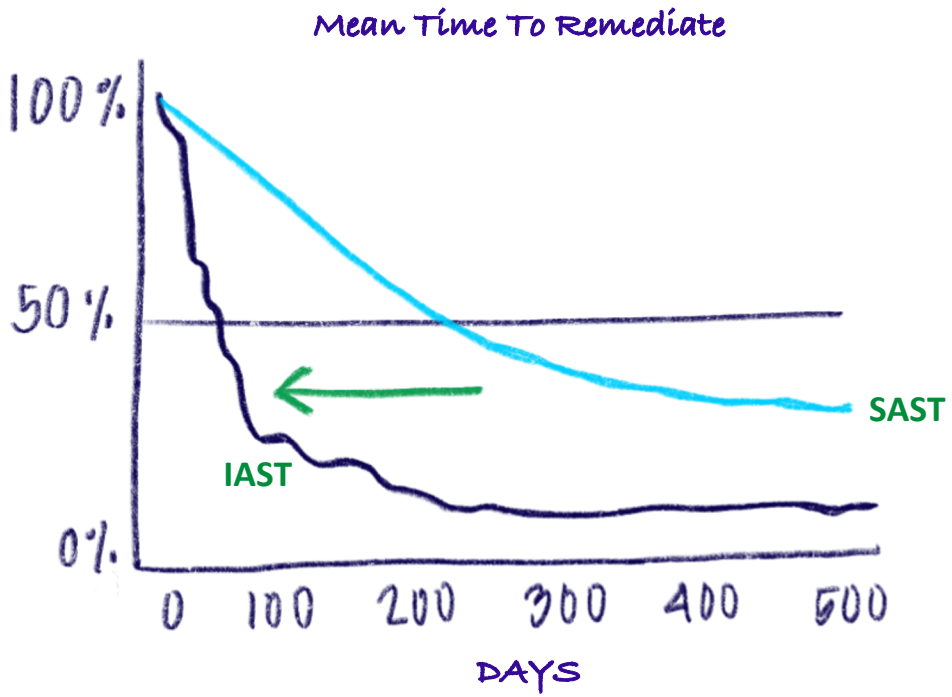
Contrast SECURITY

DevSecOps - Getting Secure Code Moving

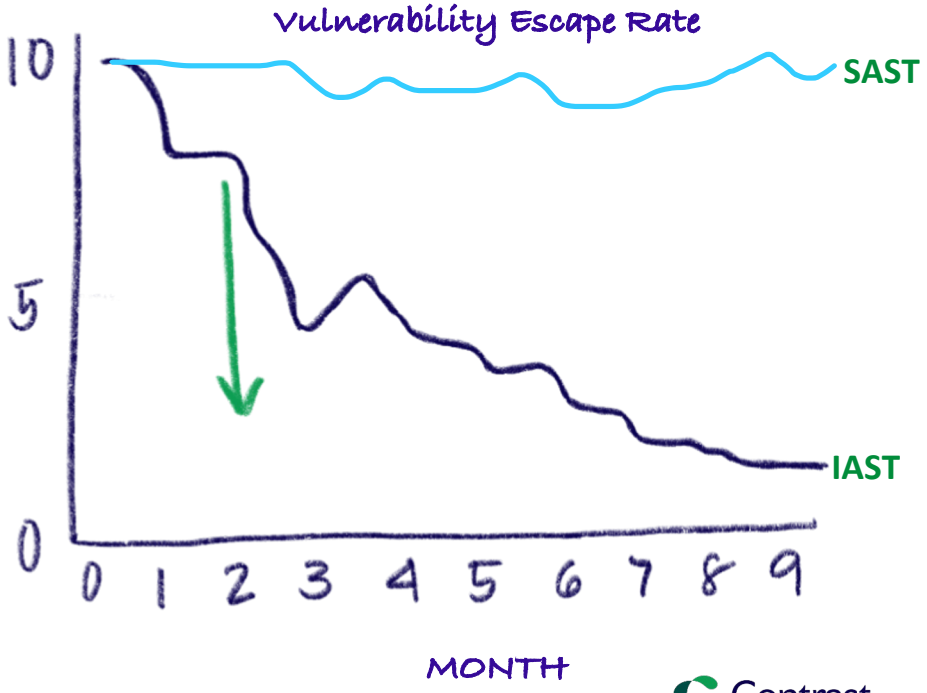


Metrics that matter

Reduce MTTR to < 1 week



Reduce VER to < 1 per month



Contrast SECURITY

Ask me ANYTHING!

Jeff Williams @planetlevel
Cofounder and CTO
Contrast Security

Contrast SECURITY

Follow us **@goto_con**
Share your experience using **#YOWlondon**

Follow us **@GOTOcon**
Share your experience using **#YOWlondon**

Follow us **GOTO Conferences**
Join **322k+ subscribers** & **36m+ views**

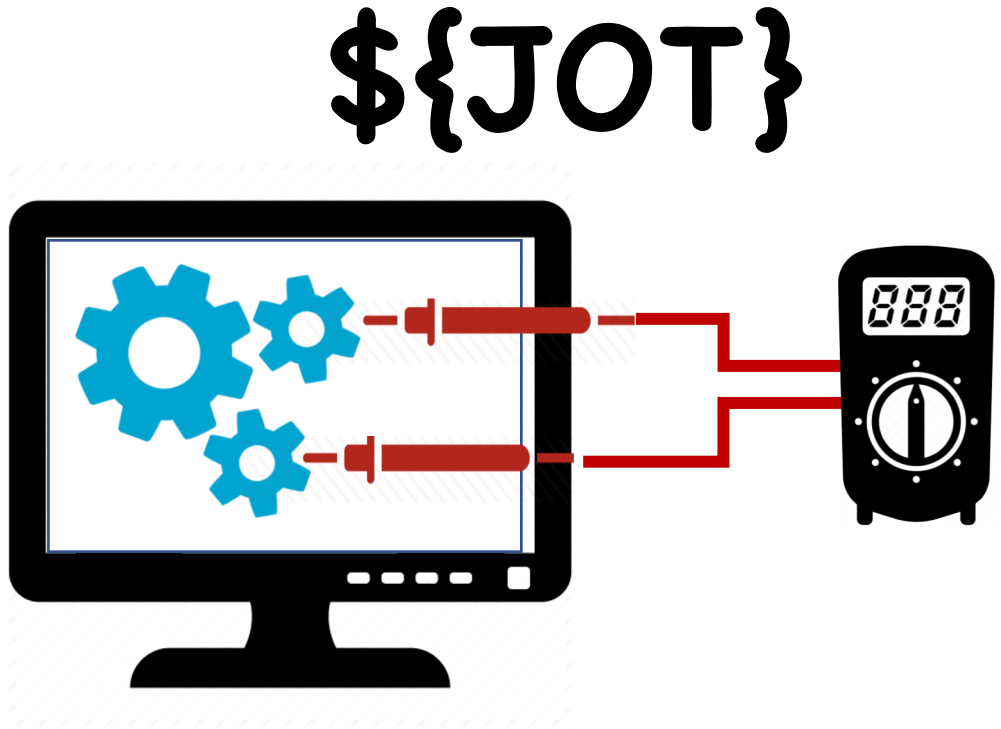
==========EXTRA==========

Try the Java Observability Toolkit (JOT)

Free and Open Source

Make your own runtime protection with a few lines of yaml

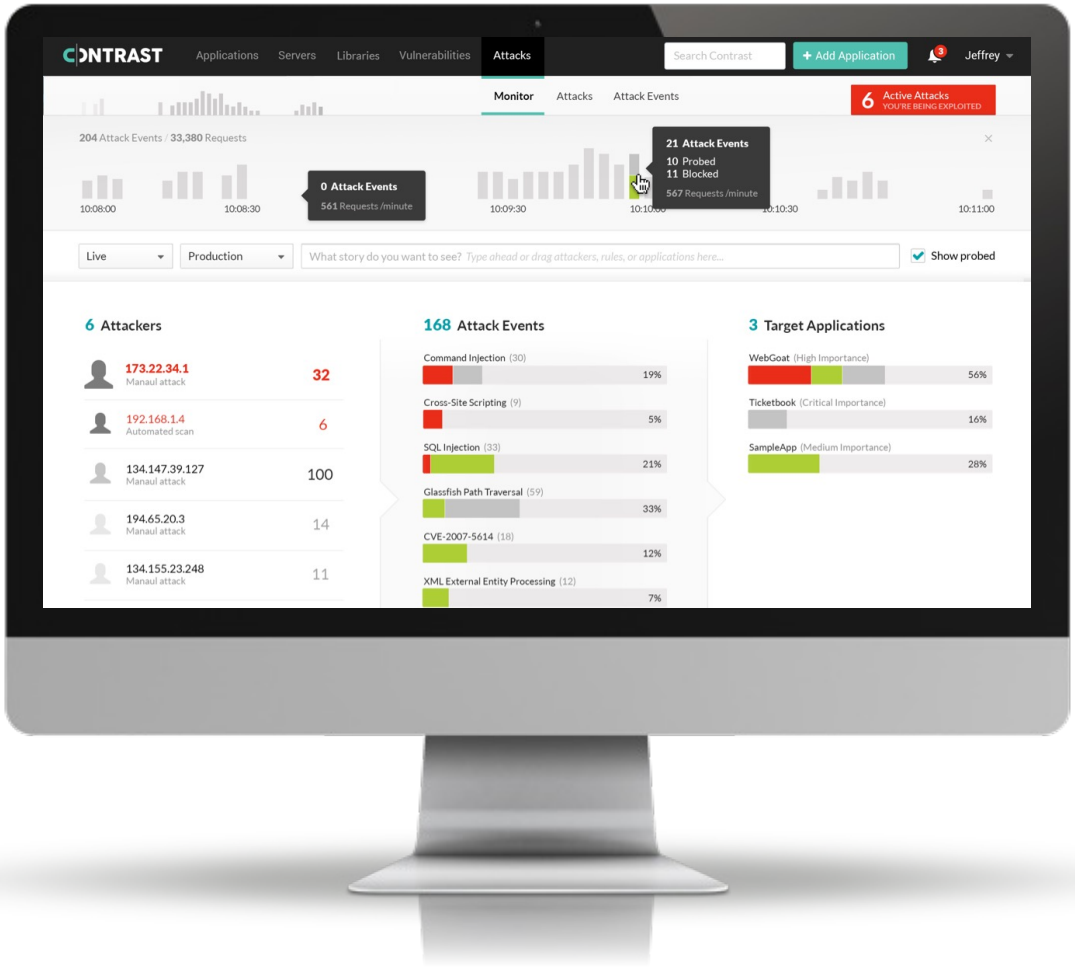
```
- name: "sandbox-expressions"
  description: "Prevents harmful methods from being used
  methods:
  - "java.lang.ProcessBuilder.<init>"
  - "java.io.Socket.<init>"
  scopes:
  - "javax.el.ValueExpression.getValue"
  captures:
  - "#P0"
  exception: "Attempt to escape expression language sandb
```

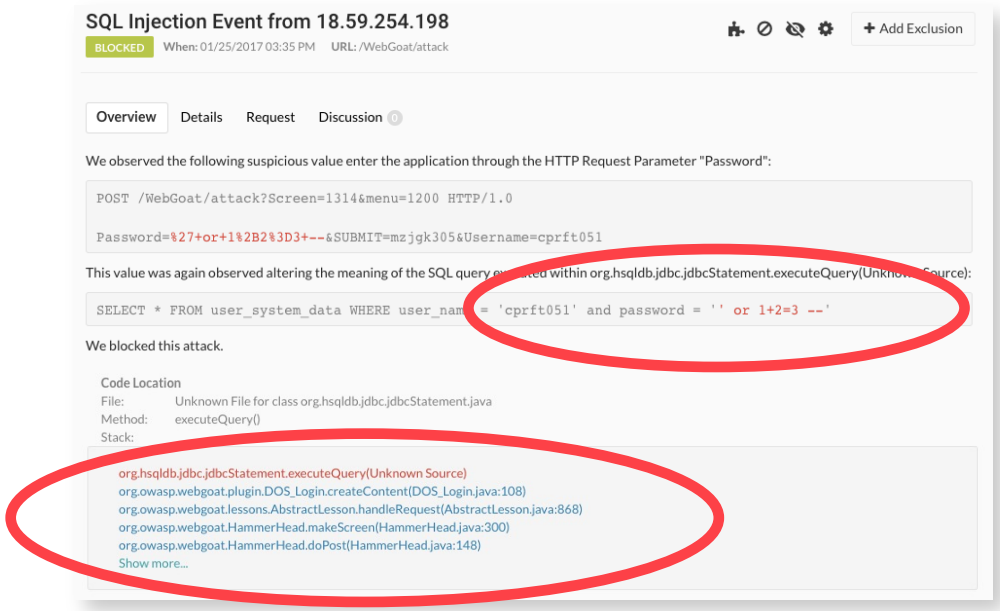


https://github.com/planetlevel/jot

Contrast SECURITY

Try it for free...





https://contrastsecurity.com/ce

Contrast SECURITY