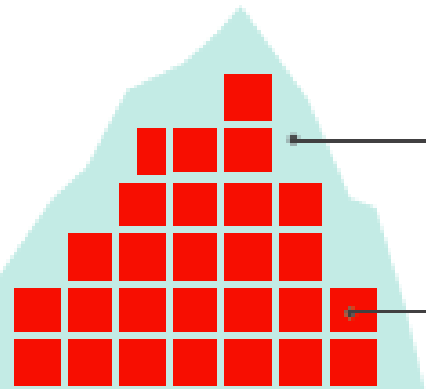


THE THREE WAYS OF SECURITY

Jeff Williams
Co-founder and CTO
Contrast Security



1. TODAY'S "AVERAGE" APPLICATION IS A SECURITY DISASTER



21% CUSTOM CODE

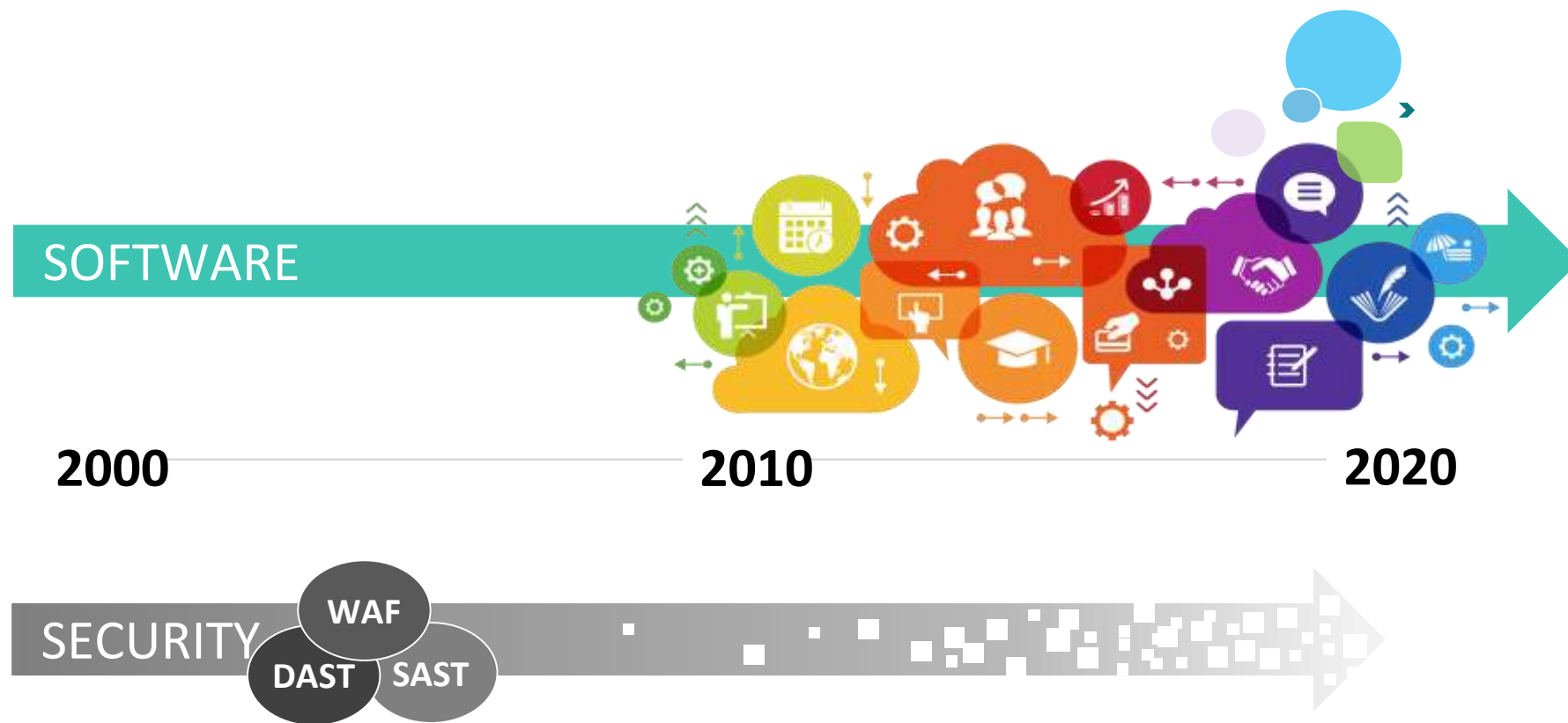
26.7 SERIOUS VULNERABILITIES

8.5% ACTUALLY INVOKED LIBRARY CODE ACROSS 27 LIBRARIES

70.5% UNUSED LIBRARY CODE ACROSS 30 LIBRARIES

2.0 VULNERABILITIES (CVE)

2. SOFTWARE IS LEAVING SECURITY IN THE DUST



- Typical enterprise has hundreds or thousands of applications
- Applications are by far the leading cause of breaches (Verizon DBIR)

3. SOFTWARE SUPPLY CHAIN SECURITY IS TOTALLY BROKEN



March 7
CVE-2017-5638
Disclosed, Apache
releases fixed version

Mid-May
Equifax
breach
occurs

July 29
Equifax
learns of
breach

Sept 7
Equifax discloses,
Four more Struts2
CVEs disclosed

Livin' la vida loca

Equifax ignores

Equifax unaware

Disaster

Jan

Feb

Mar

Apr

May

Jun

Jul

Aug

Sept

Oct

Prepared

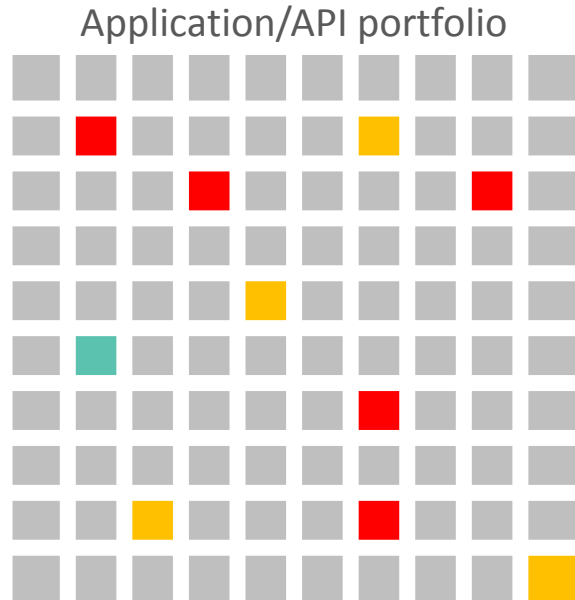
Protected

March 8
We observed
widespread
attack probes



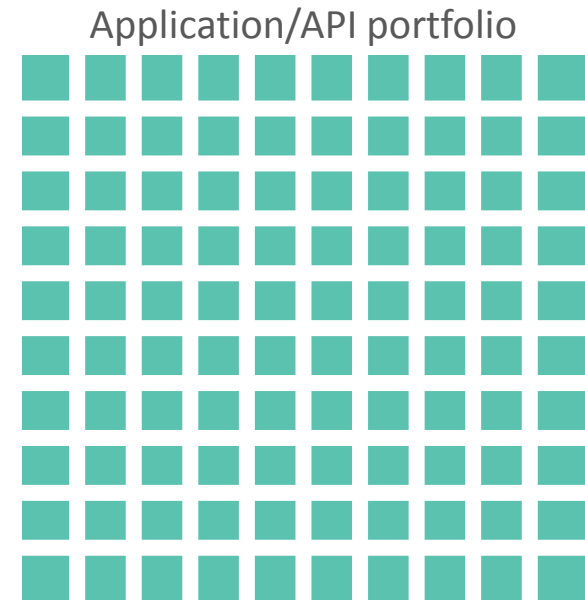
DIAGNOSIS: GOALS UNCLEAR, TIME WASTED

What we are delivering:



- ✓ “I ran a scanner”

What we must deliver:



- ✓ Right defenses in place
- ✓ Defenses are effective
- ✓ Attacks detected/blocked

PUPPY MONKEY BABY

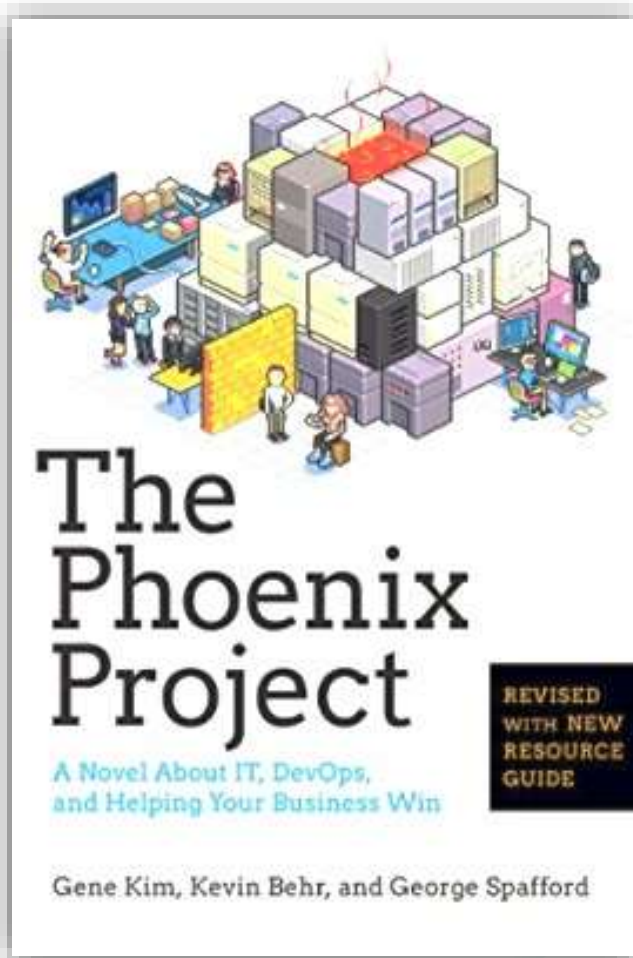


DEV

SEC

OPS

SO WHAT IS DEVOPS?



The “Three Ways”

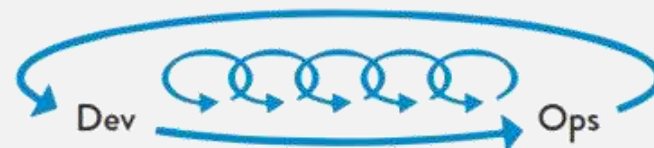
1. Establish work flow



2. Ensure instant feedback



3. Culture of experimentation

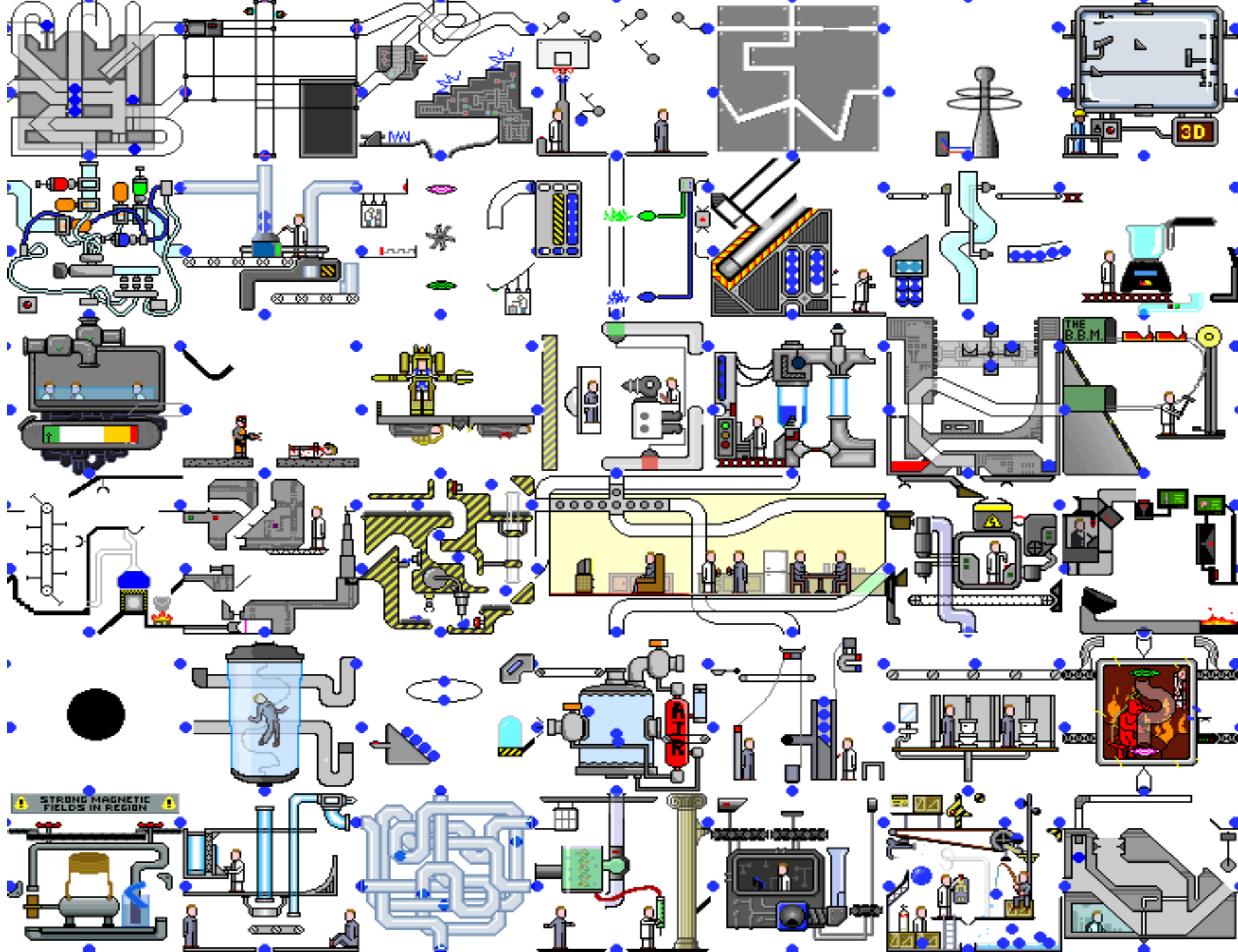


Small
batch
sizes

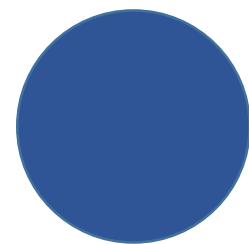
Tight
feedback
loops

Swarm
on
problems

Optimize
for
downstream
consumers



Produce
awesome
software



QUESTION: CAN DEVOPS HELP SECURITY?

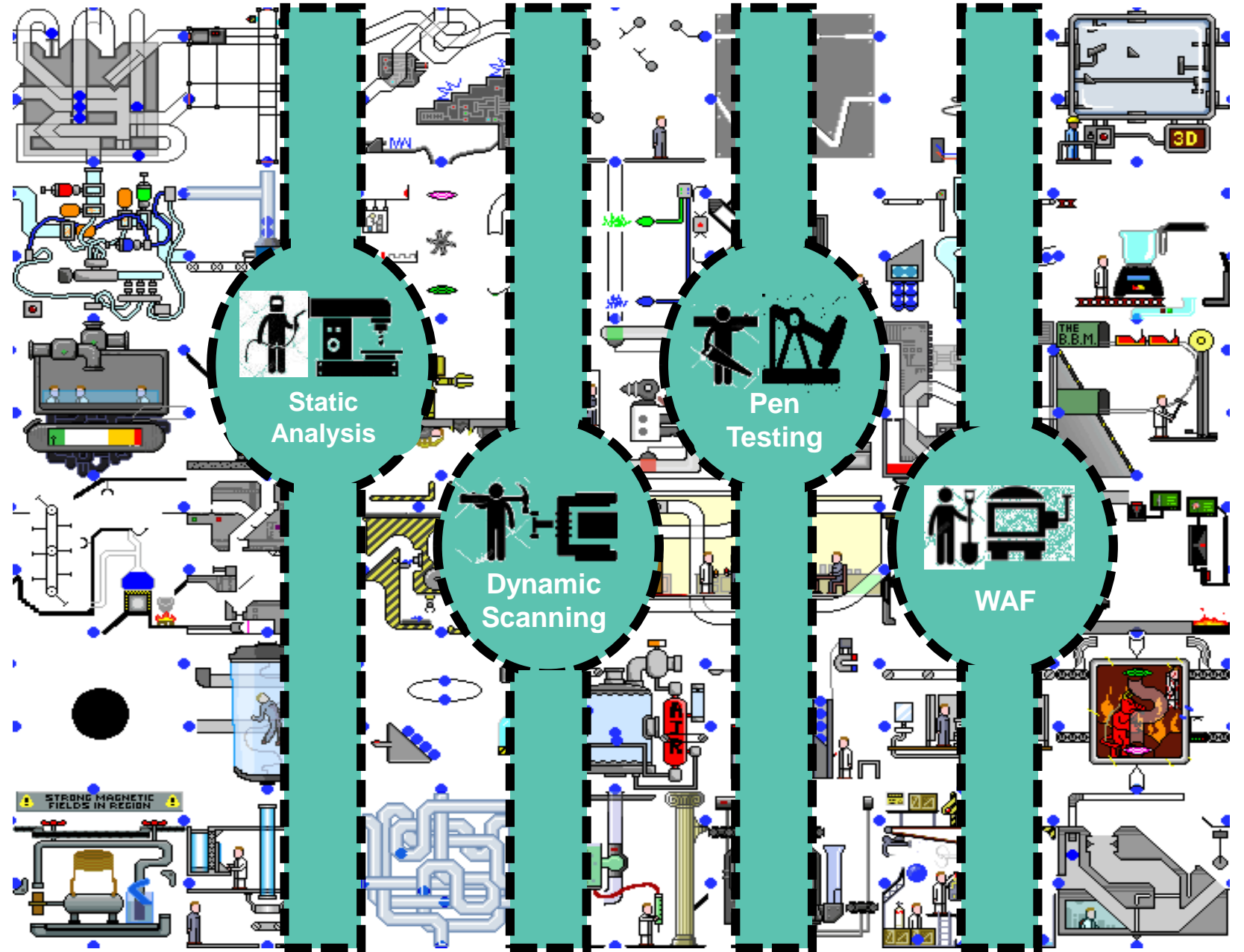
- **Problem:** **software** is poor quality, late, slow, and doesn't provide business value.
- **Approach:** DevOps
- **Outcomes:**
 - 5x lower change failure rate
 - 96x faster MTTR service
 - 2x likely to exceed bus. goal

- **Problem:** **security** is poor quality, late, slow, and doesn't provide business value.
- **Possible Approach:** DevOps
- **Required Outcomes:**
 - 10x increase in portfolio coverage?
 - 80% reduction in vulns to prod?
 - 0x increase in time to market?

SEC
DEV
OPS

!=

SHOVING
LEGACY
SECURITY TOOLS
AND
PROCESSES
SEC INTO



The “Three Ways” of Security*

- 1. Establish security work flow**
 - Build a concrete security story over time
 - Enable development to build security
 - Rip, mix, and burn security work
- 2. Ensure instant security feedback**
 - Enable self-inventory
 - Get real application threat intelligence
 - Create security notification infrastructure
- 3. Build a security culture**
 - Migrate to “positive” security
 - Accelerate evolution of your security story
 - Promote “security in sunshine”

* Shamelessly adapted from The Phoenix Project, by Gene Kim

The First
Security Way

Establish Security Work Flow

Optimize delivery of security work that is valued by the business

UMM.... WHAT IS SECURITY “WORK”?

1

Business Security Projects

Building defenses, compliance,
reporting, etc...

2

Internal Security Work

Threat modeling, security
architecture, security research,
vulnerability assessment, tools

3

Operational Security Jobs

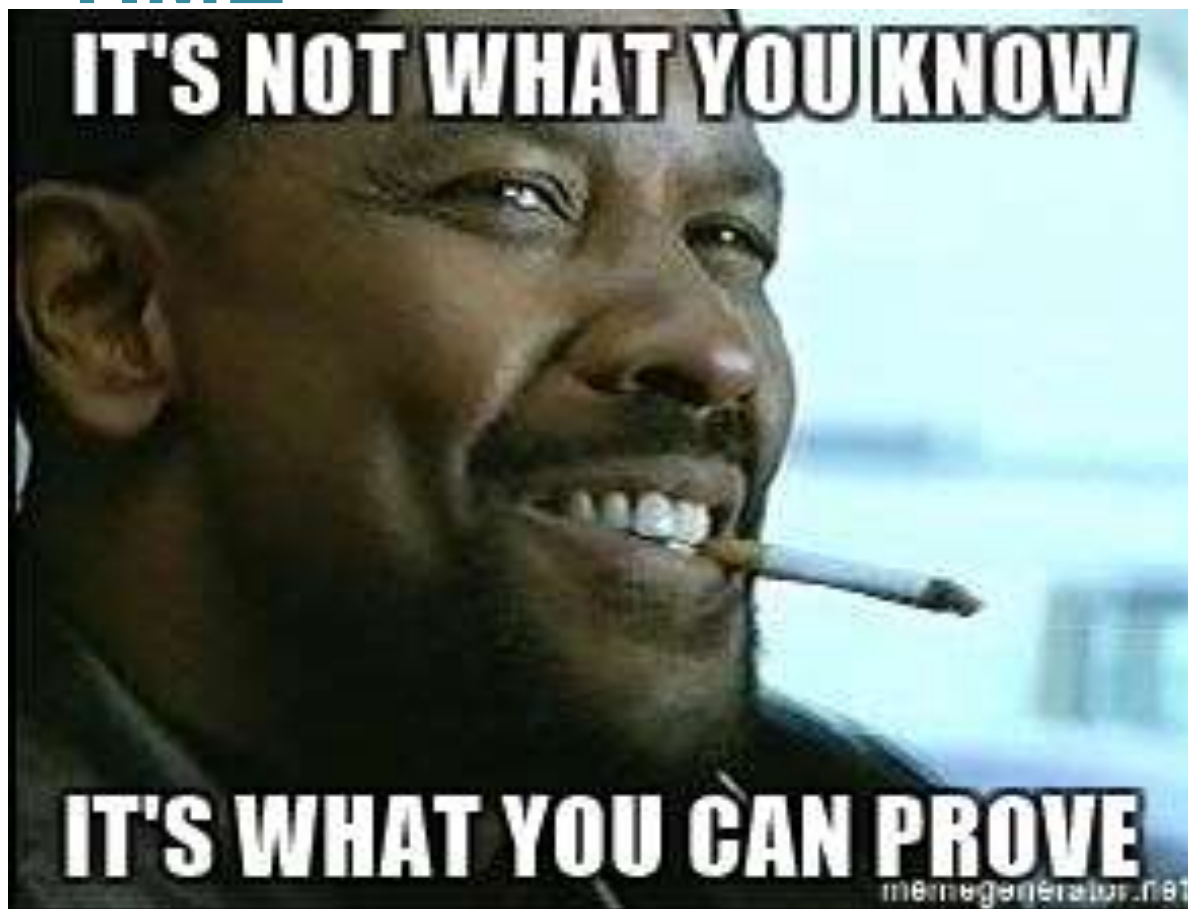
Remediation, updates,
analytics, alerts, tickets,
etc...

4

Unplanned Security Tasks

Security “firefighting,”
response, recovery, public
relations, etc...

FIRST WAY – BUILD A CONCRETE SECURITY STORY OVER TIME



The Rugged Bank Security Story

Commitment: Brick-and-mortar banks protect money with vaults, police, and alarms. As we move these operations to cyberspace, everyone should expect even better protection of their money and financial information. RuggedBank is committed to the highest standards of application and network security for our RBOOnline application. We secure our infrastructure, ensure data is always protected, build defenses against injection and other application attacks, practice rugged software development, and carefully verify our code. At the core of our security is a commitment to transparency – across our protections, processes, and even potential problems.

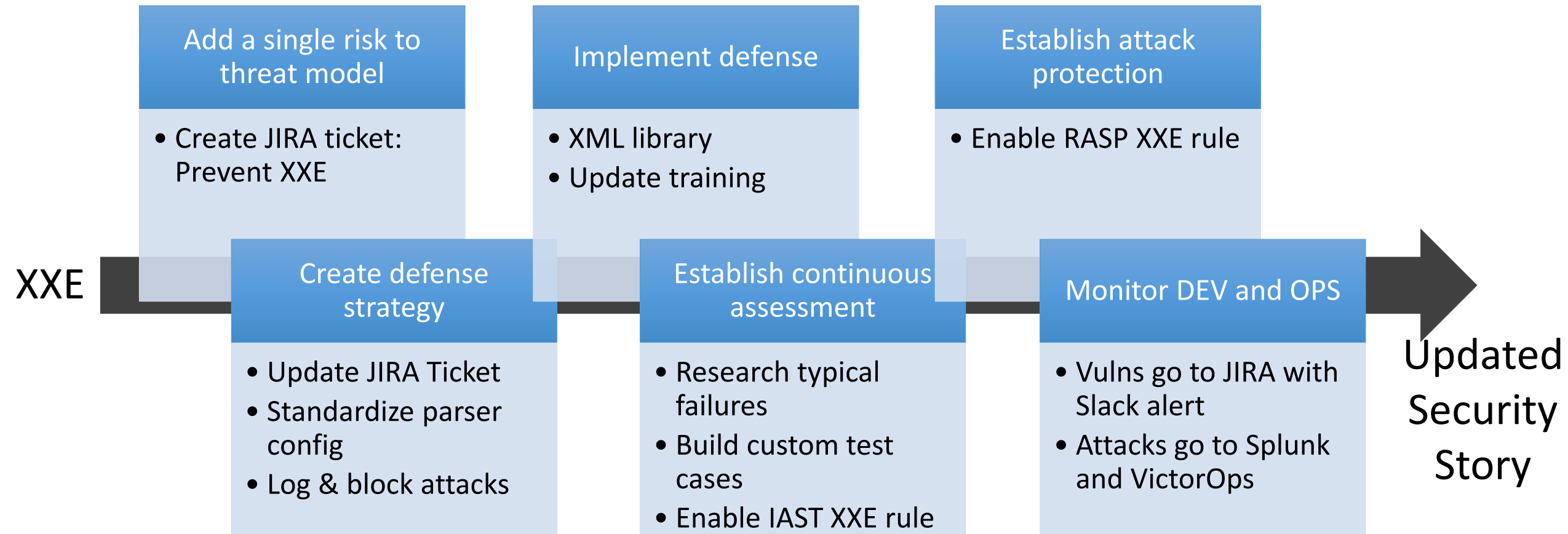
Your security story maps
threat model →
defense strategy →
defenses → assurance

Making security concrete:

- Enables communication
- Aligns your team
- Expose gaps and priorities
- Creates line-of-sight

* Shamelessly lifted from the Rugged Software Project

FIRST WAY – WORK ON BIGGEST THREATS, ONE AT A TIME



Do you really need security experts for all these tasks?

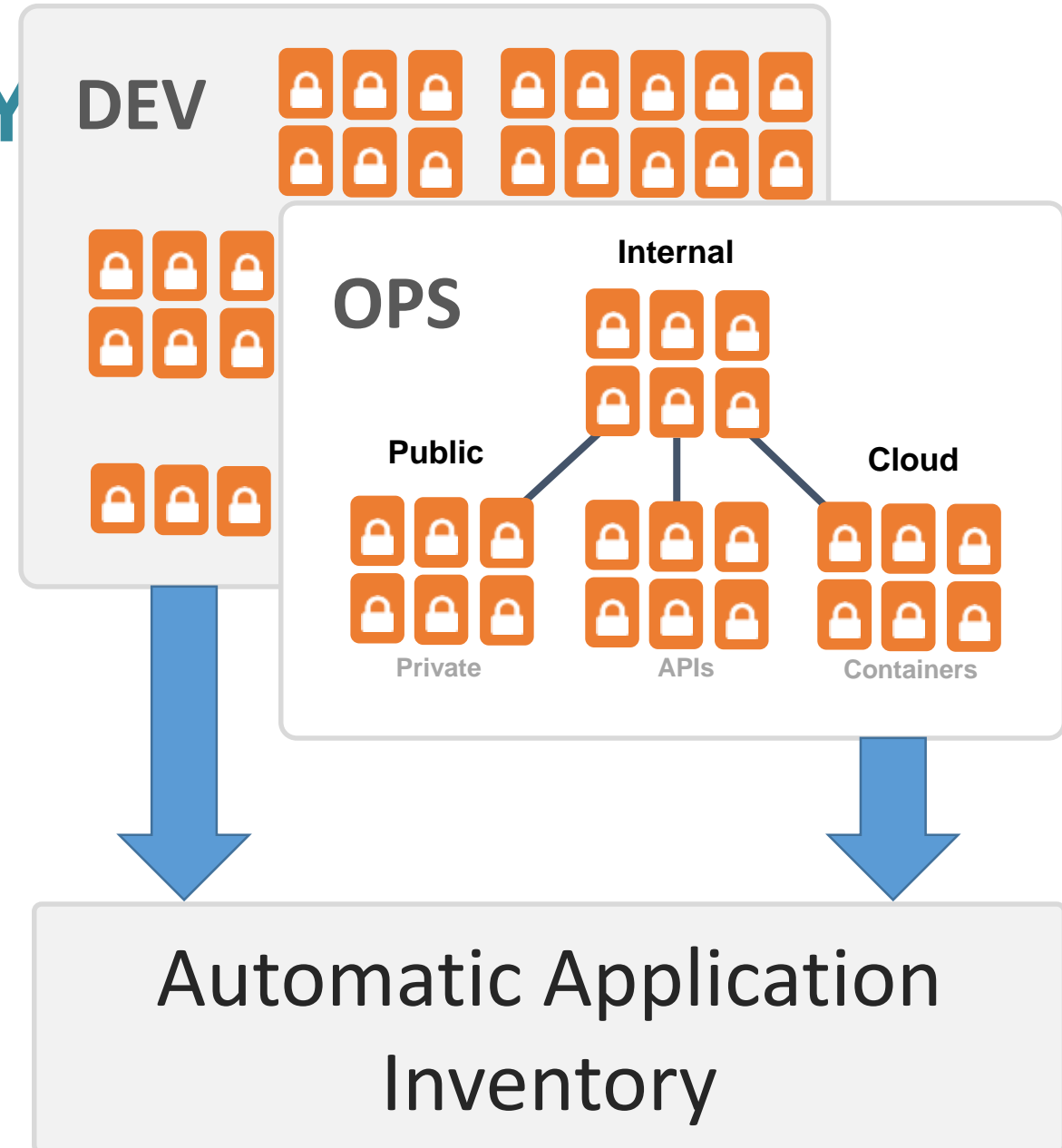
The Second
Security Way

Ensure Instant Security Feedback

**Establish tight security
feedback loops across the
lifecycle**

SECOND WAY – ENABLE SELF-INVENTORY

- You need to know the exact version of every app, api, and library running on every server in every environments
- Not hard to fully automate self-inventory



SECOND WAY – GET REAL APPLICATION THREAT INTELLIGENCE

Chrome File Edit View History Bookmarks People Window Help

Contrast Security

Secure https://apptwo.contrastsecurity.com/Contrast/static/ng/Index.html#/3c3a73d6-78a0-46c7-944a-b07b94d55711/attacks/events

CONTRAST Applications Servers Libraries Vulnerabilities Attacks Search Contrast + Add Application Jeff

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 + Add Exclusion

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

Overview Request Discussion

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

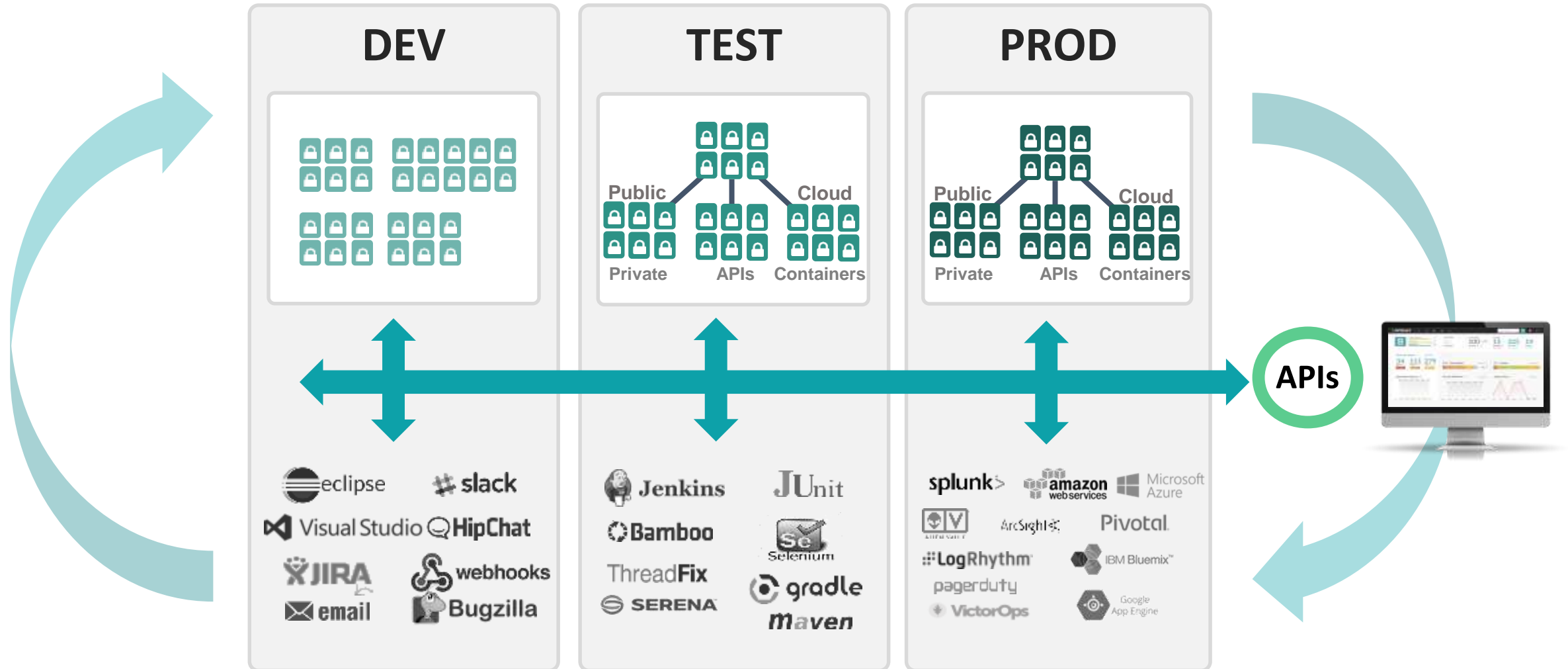
```
GET /Contrast/error/404.html HTTP/1.0
Accept: /*
Accept-Language: zh-cn
Connection: close
Content-Type: application/javascript
Cookie: ANSELB=539F750F10478D4E063589242269EA3B38F3BDF0DC18B0F7A35AA369BDF2525DBE006E8DA108F4FC48572AD541F9C37F85D9F6382CF8E20CC1054089C7766B93FCB079E28F15EF3BAF264DDEB64E0691CC65B16F00F; 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
```

Equifax Attack

Establish the infrastructure to...

- Know who is attacking you
- Know what techniques they're using
- Know what they're targeting
- ... and protect within hours

SECOND WAY – ESTABLISH A REALTIME APPSEC CONTROL PLANE

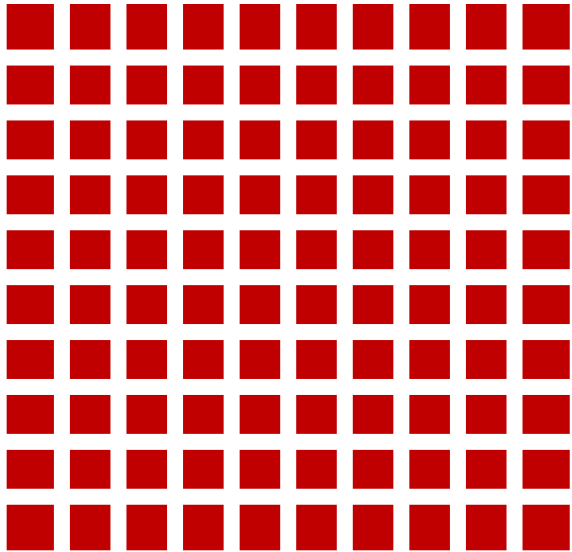


The Third Security Way

Build Security Culture

A culture that constantly advances security with the threat through experimentation and learning

THIRD WAY – MIGRATE TO “POSITIVE” SECURITY



Testing for all the ways you
might introduce XSS

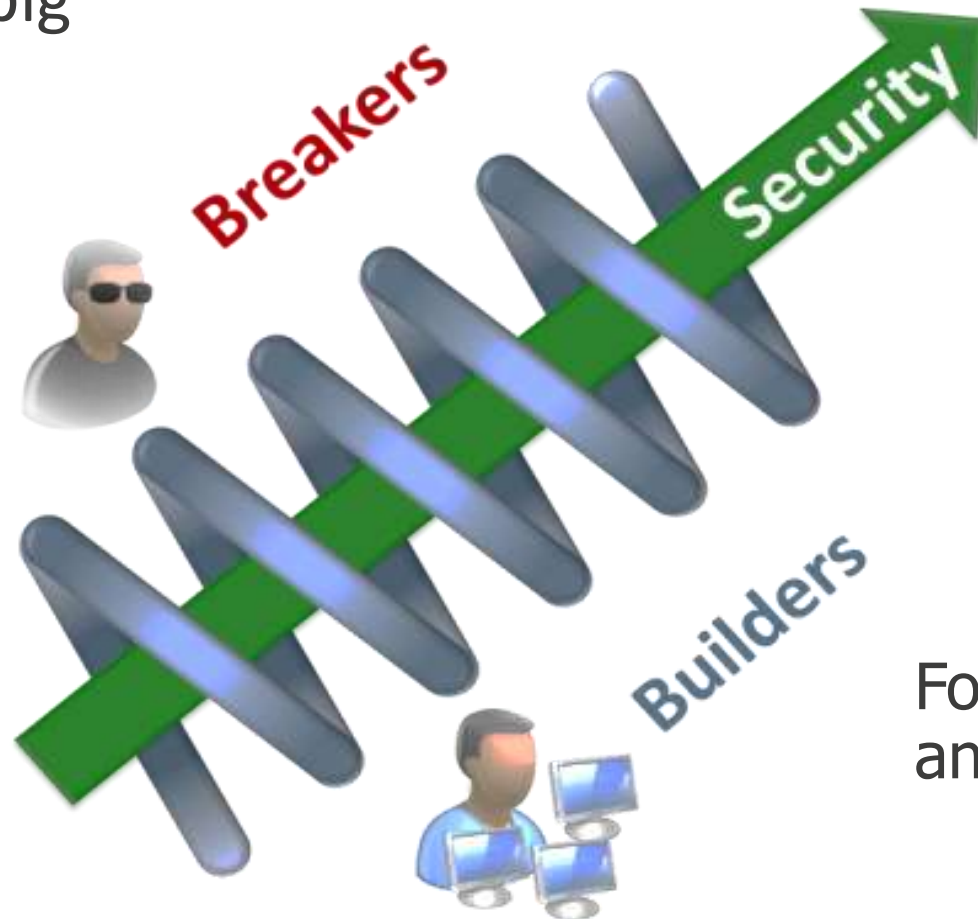
Measure positive security
directly from your running
application



Testing to verify
your XSS defense

THIRD WAY – ACCELERATE THE EVOLUTION OF YOUR SECURITY STORY

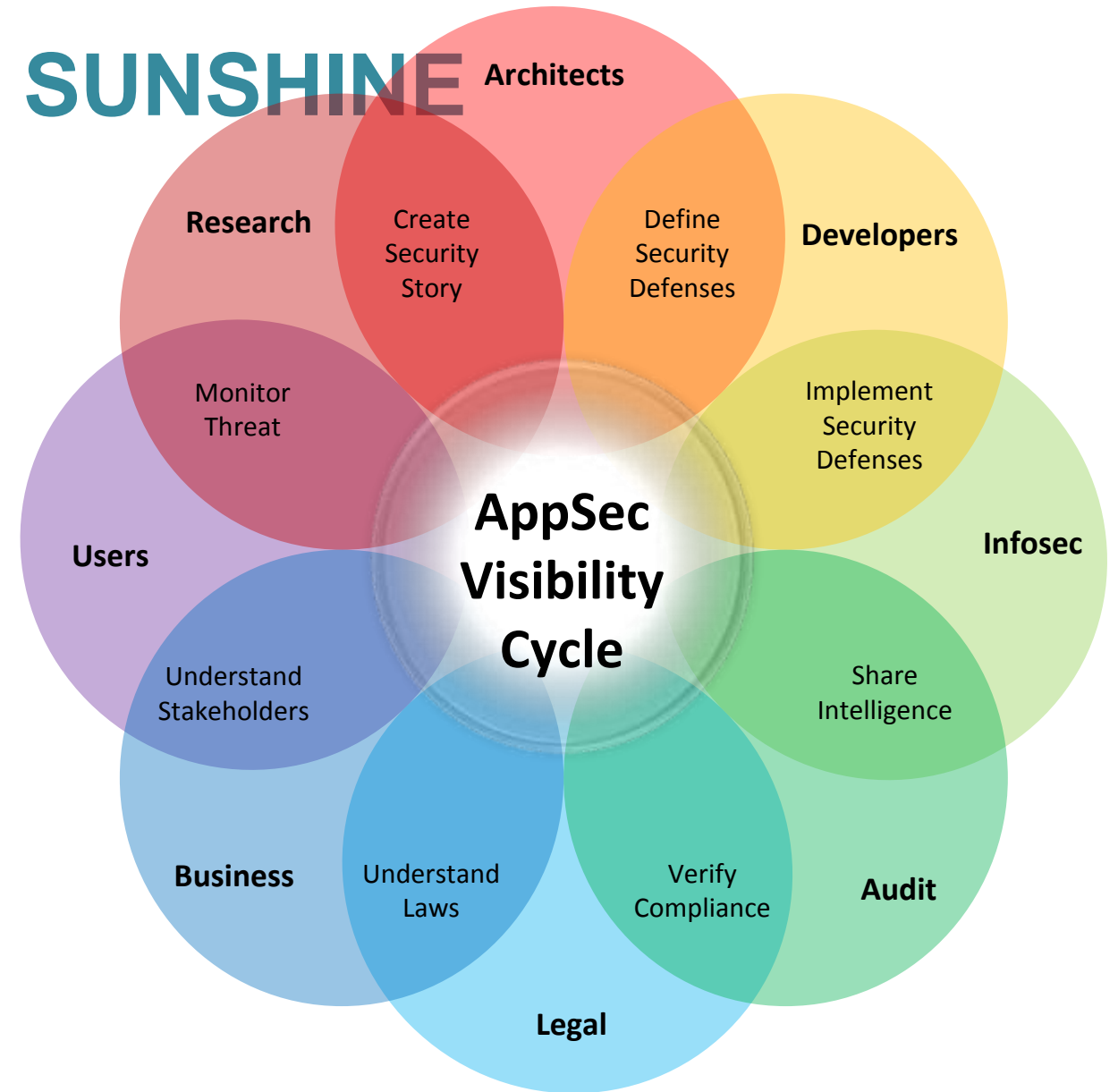
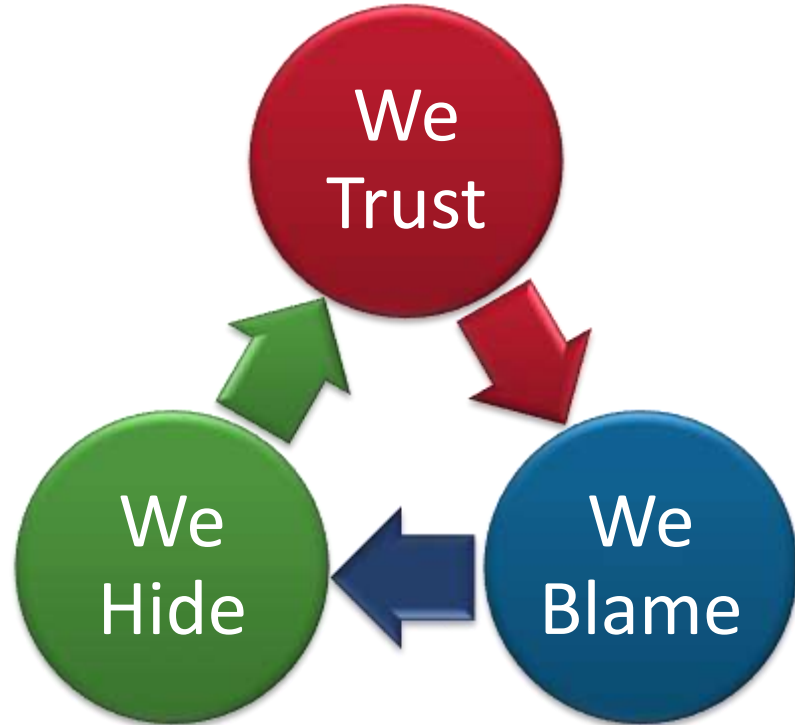
Celebrate new big risks without recrimination



The faster you cycle, the faster you get secure

Focus on strength and simplicity

THIRD WAY – PROMOTE SECURITY IN SUNSHINE



TRUST

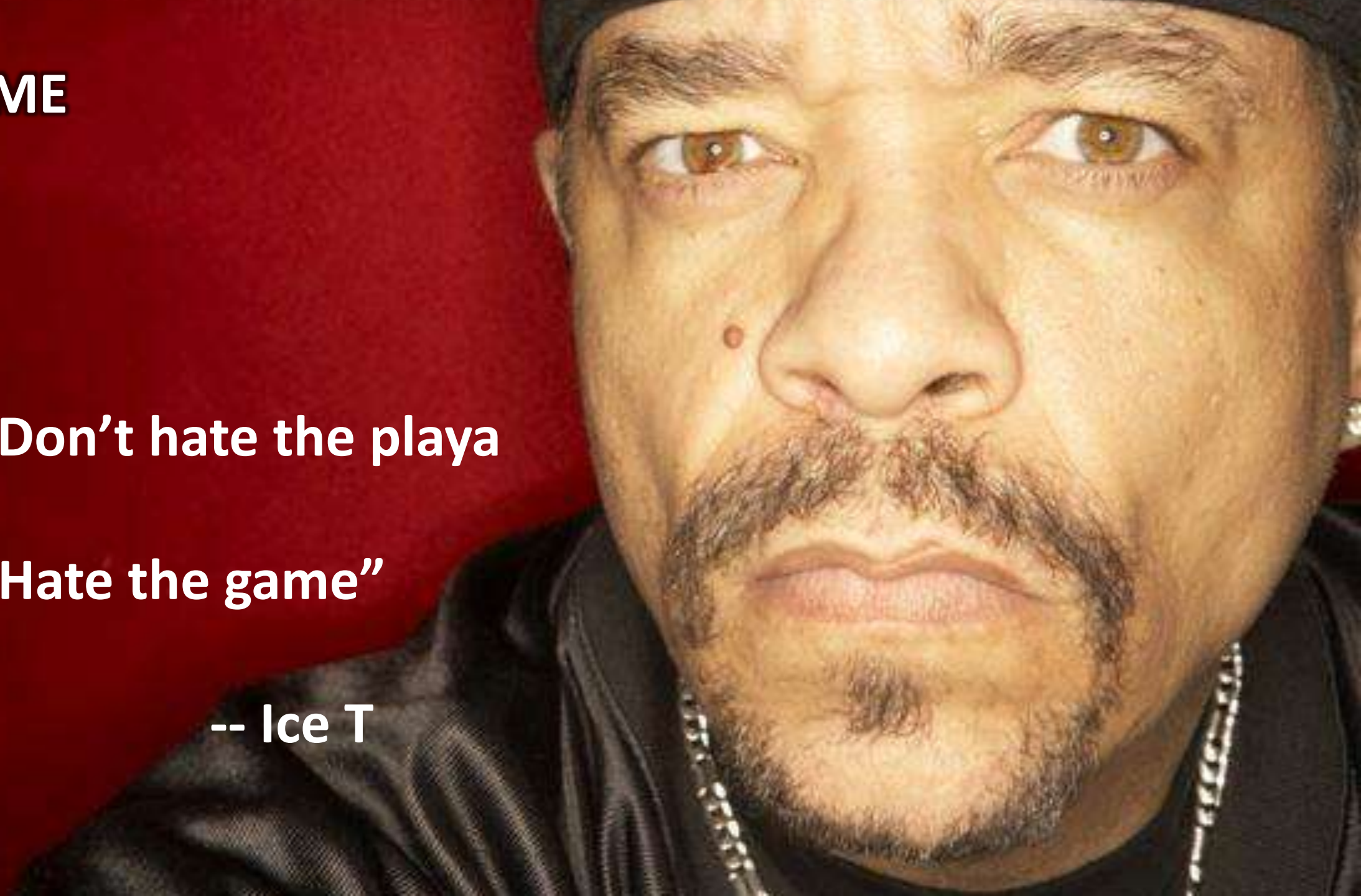


BLAME

“Don’t hate the playa

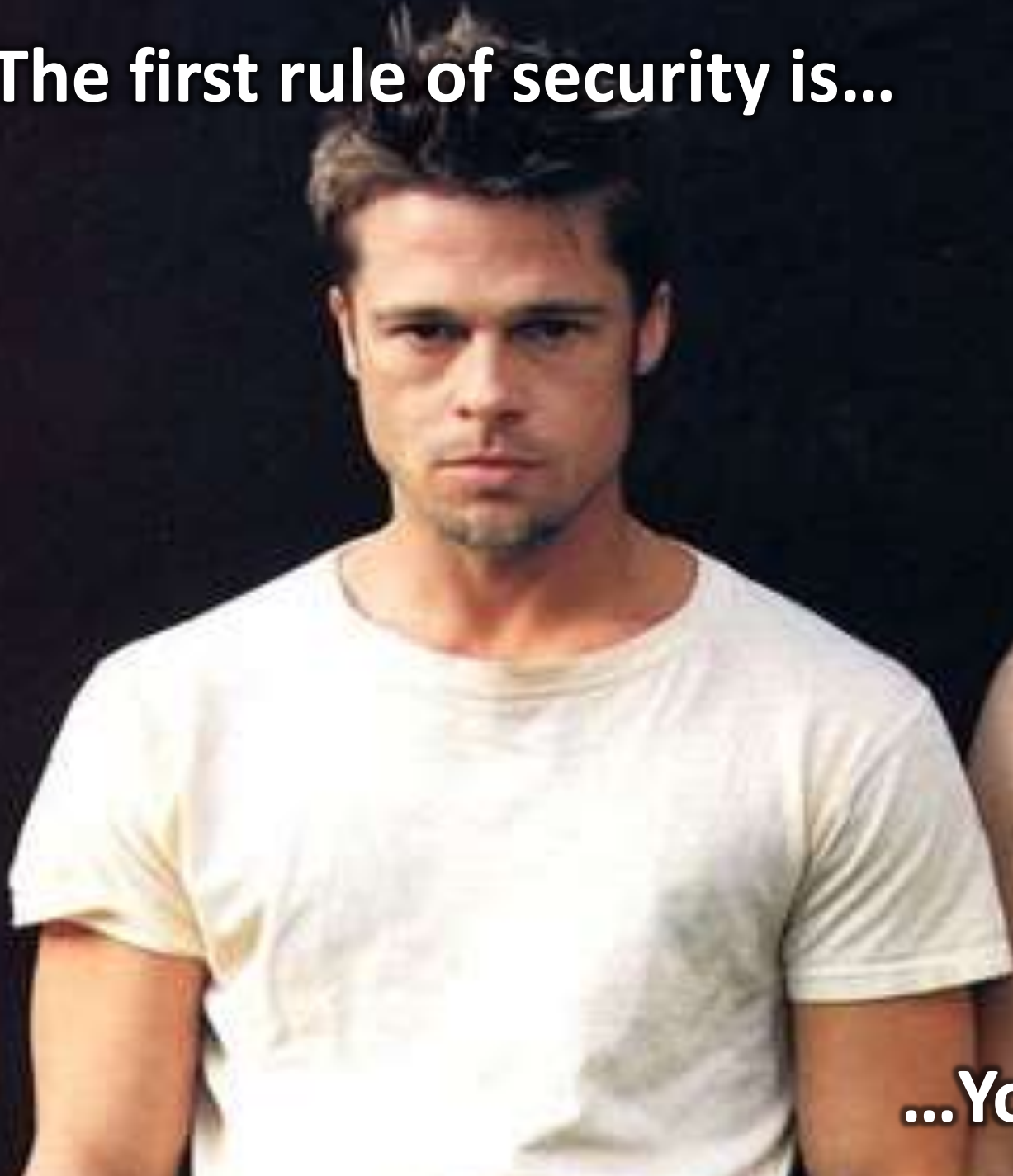
Hate the game”

-- Ice T



The first rule of security is...

HIDE



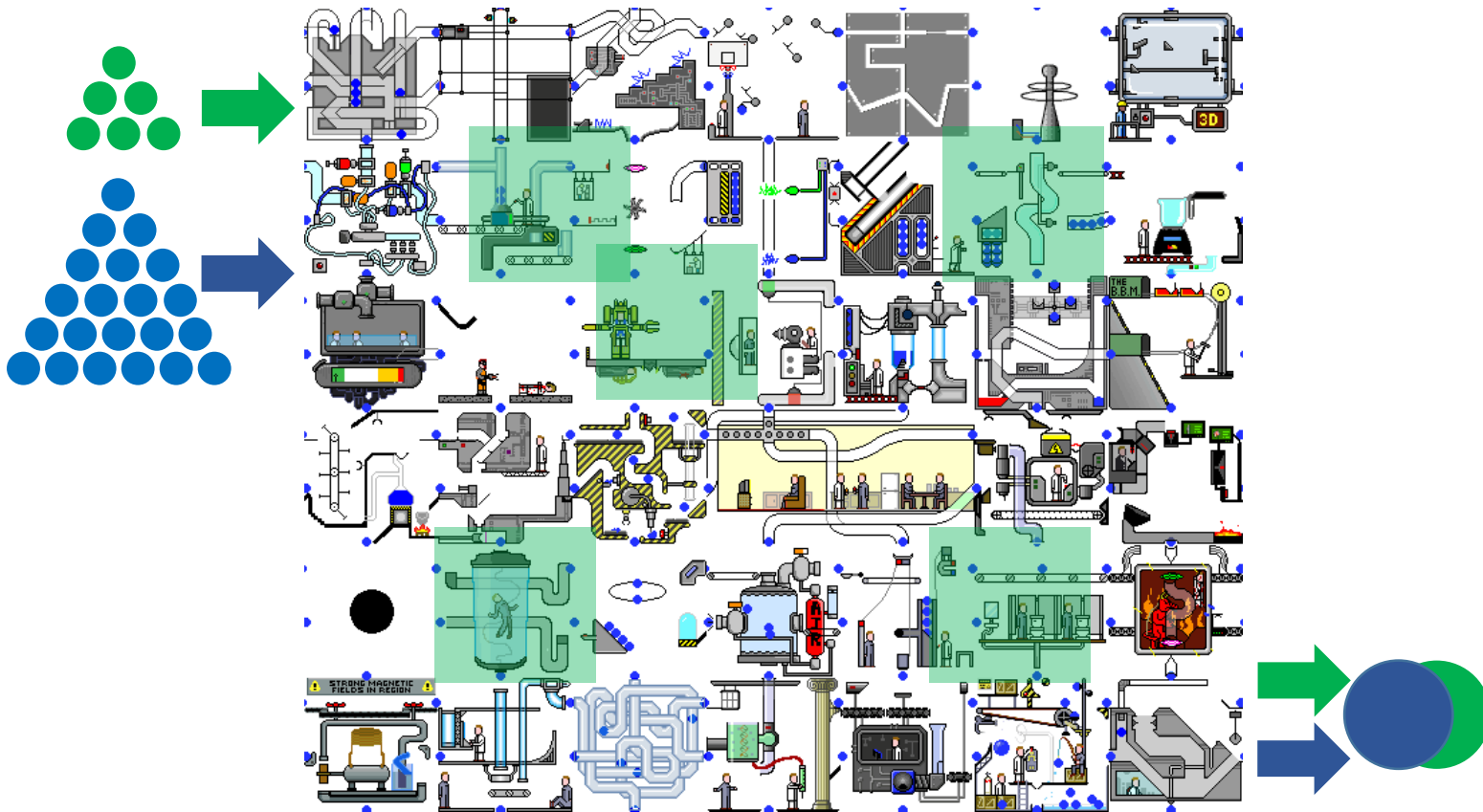
...You do not talk about security

The “Three Ways” of Security*

- 1. Establish security work flow**
 - Build a concrete security story over time
 - Enable development to build security
 - Rip, mix, and burn security work
- 2. Ensure instant security feedback**
 - Enable self-inventory
 - Get real application threat intelligence
 - Create security notification infrastructure
- 3. Build security culture**
 - Migrate to “positive” security
 - Accelerate evolution of your security story
 - Promote “security in sunshine”

* Shamelessly adapted from The Phoenix Project, by Gene Kim

CLOSING THOUGHTS – TURNING SECURITY INTO CODE

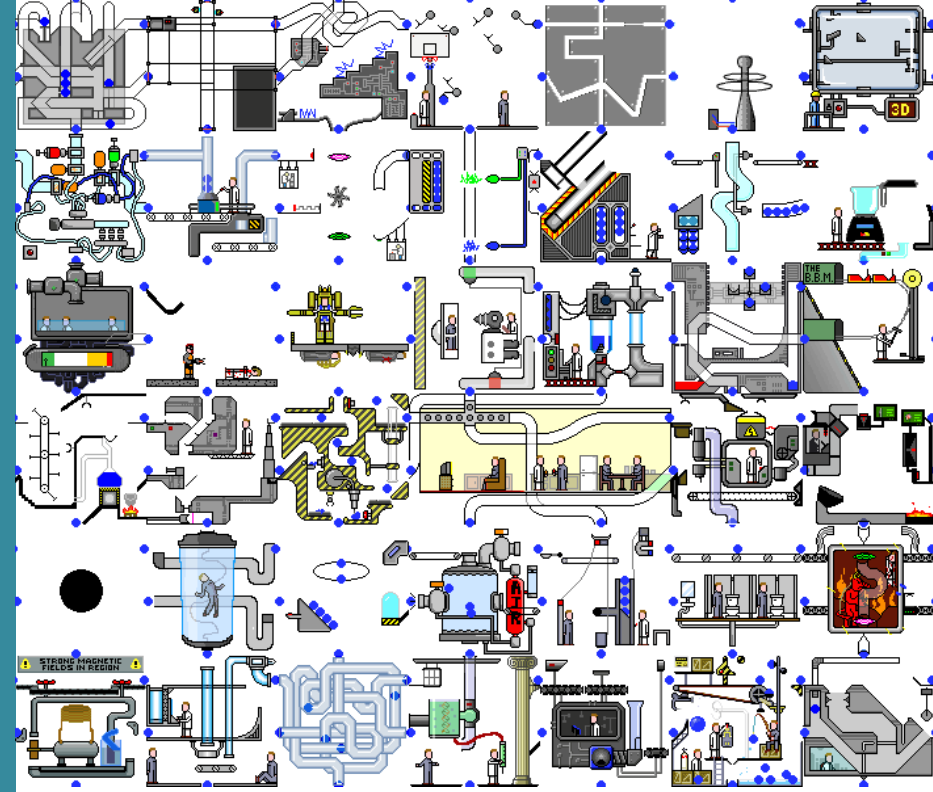


- Don't focus on how to build software securely...
- Make software security into something you build!

Ask me anything.

@planetlevel

contrastsecurity.com



CONTRAST
SECURITY

Gartner
VISIONARY

FORRESTER
LEADER



Software
Development
Solution