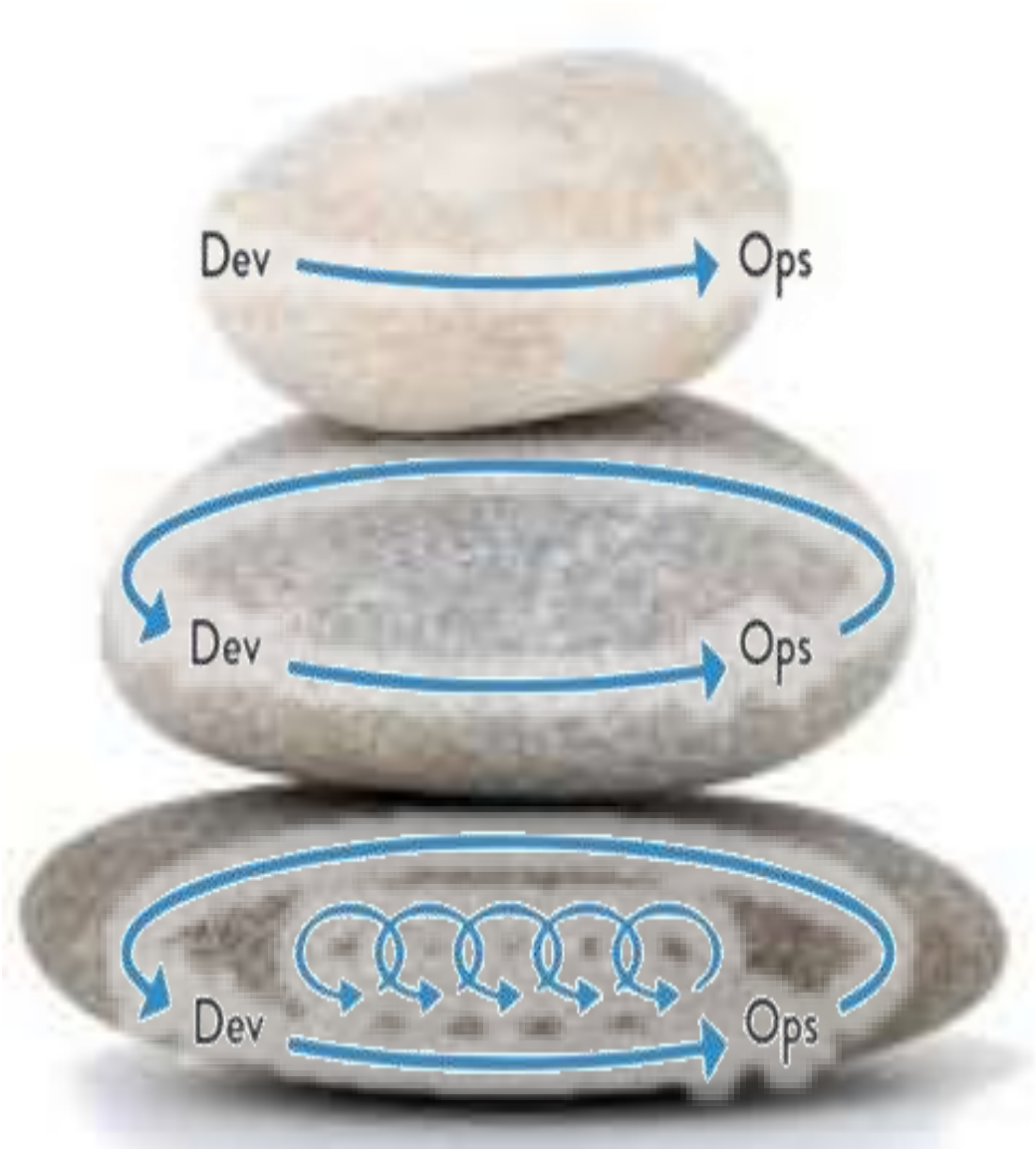
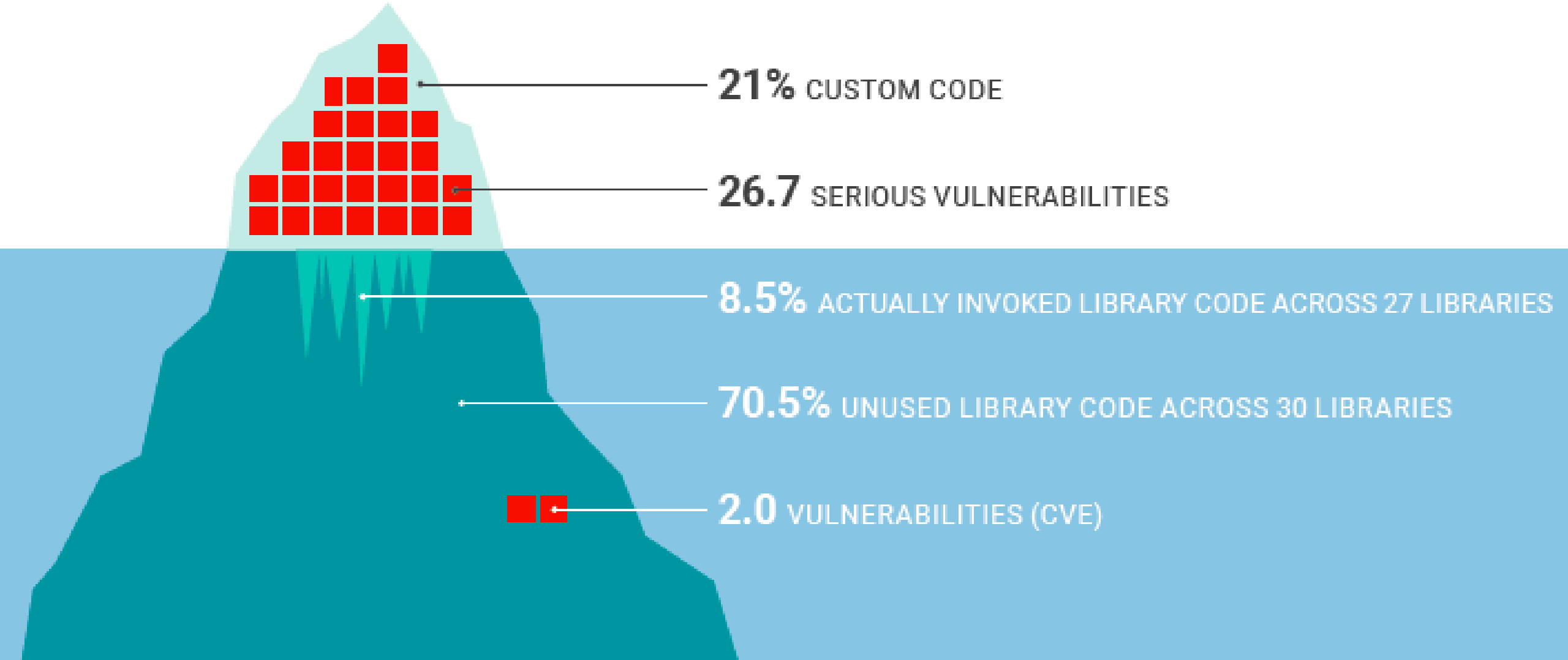
THE THREE WAYS OF SECURITY

Jeff Williams
Co-founder and CTO
Contrast Security

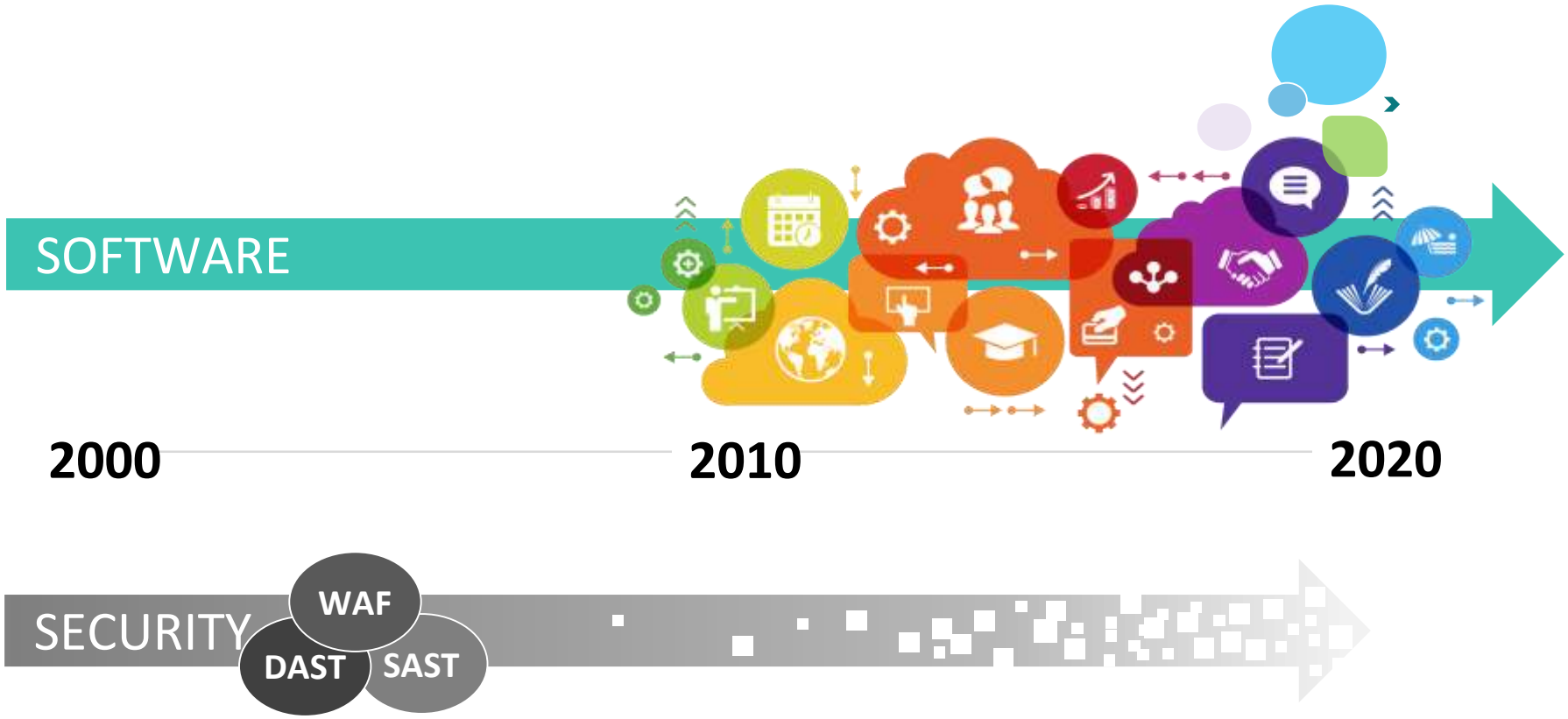
CONTRAST SECURITY



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



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

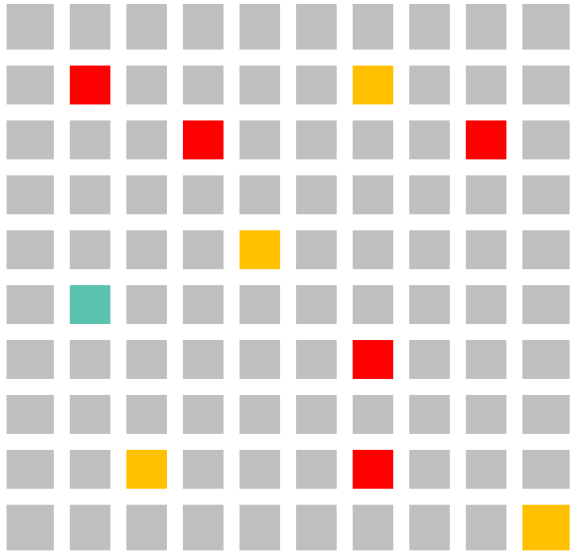
Prepared | Protected

March 8
We observed widespread attack probes

DIAGNOSIS: GOALS UNCLEAR, TIME WASTED

What we are delivering:

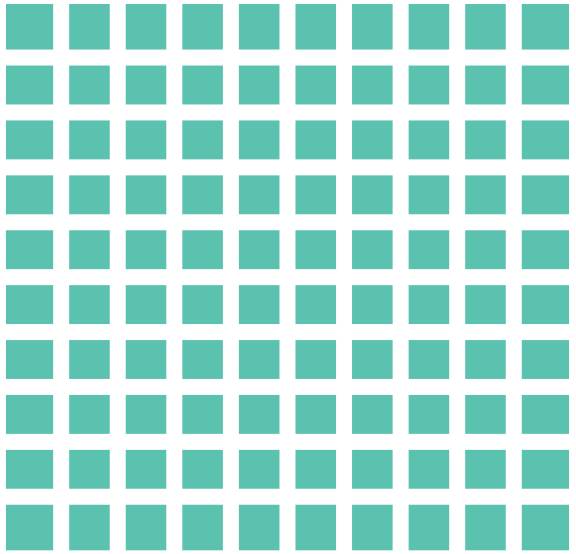
Application/API portfolio



✓ “I ran a scanner”

What we must deliver:

Application/API portfolio



✓ Right defenses in place

✓ Defenses are effective

✓ Attacks detected/blocked

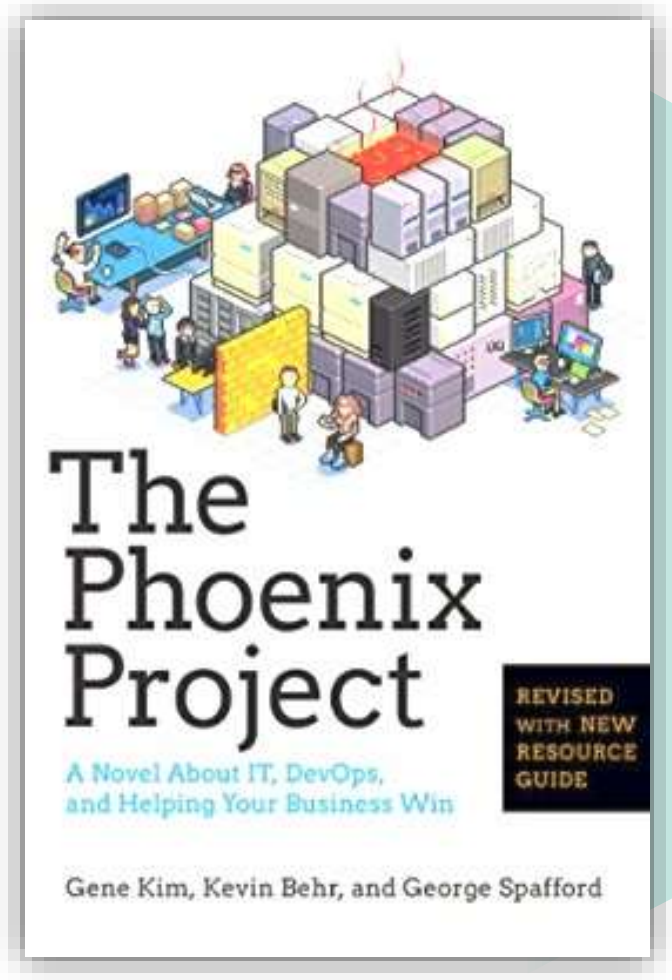
PUPPY MONKEY BABY

DEV

SEC

OPS

SO WHAT IS DEVOPS?



The "Three Ways"

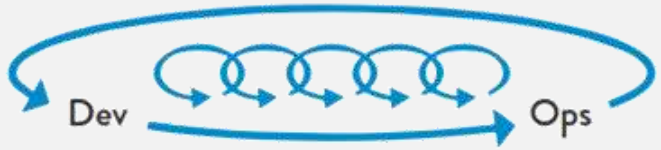
1. **Establish work flow**

(Business) (Customer)

Dev → Ops

2. **Ensure instant feedback**

3. **Culture of experimentation**



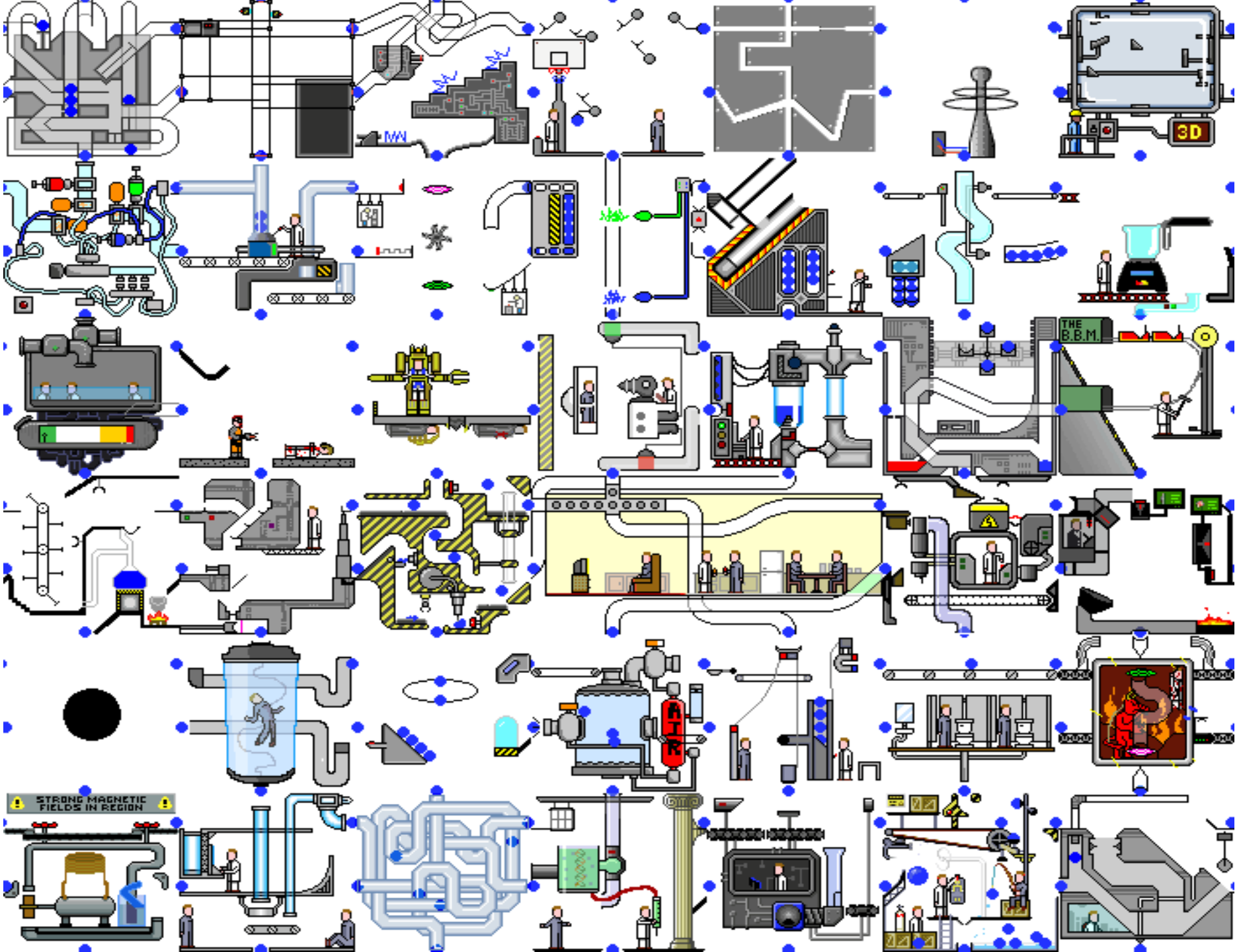
https://itrevolution.com/the-three-ways-principles-underpinning-devops/

Small batch sizes

Tight feedback loops

Swarm on problems

Optimize for downstream consumers



Produce awesome software

QUESTION: CAN DEVOPS HELP SECURITY?

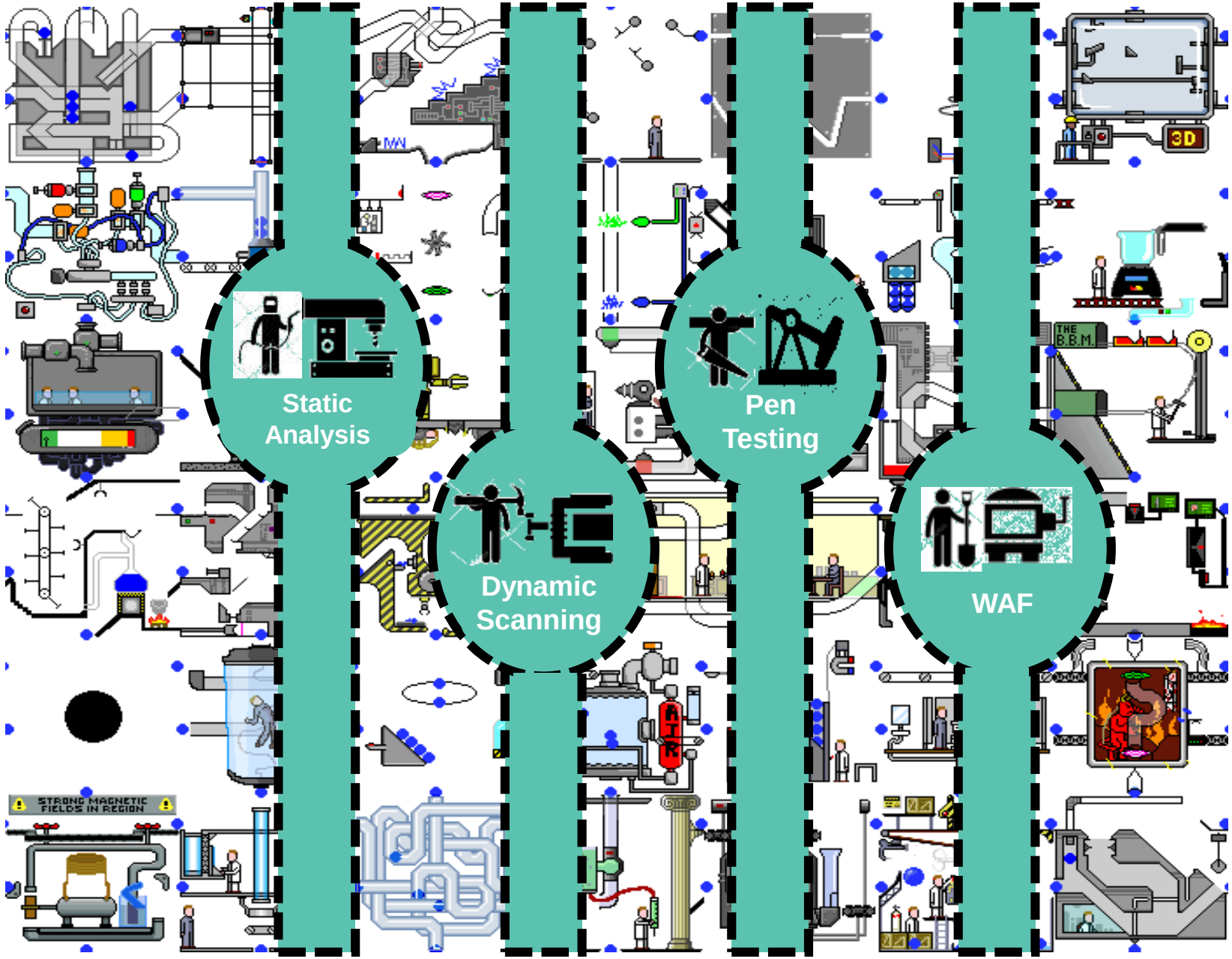
- **Problem**: **software** is poor quality, late, slow, and doesn't provide business value.
- **Approach**: DevOps
- **Outcomes**:
  - 5x lower change failure rate
  - 96x faster MTTR service
  - 2x likely to exceed bus. goal

- **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 PROCES



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

Establish Security Work Flow

The First Security Way

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

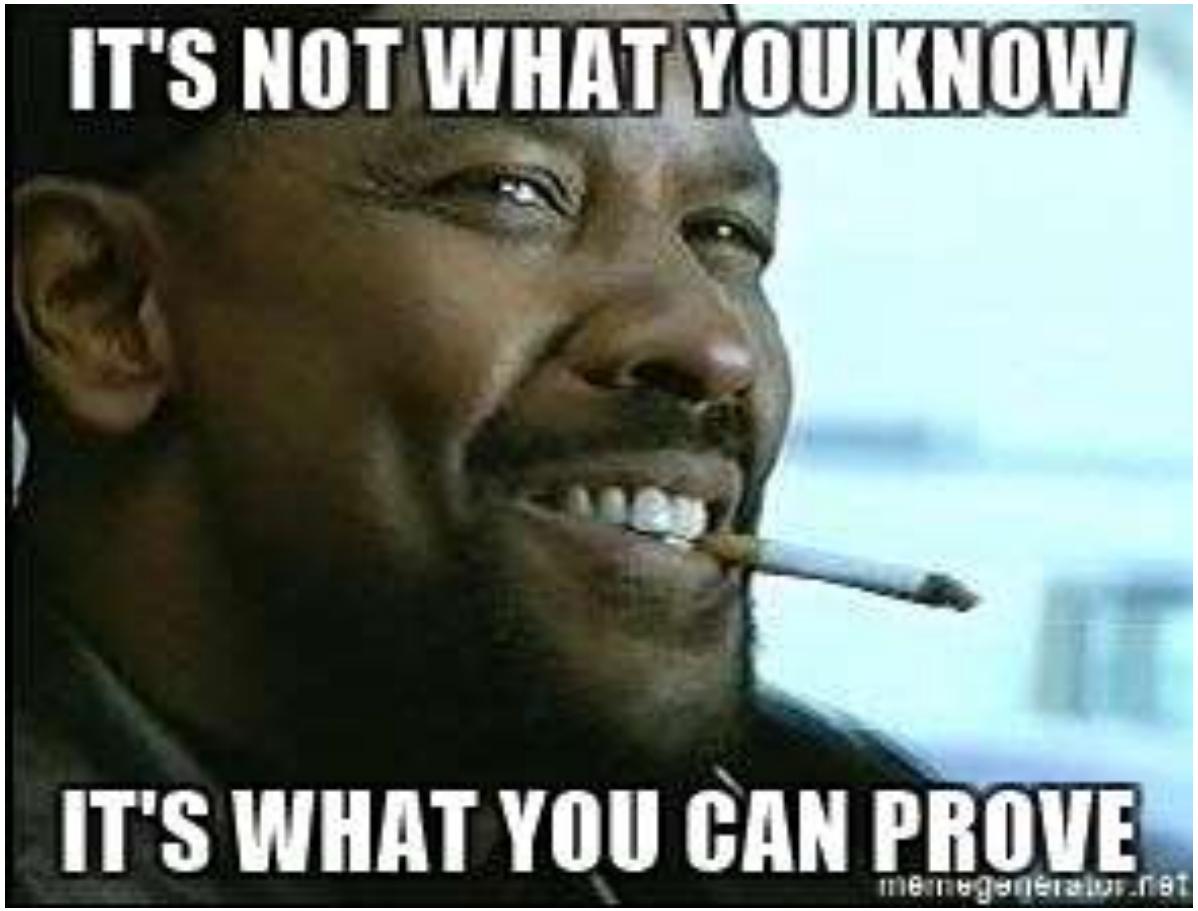
Remediation, updates, analytics, alerts, tickets, etc…

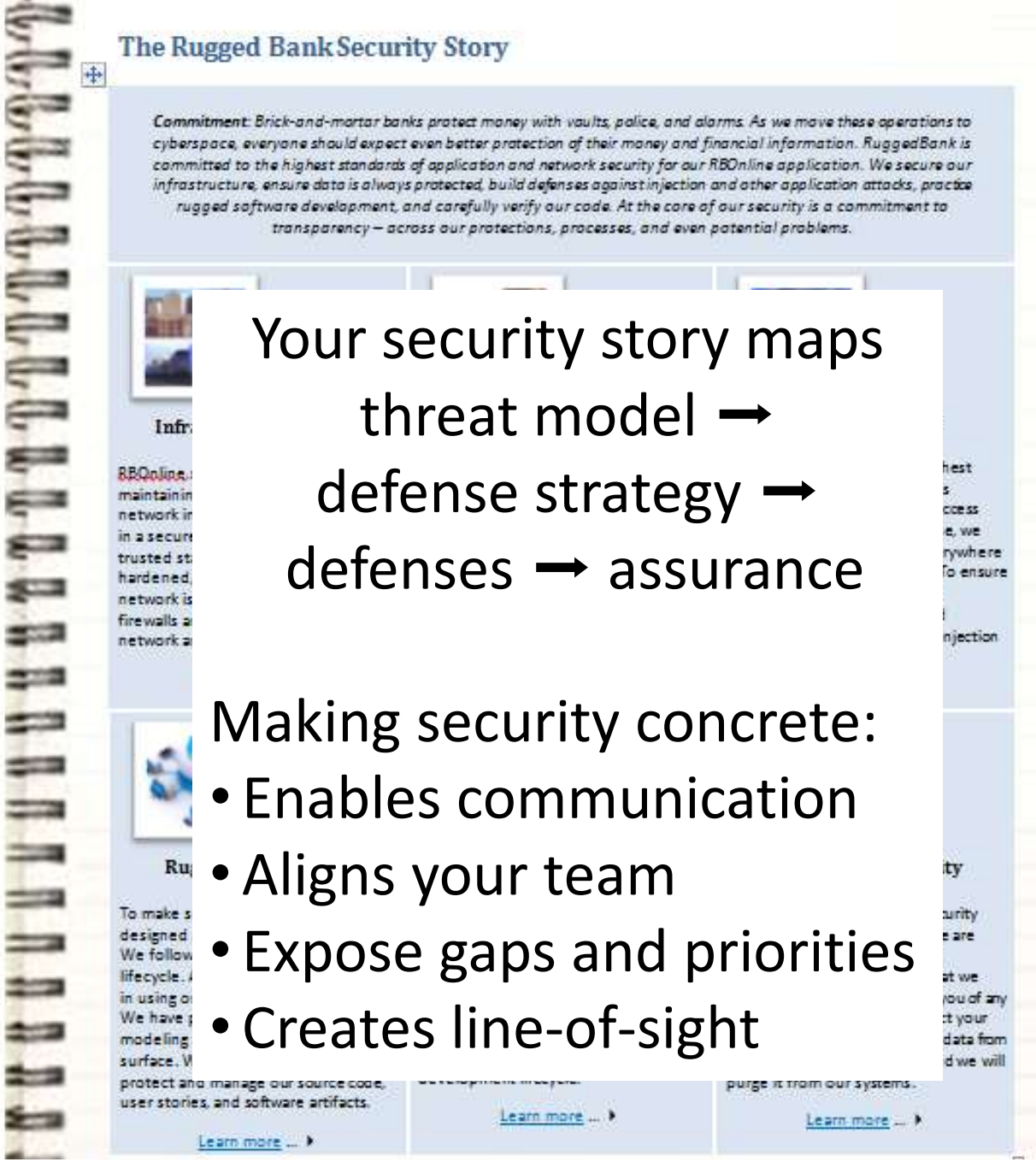
4

Unplanned Security Tasks

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

FIRST WAY – BUILD A CONCRETE SECURITY STORY OVER TIME





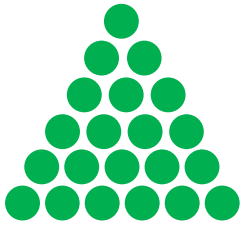
Your security story maps
threat model ➞
defense strategy ➞
defenses ➞ assurance

Making security concrete:

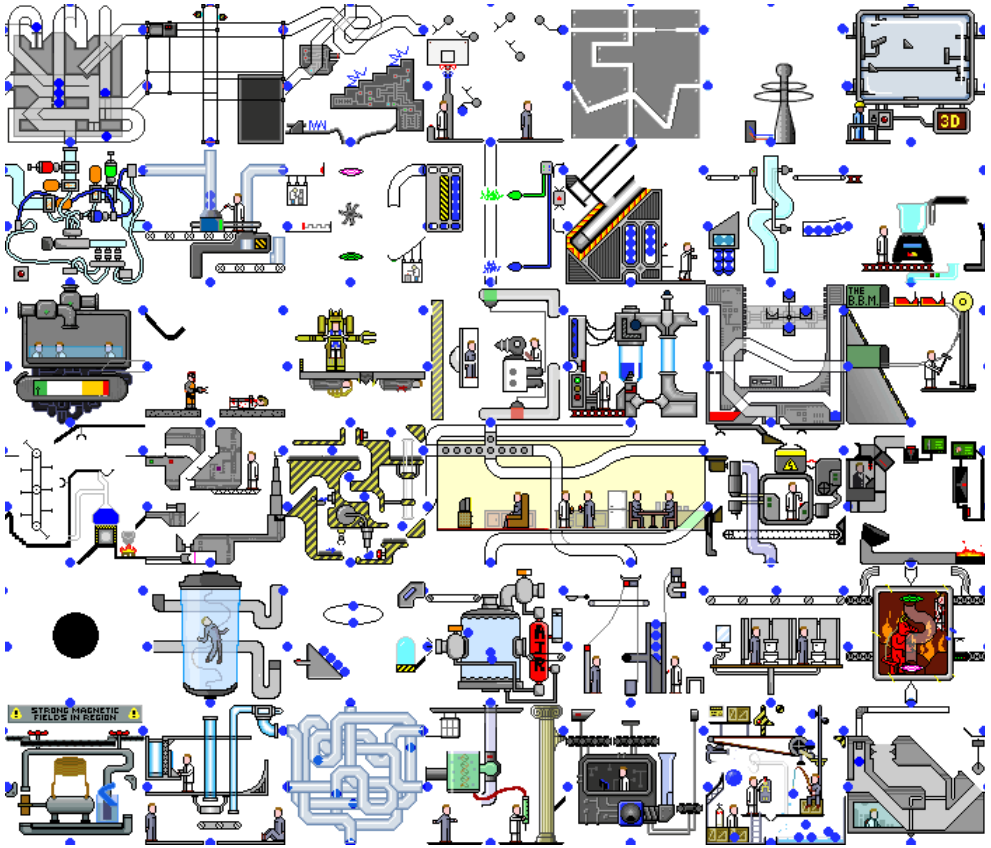
- Enables communication
- Aligns your team
- Expose gaps and priorities
- Creates line-of-sight

* Shamelessly lifted from the Rugged Software Project

FIRST WAY – ENABLE DEVELOPMENT TO BUILD SECURITY

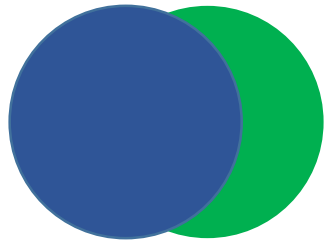


Refactor monolithic security tasks into small batch sizes.

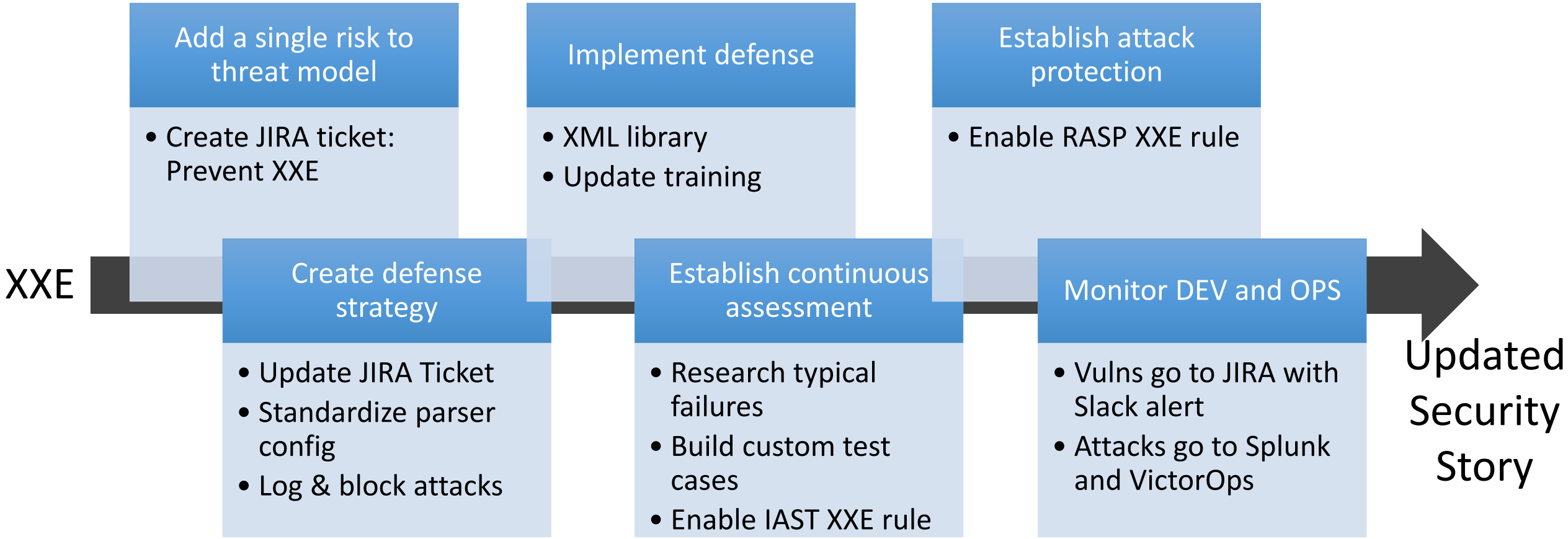


Leverage existing DevOps processes and tools

Deliver security one little piece at a time



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



Do you really need security experts for all these tasks?

The Second Security Way

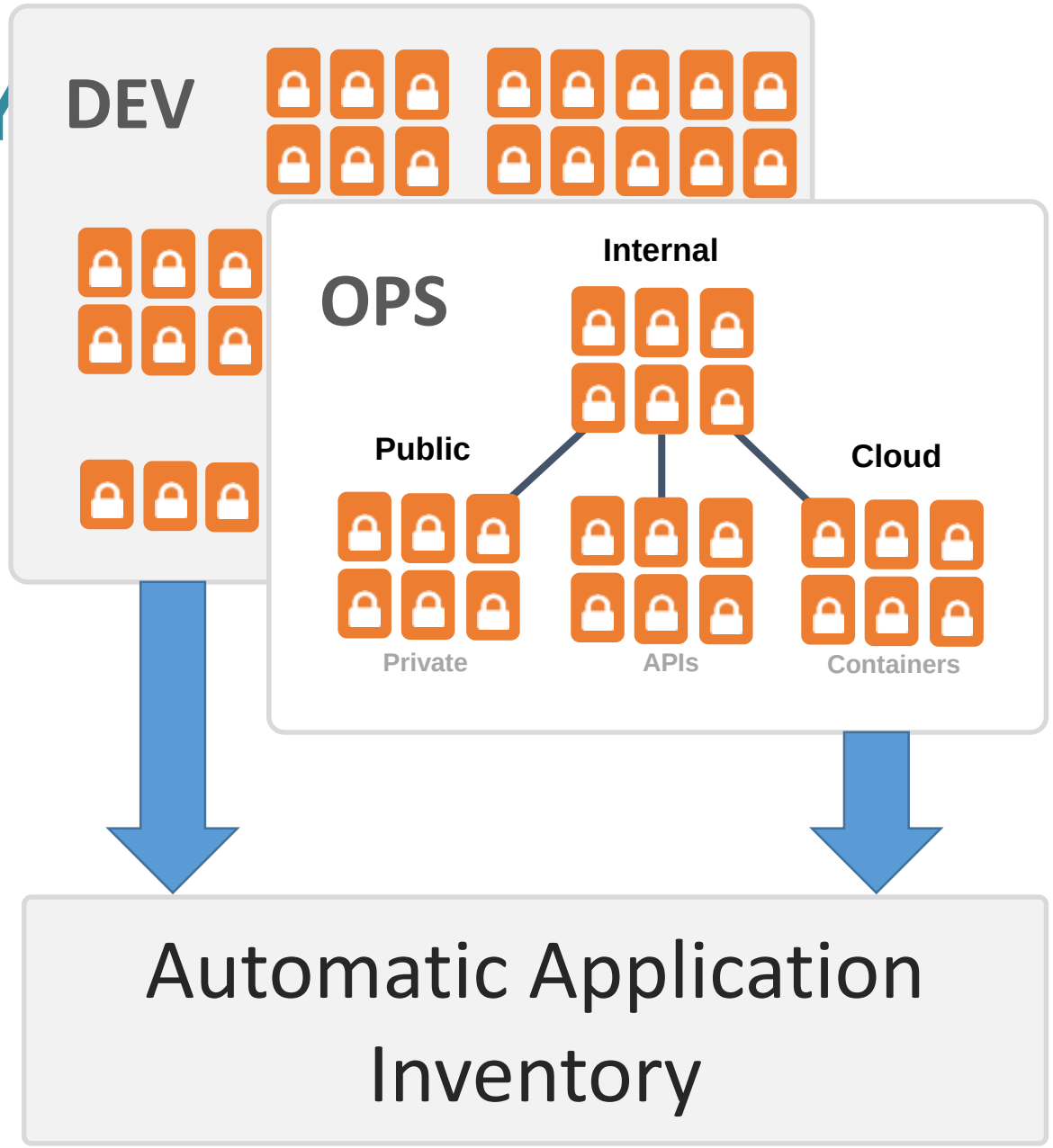
Ensure Instant Security Feedback

Establish tight security feedback loops across the lifecycle

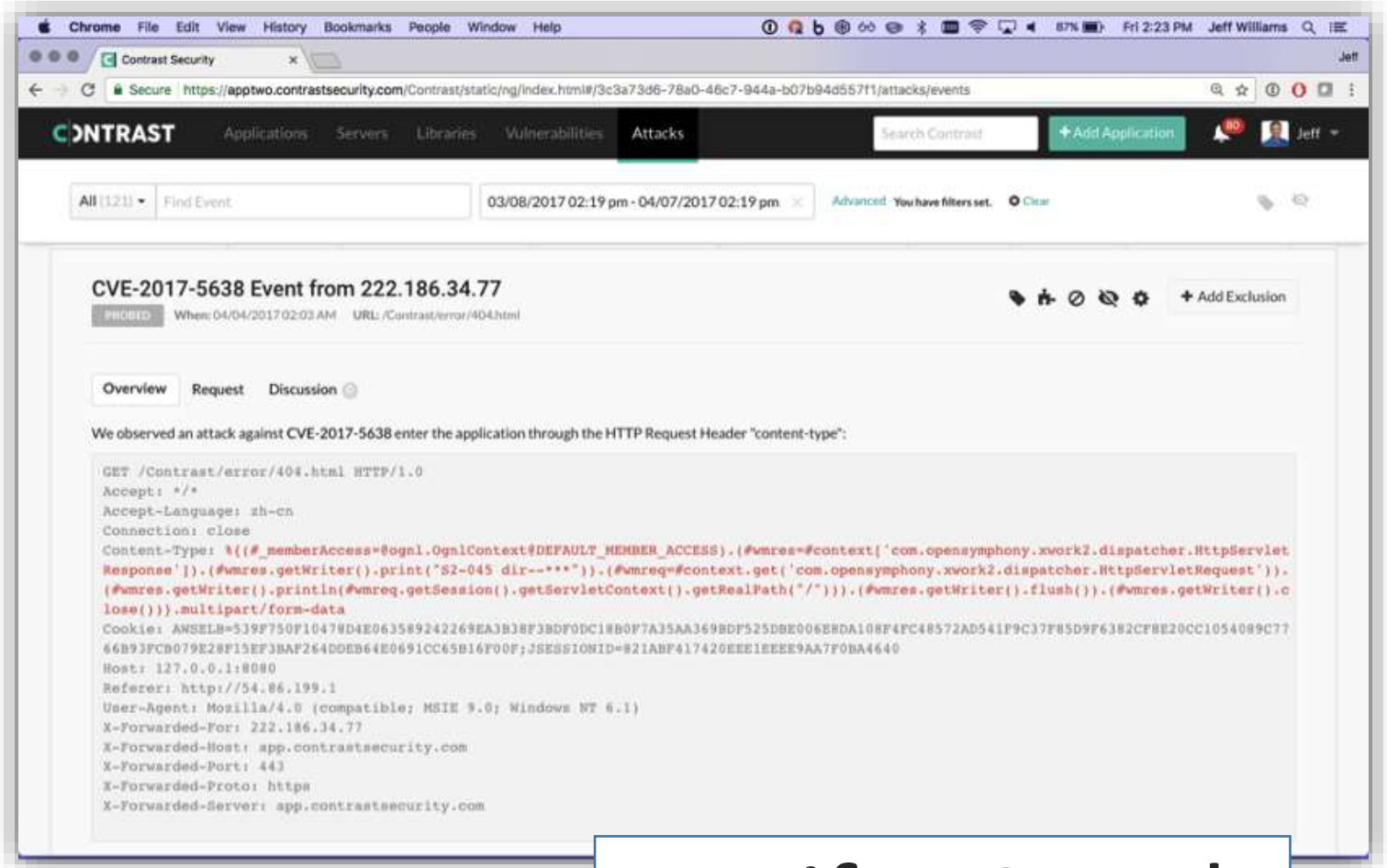
SECOND WAY – ENABLE SELF-INVENTORY

- 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

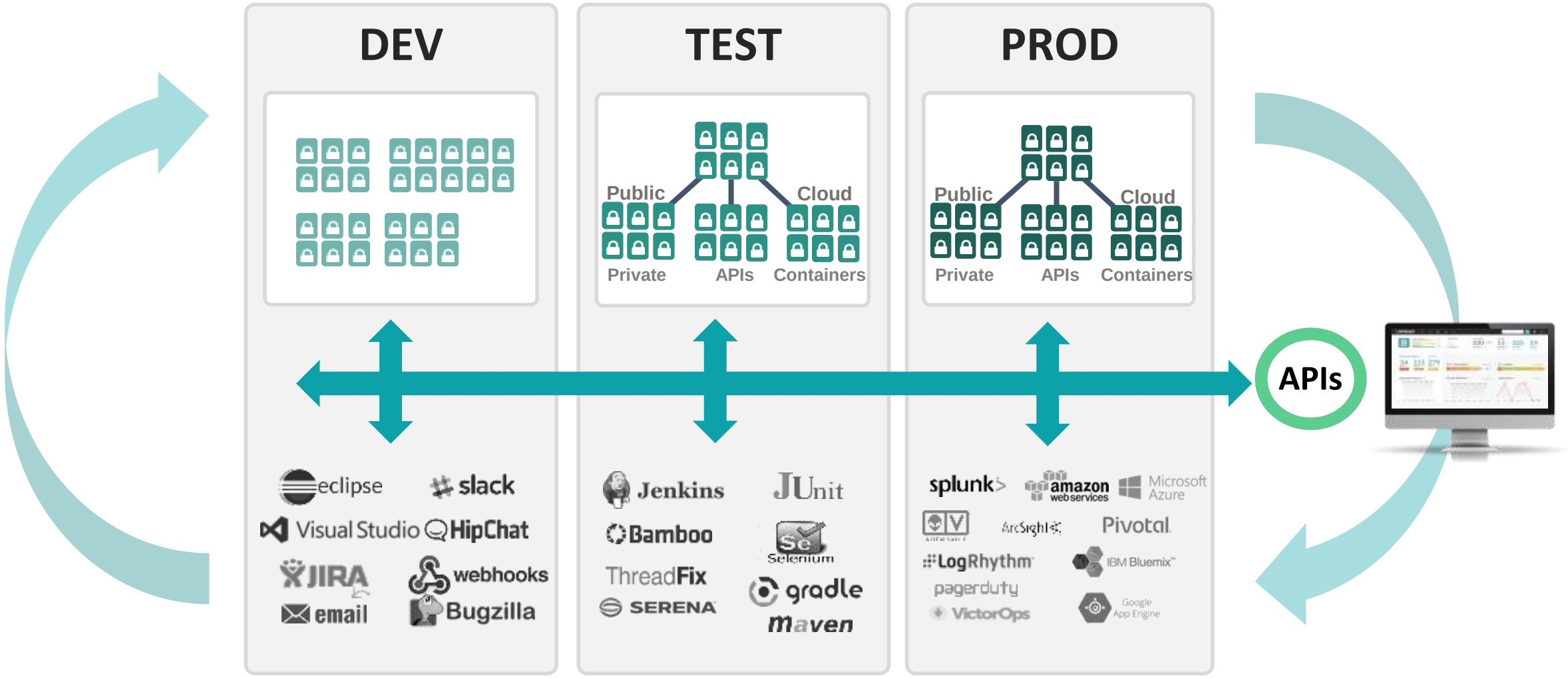


Equifax Attack

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

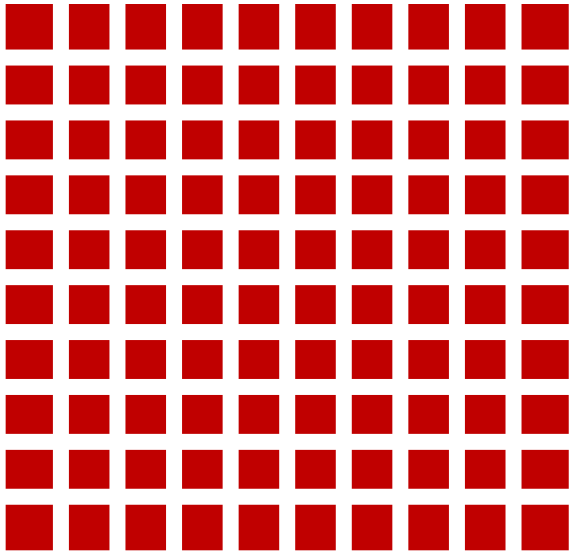


The Third Security Way

Build Security Culture

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

THIRD WAY – MIGRATE TO “POSITIVE” SECURITY



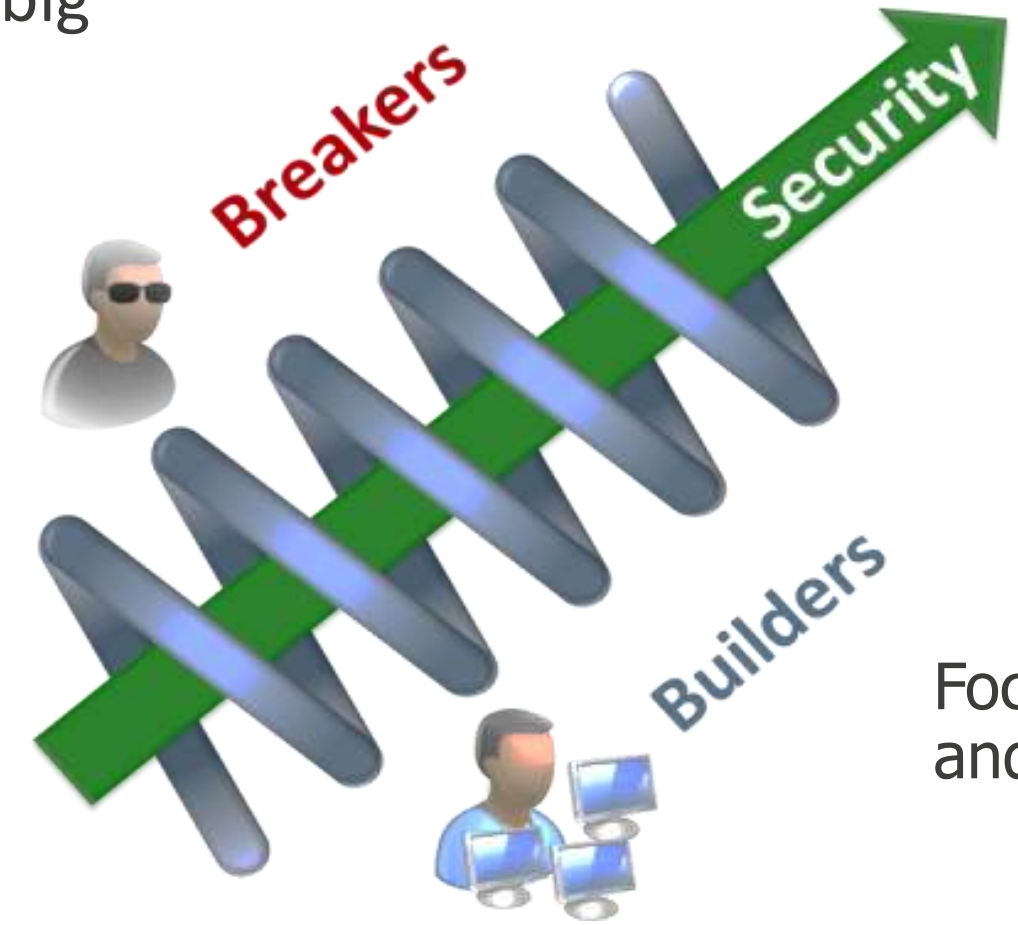
Testing for all the ways you might introduce XSS

Measure positive security directly from your running application

Testing to verify <u>your</u> XSS defense

THIRD WAY – ACCELERATE THE EVOLUTION OF YOUR SECURITY STORY

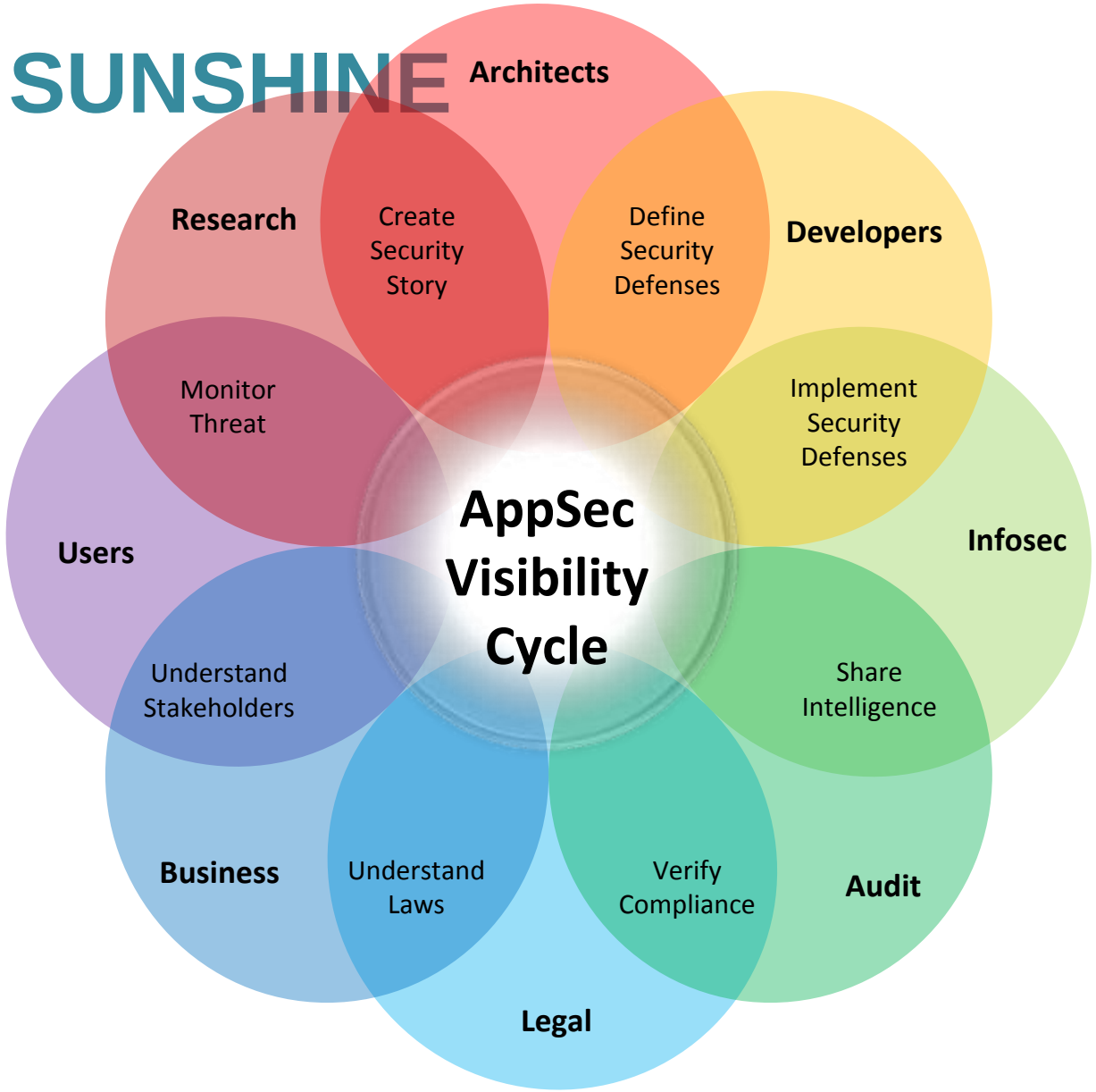
Celebrate new big risks without recrimination



The faster you cycle, the faster you get secure

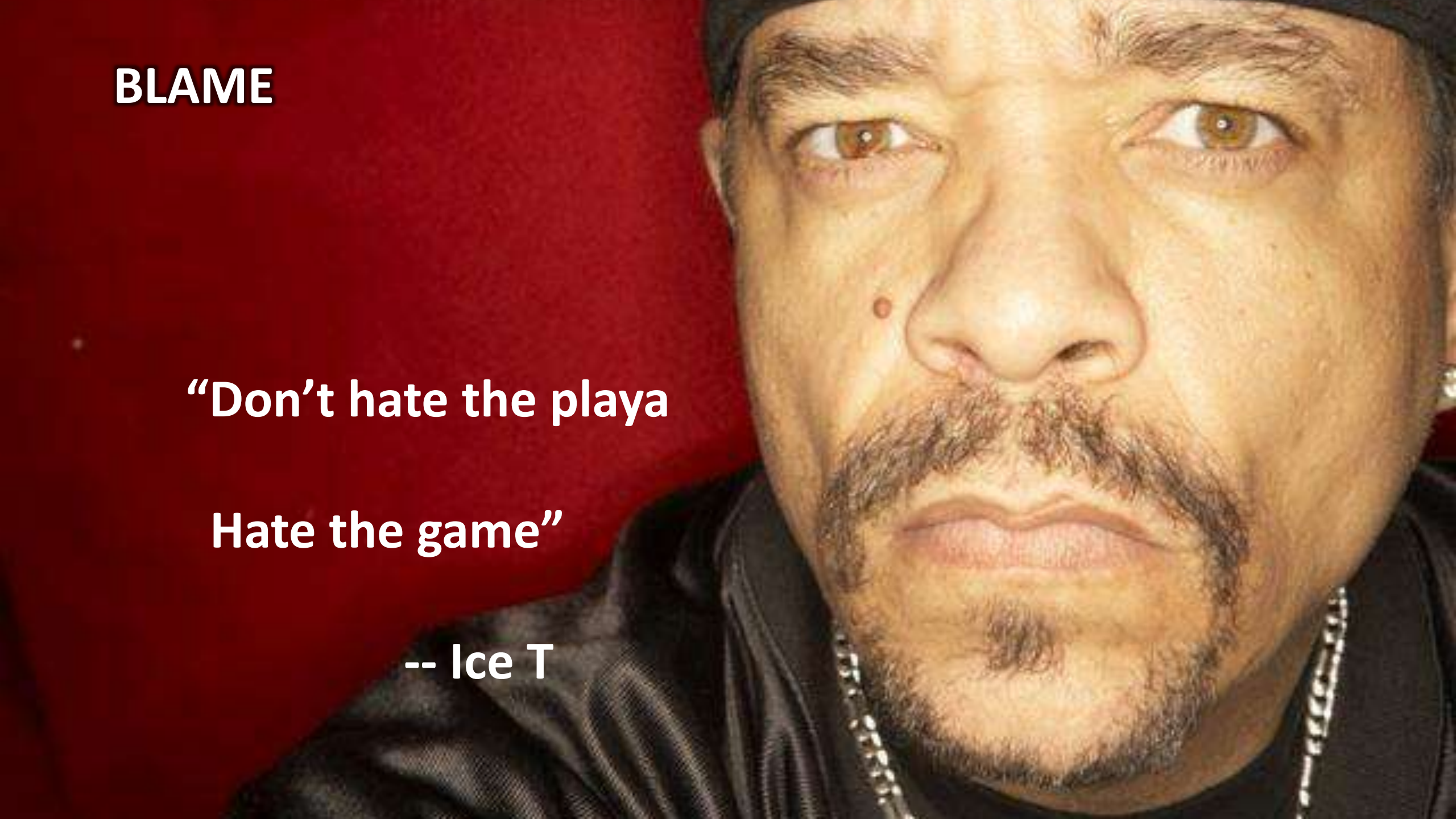
Focus on strength and simplicity

THIRD WAY – PROMOTE SECURITY IN SUNSHINE




TRUST
$495

BLAME



"Don't hate the playa

Hate the game"

-- Ice T

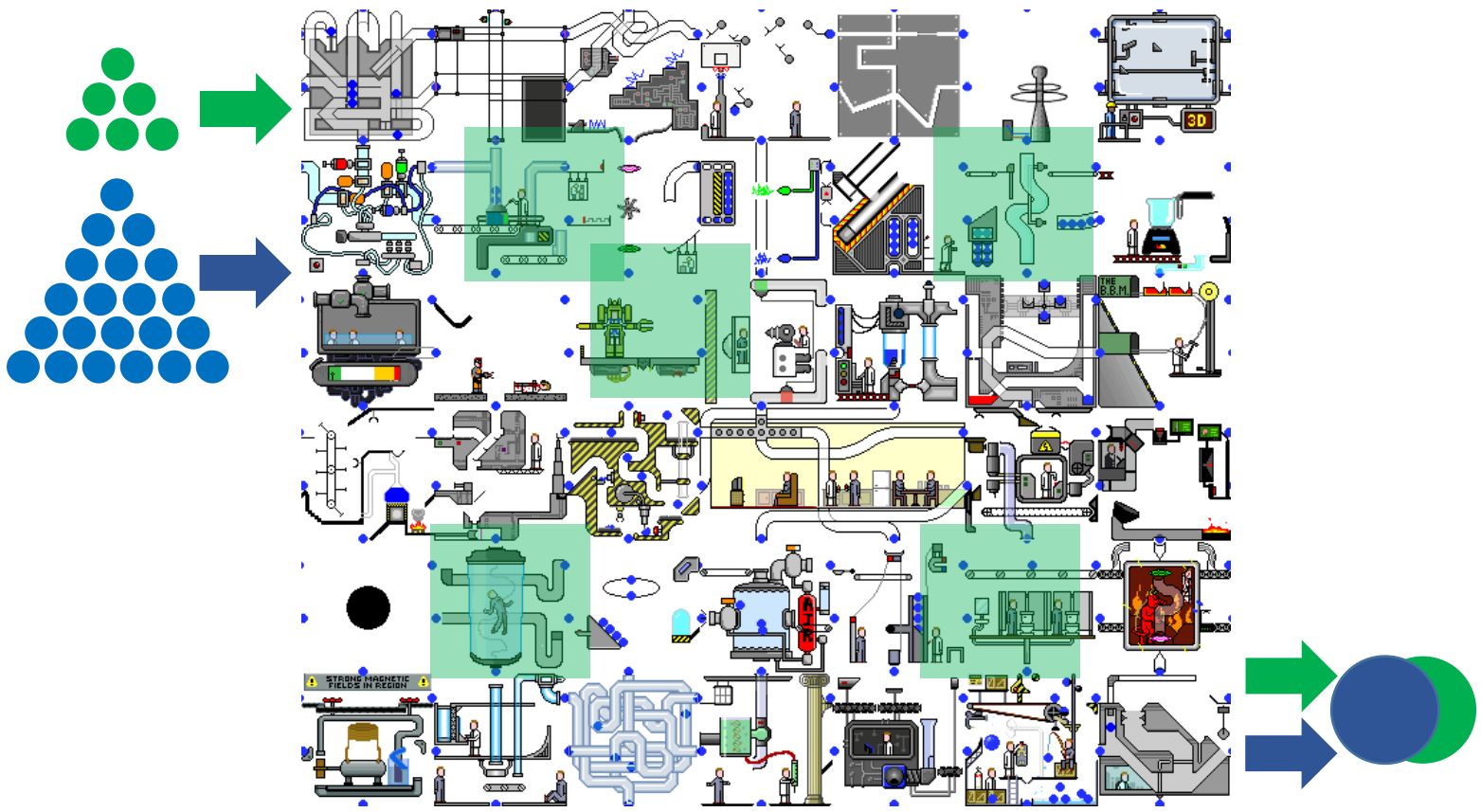

The first rule of security is…
HIDE
…You do not talk about security

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

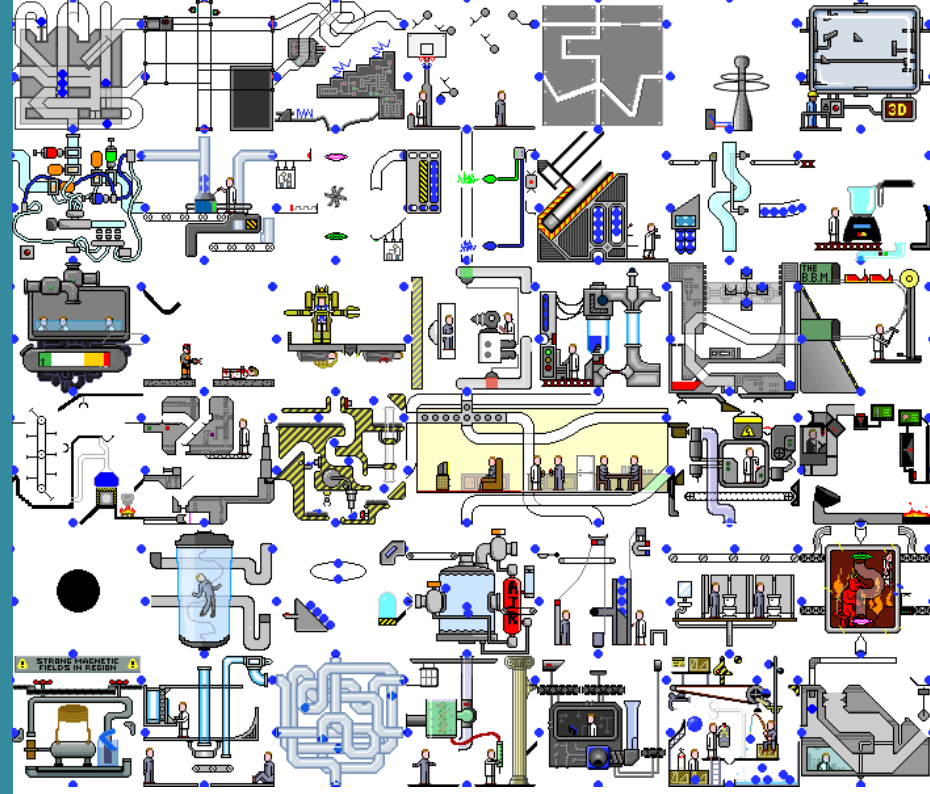


- Don’t focus on how to build software securely…
- Make software security into something you build!

Ask me anything.

@planetlevel

contrastsecurity.com



CONTRAST SECURITY

Gartner VISIONARY

FORRESTER LEADER

RED HERRING N. AMERICA 100 WINNER

RSAC Innovation Sandbox 2017 FINALIST

CYBER SECURITY EXCELLENCE AWARDS WINNER 2017

2016 SINET 16

CRN SECURITY 100

SC Awards Winner

2017 Cool Vendor Software Development Solution

TiE 50 2017 TOP START-UP