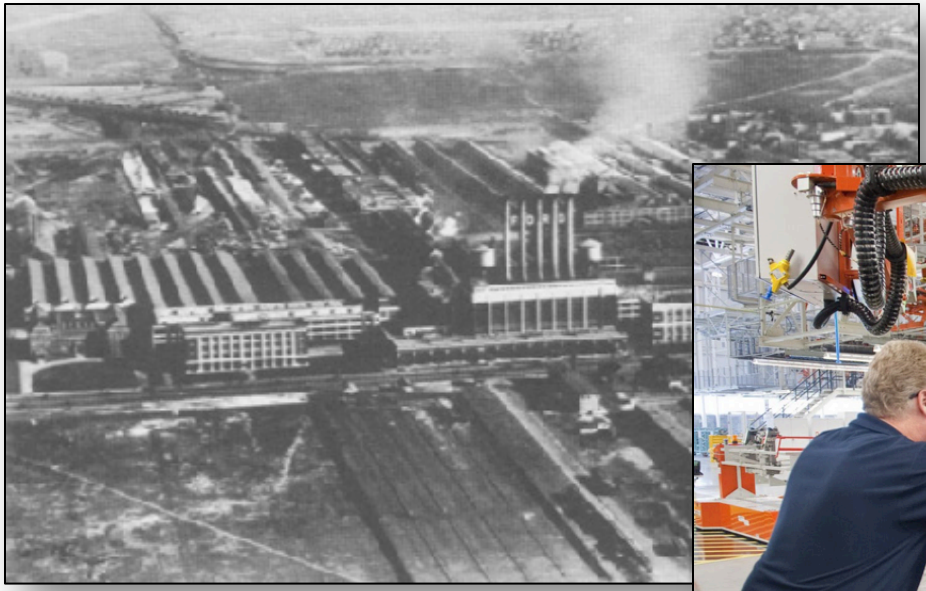
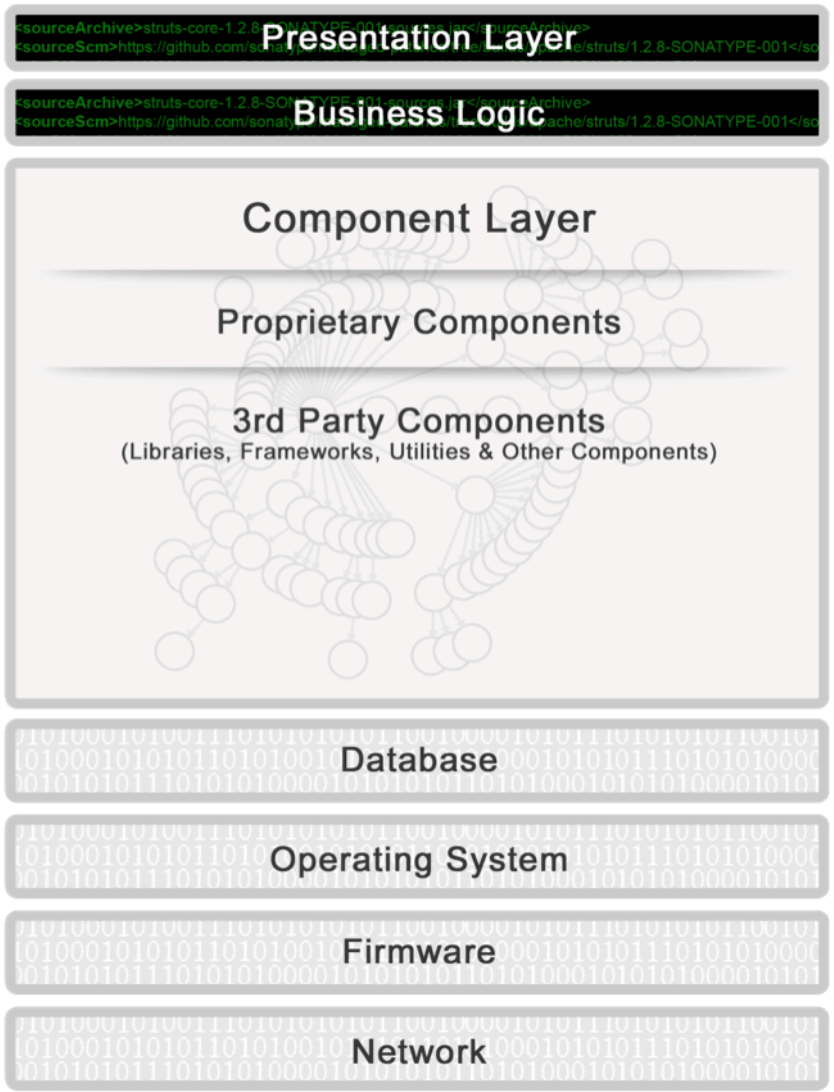
Removing the security and legal bottlenecks in a continuous world

What can we learn from other industries?

Brian Fox @brian_fox

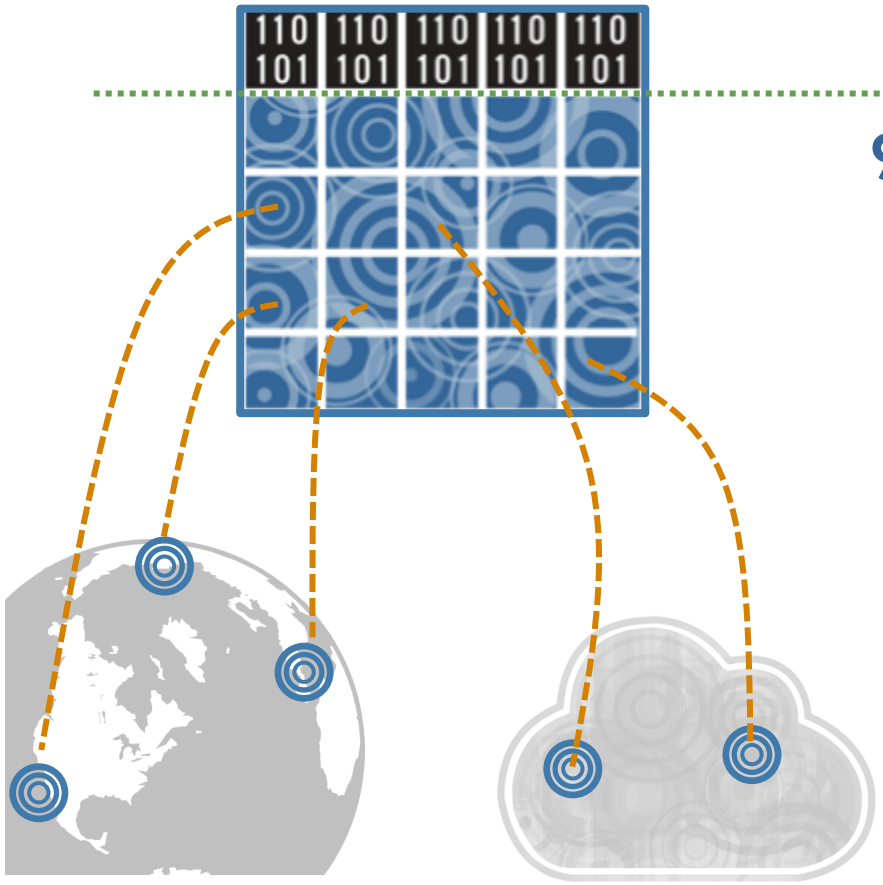
INDUSTRIAL EVOLUTION




Presentation Layer
Business Logic
Component Layer
Proprietary Components
3rd Party Components
(Libraries, Frameworks, Utilities & Other Components)
Database
Operating System
Firmware
Network

HOW DEPENDENT ON 3RD PARTIES ARE WE?

Typical Application



10% Custom Written Code

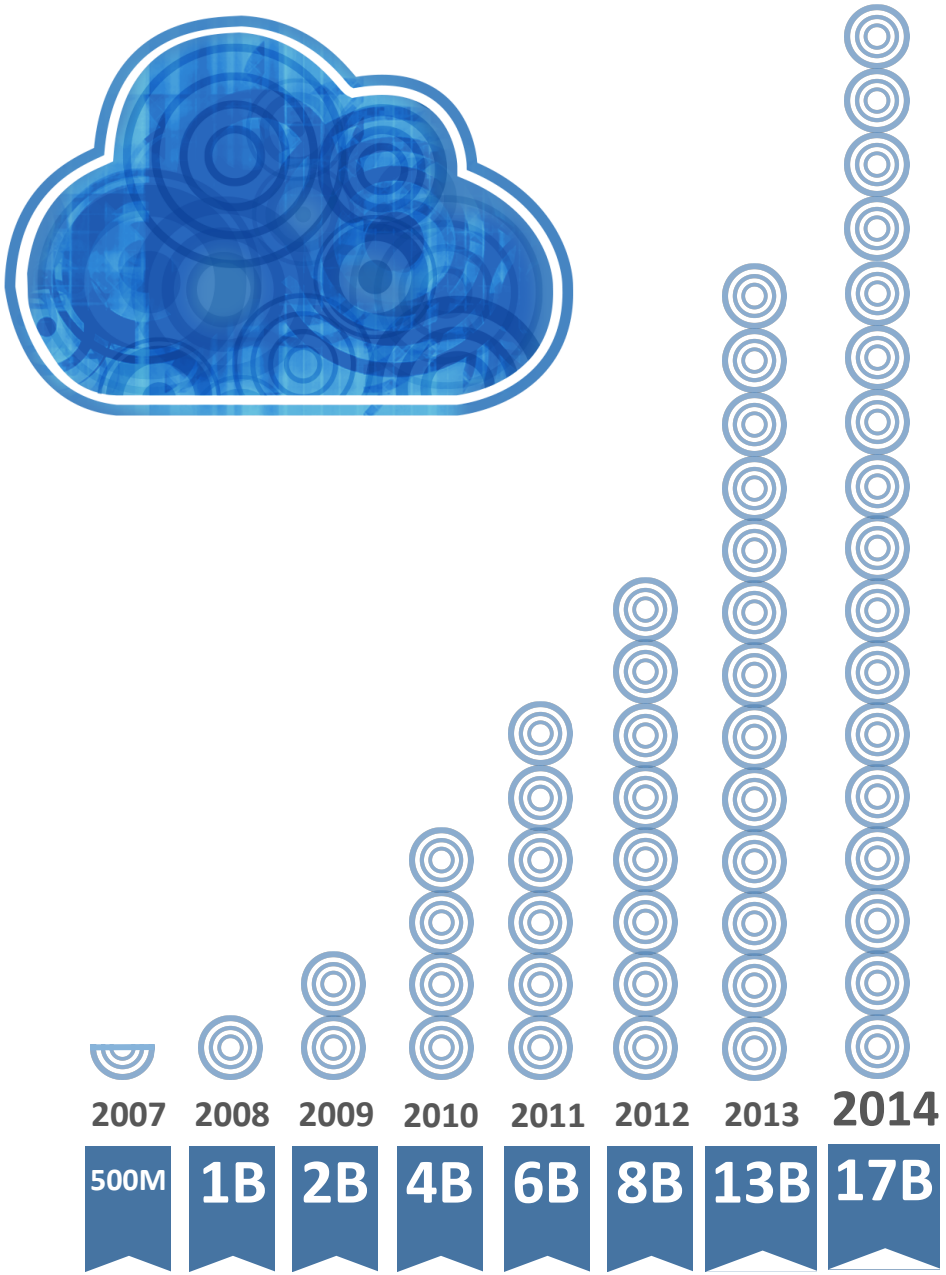
90% From 3rd Parties

Open Source

Closed Source

Cloud Services

Sonatype



Open source usage is

EXPLODING

Yesterday's custom code is now replaced with

OPEN SOURCE

components

Source: Sonatype, Inc. analysis of (Maven) Central Repository component requests.

Sonatype

ON ONE HAND WE AREN'T DOING ENOUGH

It just might get worse from here…

Security as evidence

KEY QUESTIONS

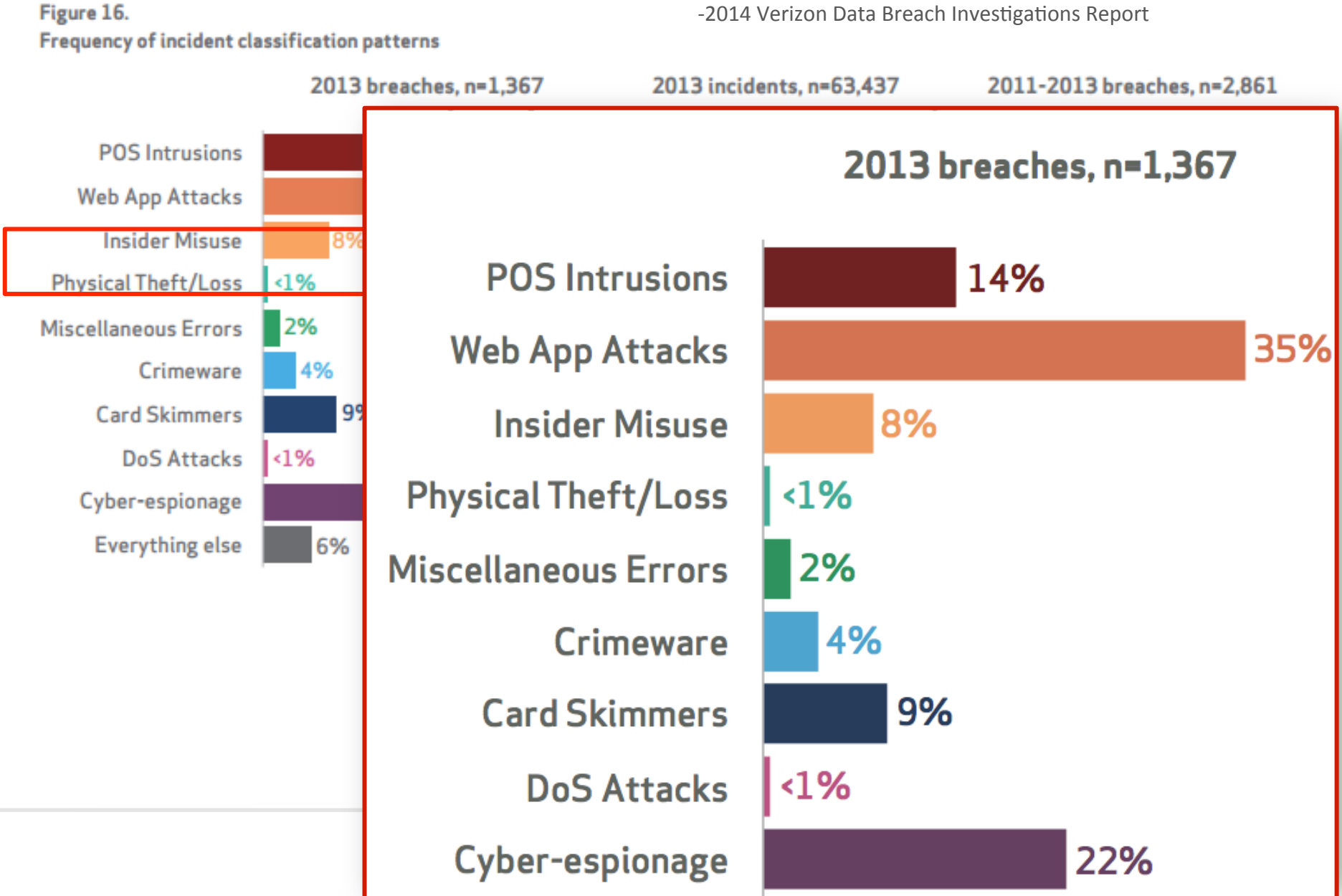
Where are Attackers most focused?

Where are Defenders most focused?

Which Activities have the most security impact?

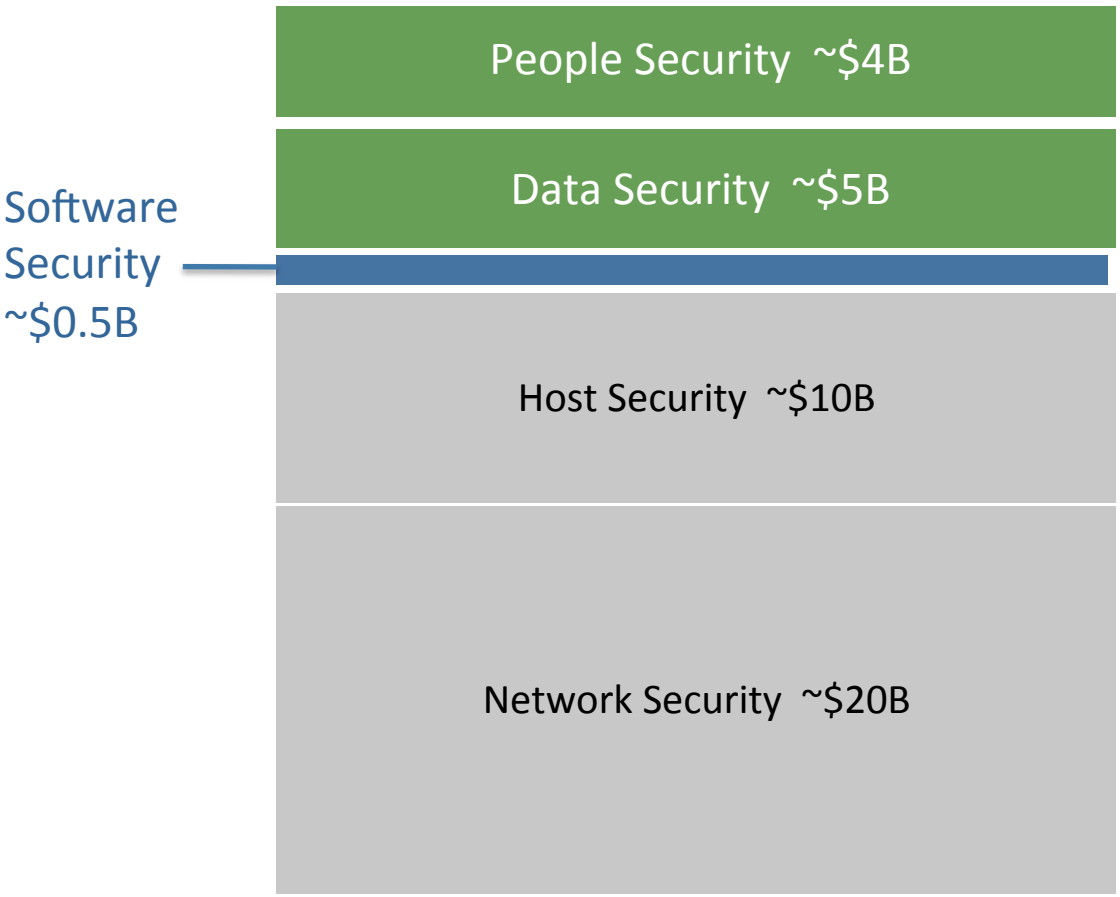
MOST ATTACKED: WEAK SOFTWARE IS #1 ATTACK VECTOR

-2014 Verizon Data Breach Investigations Report



LEAST SPENDING/PRIORITY: WEAK SOFTWARE

Software Security gets LEAST $ but MOST attacker focus

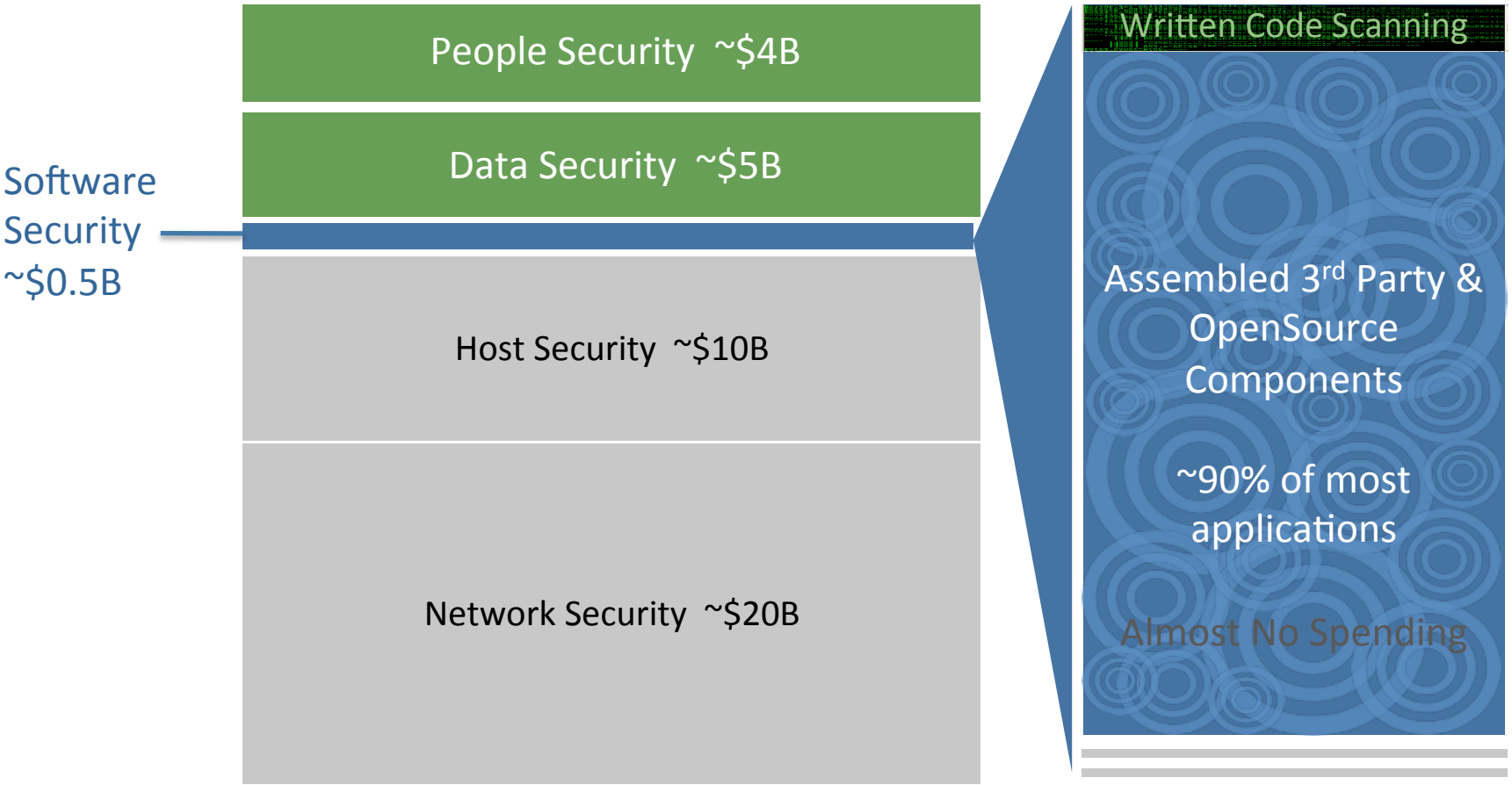


Source: Normalized spending numbers from IDC, Gartner, The 451 Group ; since groupings vary

LEAST SPENDING/PRIORITY: WEAK SW

Software Security gets LEAST $ but MOST attacker focus

Worse, within Software, existing dollars go to the 10% written



Source: Normalized spending numbers from IDC, Gartner, The 451 Group ; since groupings vary

Sonatype

MOST IMPACT: BUY/BUILD DEFENSIBLE SOFTWARE

THINK LIKE AN ATTACKER

When software was first being written, finding exploitable code was like

LOOKING

for a needle in a

HAYSTACK

THINK LIKE AN ATTACKER

Now that software is

ASSEMBLED…

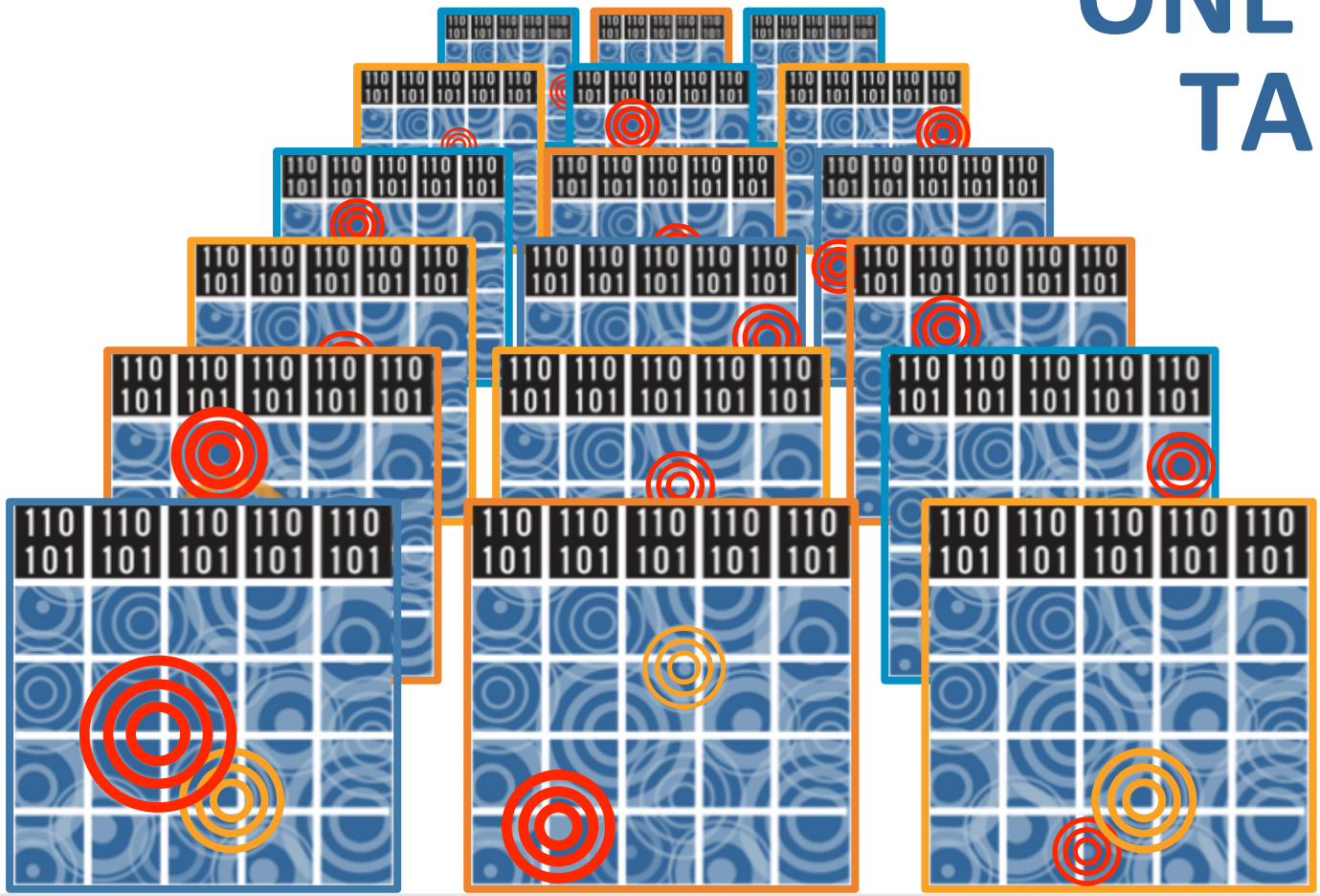
Our shared value becomes
our shared attack surface

Sonatype

THINK LIKE AN ATTACKER

One risky component,
now affects thousands of victims

ONE EASY TARGET



Java Cryptography API

CVSS v2 Base Score:

10.0 HIGH

Exploitability:

10.0

Since then

11,236

organizations downloaded it

214,484 times

Java HTTP implementation

CVSS v2 Base Score:

5.8 MEDIUM

Exploitability:

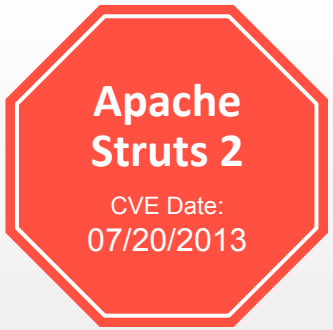
8.6

Since then

29,468

organizations downloaded it

3,749,193 times



Web application framework

CVSS v2 Base Score:

9.3 HIGH

Exploitability:

10

Since then

4,076

organizations downloaded it

179,050 times

 Source: Sonatype, Inc. analysis of (Maven) Central downloads and NIST National Vulnerability Database

Sonatype

STRUTS

Global Bank

Software Provider

Software Provider's Customer

State University

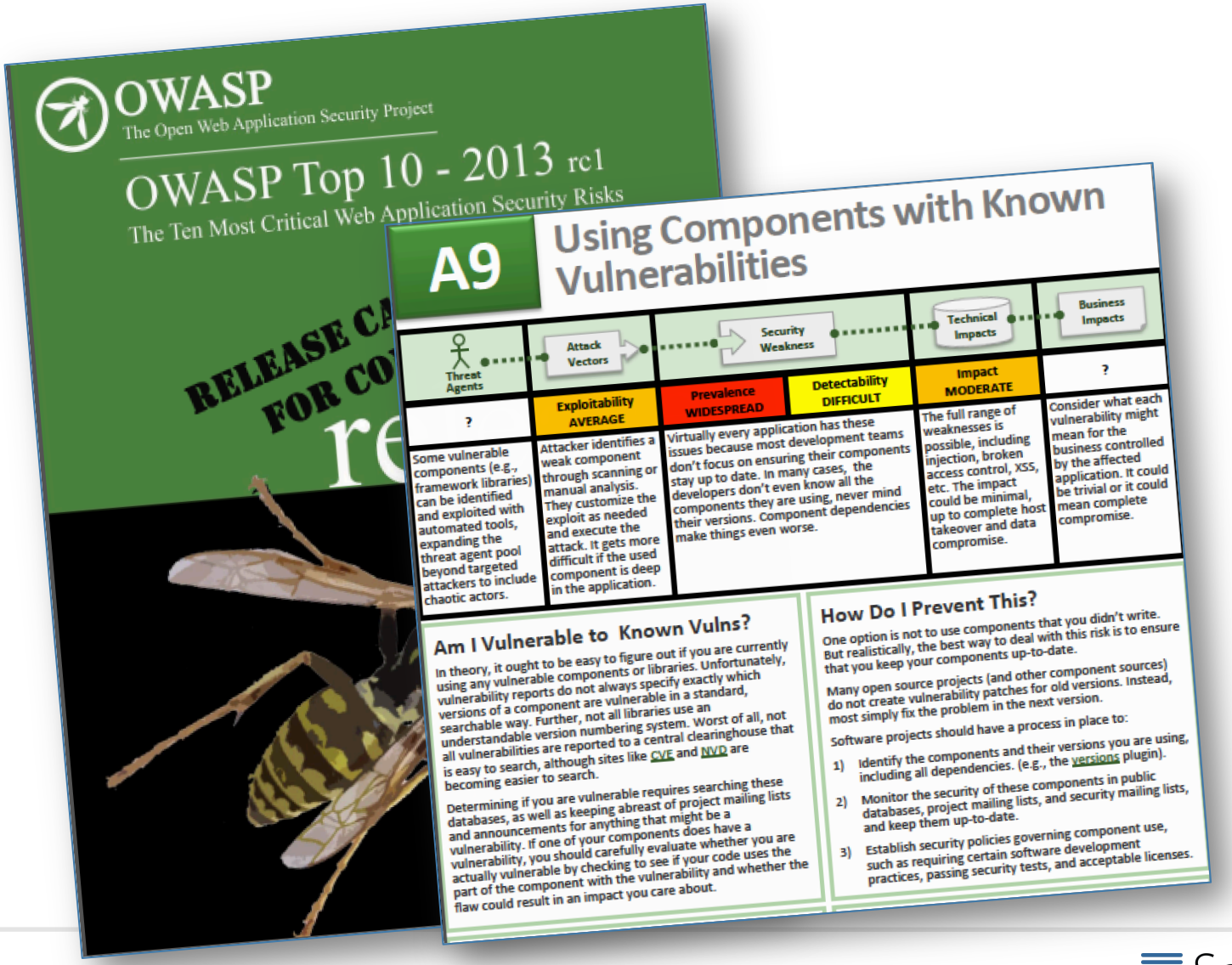
Three-Letter Agency

Large Financial Exchange

Hundreds of Other Sites

Sonatype

THOUGHT LEADERS ARE TAKING ACTION



Sonatype

WHY IS THIS SO HARD?

Modern software development

HAS CHANGED

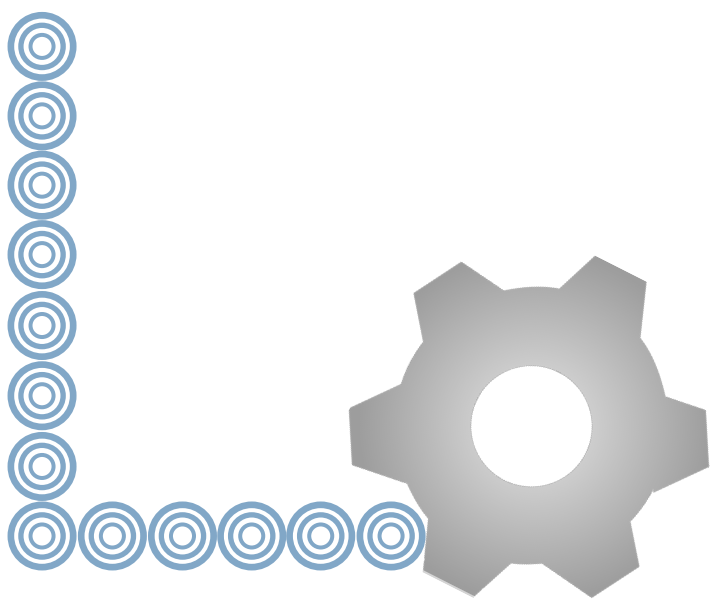
Our process

HASN'T CHANGED ENOUGH

Sonatype

Use of components creates a

SOFTWARE SUPPLY CHAIN



COMPONENT SELECTION

DEVELOPMENT

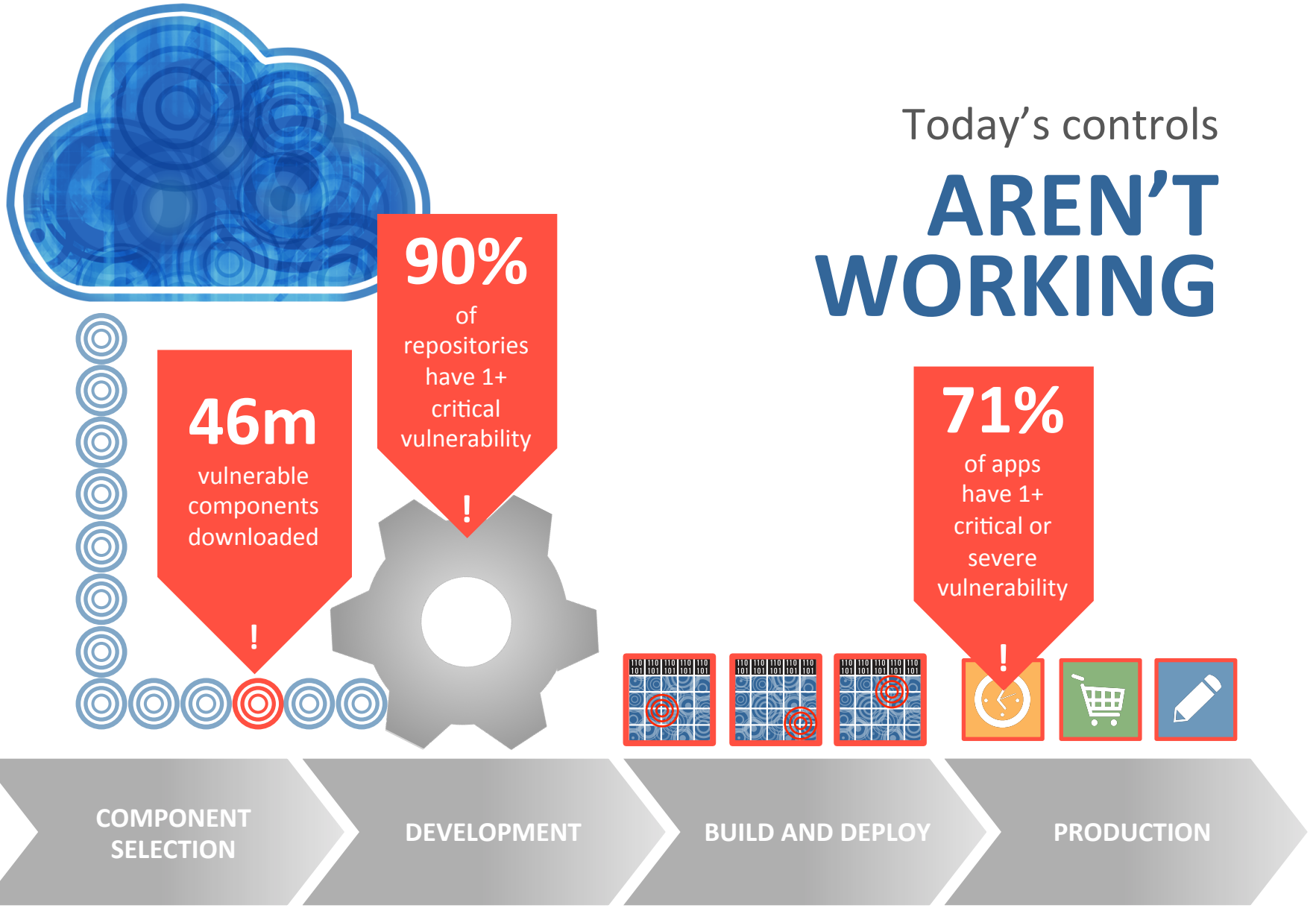
BUILD AND DEPLOY

PRODUCTION

Sonatype

Today's controls

AREN'T WORKING



Source: Sonatype, Inc. analysis based on Repository Healthchecks and Application Healthchecks used to determine component risk in repositories and applications.

Sonatype

THE NEW LIFECYCLE

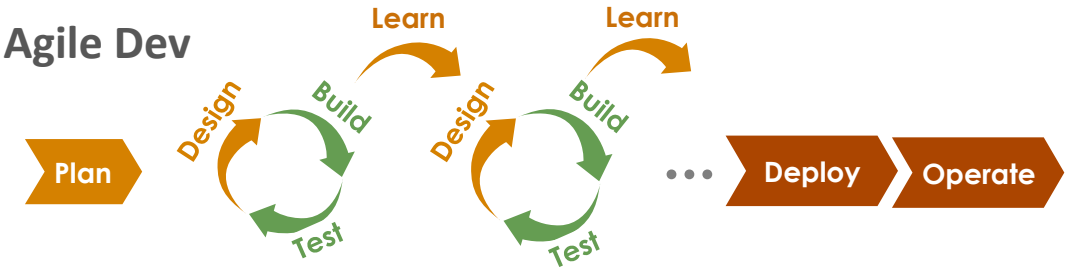
Impact on Releases per Year (Cycle Time)

Traditional Lifecycle (Waterfall)

1-2

Cycle Time: Months-Years

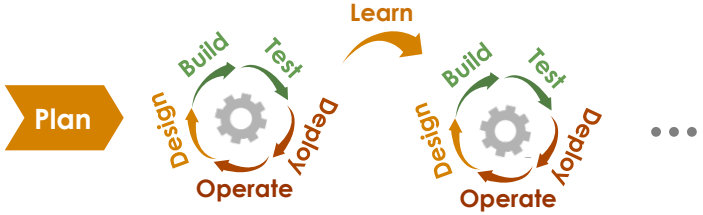
Agile Dev



10-20

Cycle Time: Days-Weeks

Modern Lifecycle (+DevOps, Continuous *)



100-200

Cycle Time: Minutes-Hours

Sonatype

THE NEW LIFECYCLE

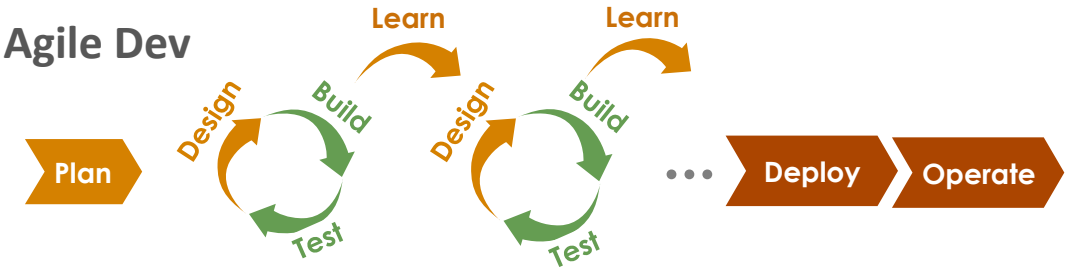
Governance?

Traditional Lifecycle (Waterfall)

Manual

Cycle Time: Months-Years

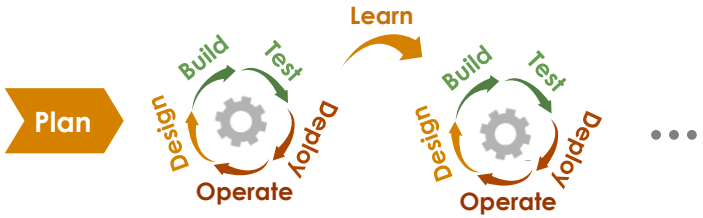
Agile Dev



Manual + Point Tools

Cycle Time: Days-Weeks

Modern Lifecycle (+DevOps, Continuous *)



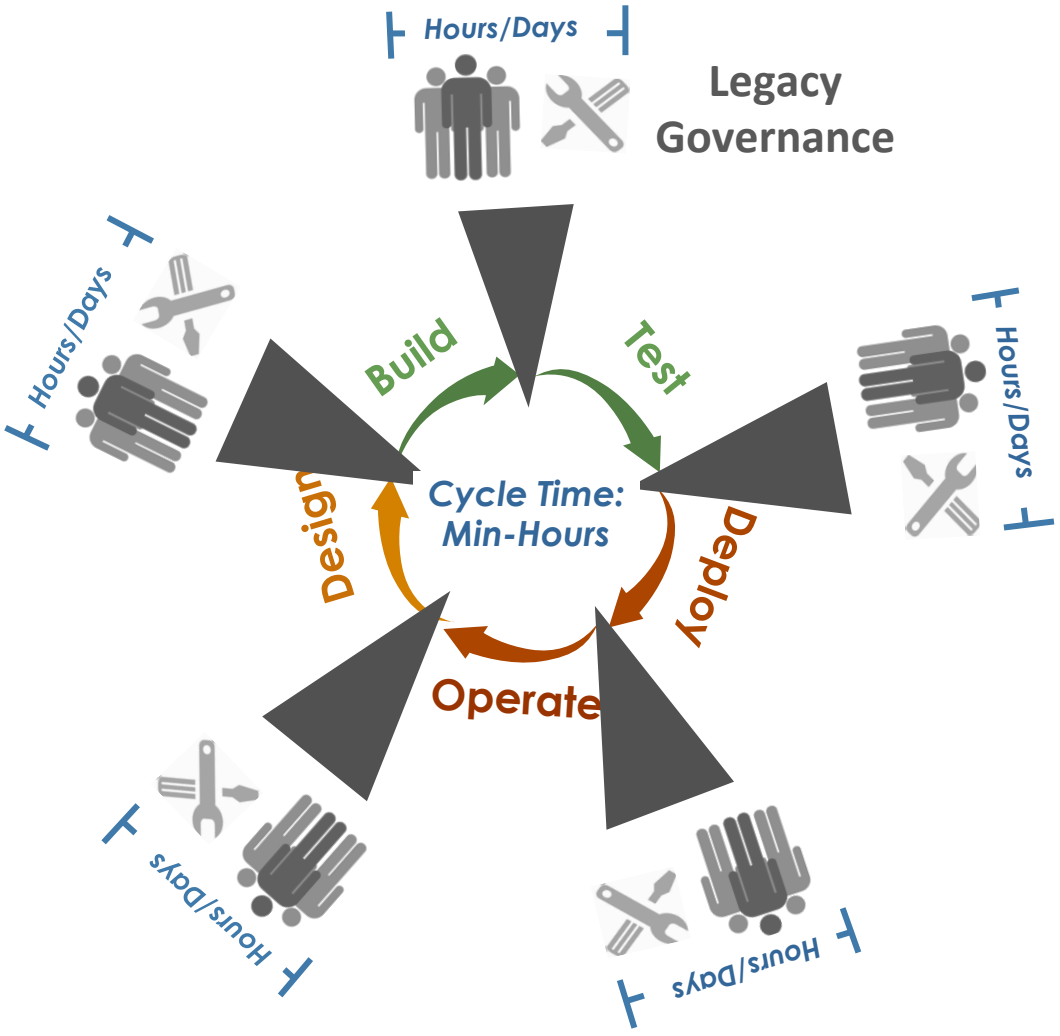
New Approach

Policy-Driven Automation

Cycle Time: Minutes-Hours

Sonatype

CYCLE TIME SQUEEZE



If it does not fit,
It does not get done.

- Work Arounds
- Batch Scans
- Rework
- Exposure

Go Fast ***OR*** Sleep at Night

Sonatype

ON THE OTHER HAND

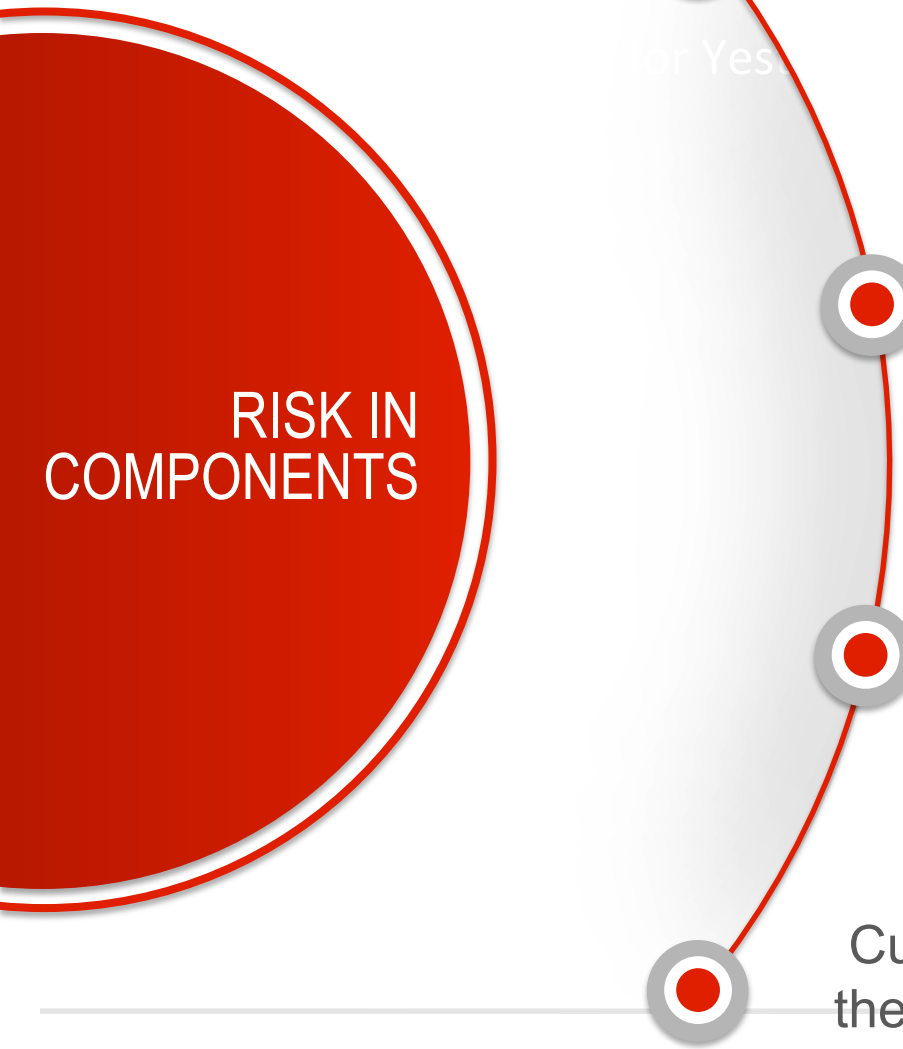
Anti Patterns

Ask someone first

(aka hurry up and wait)

Cut the cord!

Point fingers!



Component usage has **exploded**

Applications are the primary vector of **attack**

There is a proliferation of **flawed** components

Current approaches **can't handle** the complexity at speed

Sonatype

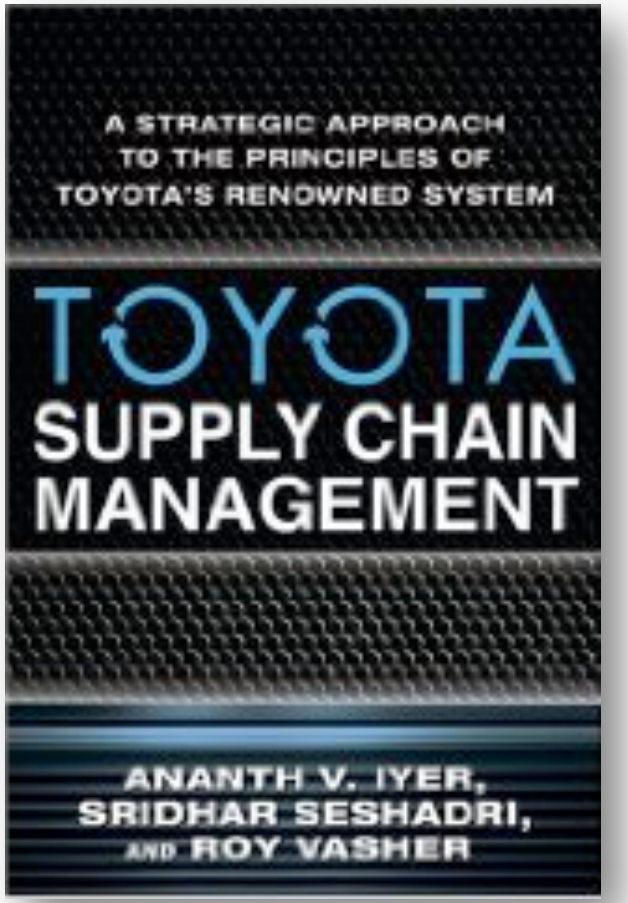
IT IS POSSIBLE TO ADDRESS SPEED AND QUALITY AT THE SAME TIME

We are not the first **INDUSTRY** to face this **CHALLENGE**

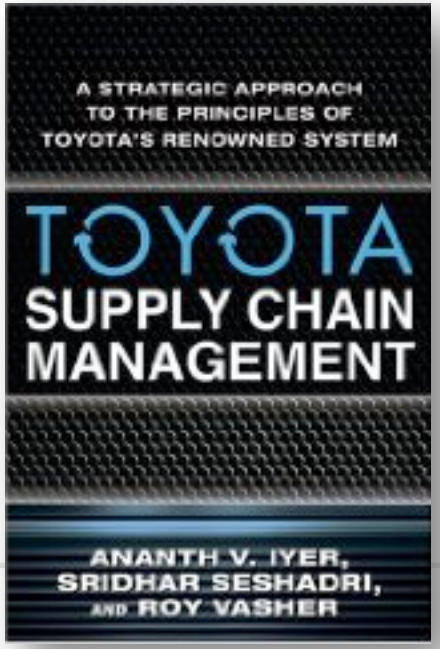
Sonatype

Comparing the Prius and Volt

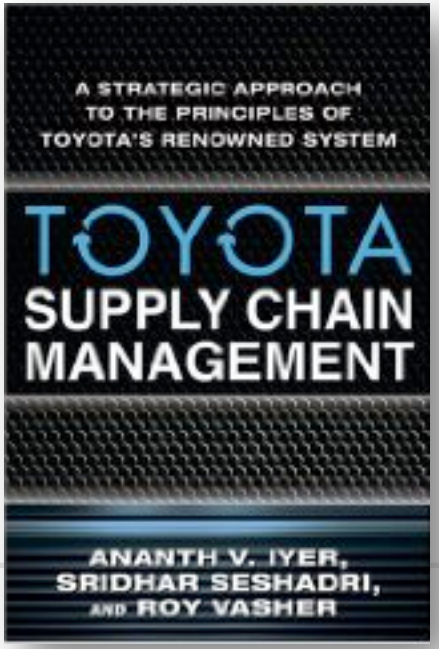
	Toyota Prius	Chevy Volt
Cost:	$24,200	$39,900
Units per month:	23,294	1,788
Plant Suppliers	125	800
Firm-Wide Suppliers	224	5,500
In-House Production	27%	54%



- Variety of products offered
- Velocity of product flow
- Variability of outcomes against forecast
- Visibility of processes to enable learning



- Variety of *software produced*
- Velocity of *software delivery*
- Variability of outcomes against forecast
- Visibility of processes to enable learning



Create Awareness

Empower

Govern

Monitor

Create Awareness

"Unless problems are seen, they will not be solved. Systems need to be in place to report ideas, problems, deviations, and potential issues with no delay."

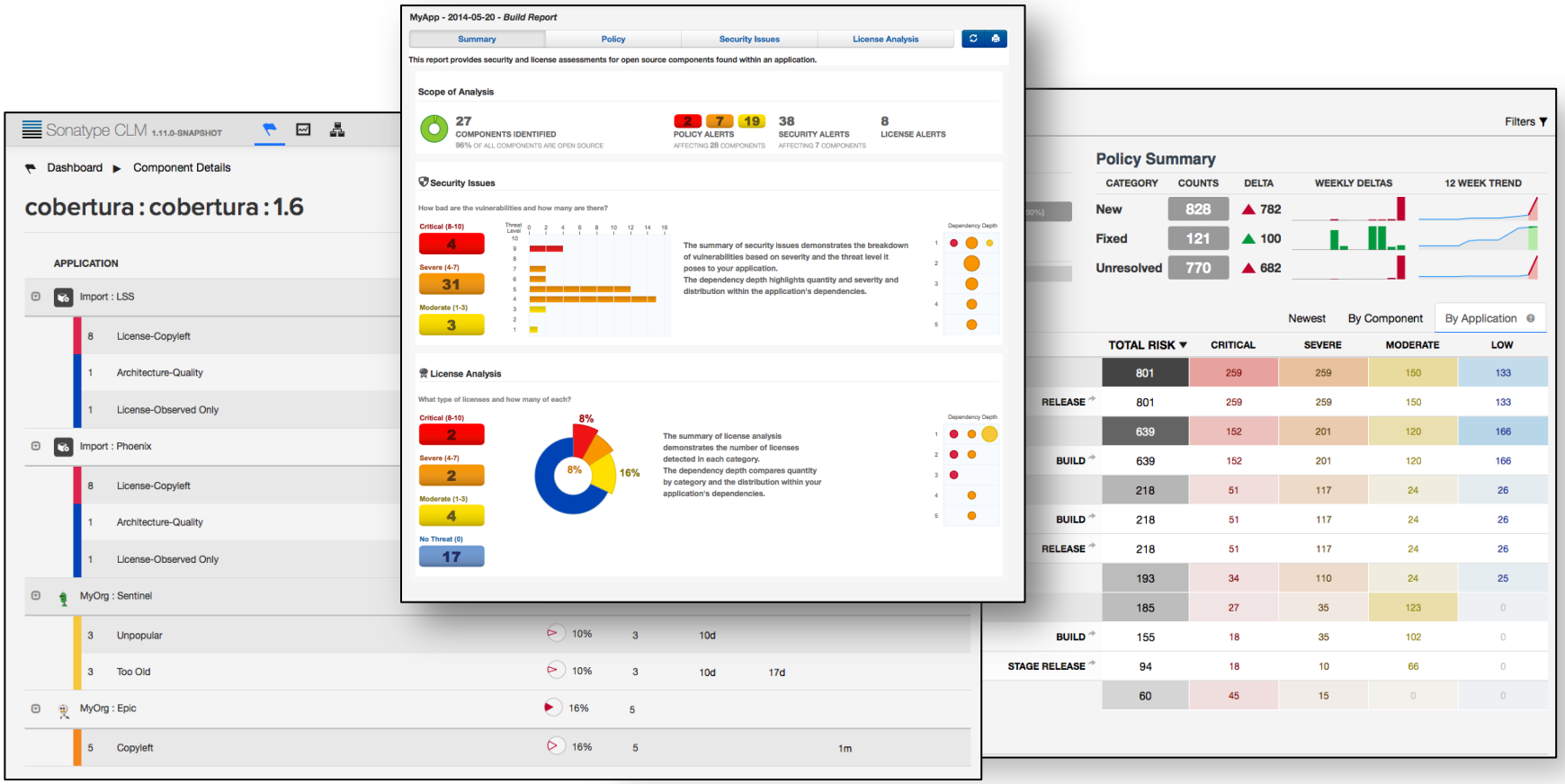
Fast so it can be

Continuous

Focus on the attributes so it can be automated

EASY TO CONSUME

Provide stakeholders actionable, easy to consume information to remediate problems



Sonatype

Empower

"Unless someone is capable of solving a problem that might arise within the boundaries set for him or her, that person will be unable to contribute to the problem solving process."

Since it's fast and automated everyone is on the same page

Precise

BE SPECIFIC

No Noise!

- There is a world of difference between saying "Struts is approved" and saying "Struts 2.3.16.1 is **good** and ~~Struts 2.3.15.0~~ ANY OLDER VERSION will **get your system owned**“

Scan found 50,313 “issues” →

Real issue count: 204 →

Contextual Results

WHY CONTEXT MATTERS

- SQL Injection vulnerabilities don't affect applications without databases.
- CopyLeft may not be a problem for internal applications or services.
- I need information that applies to my application.

Actionable

PROVIDE A SOLUTION

- Now that you've told me about a problem, tell me what I can do to fix it.
- Suggest alternatives.
- Even if I don't completely understand the risk,

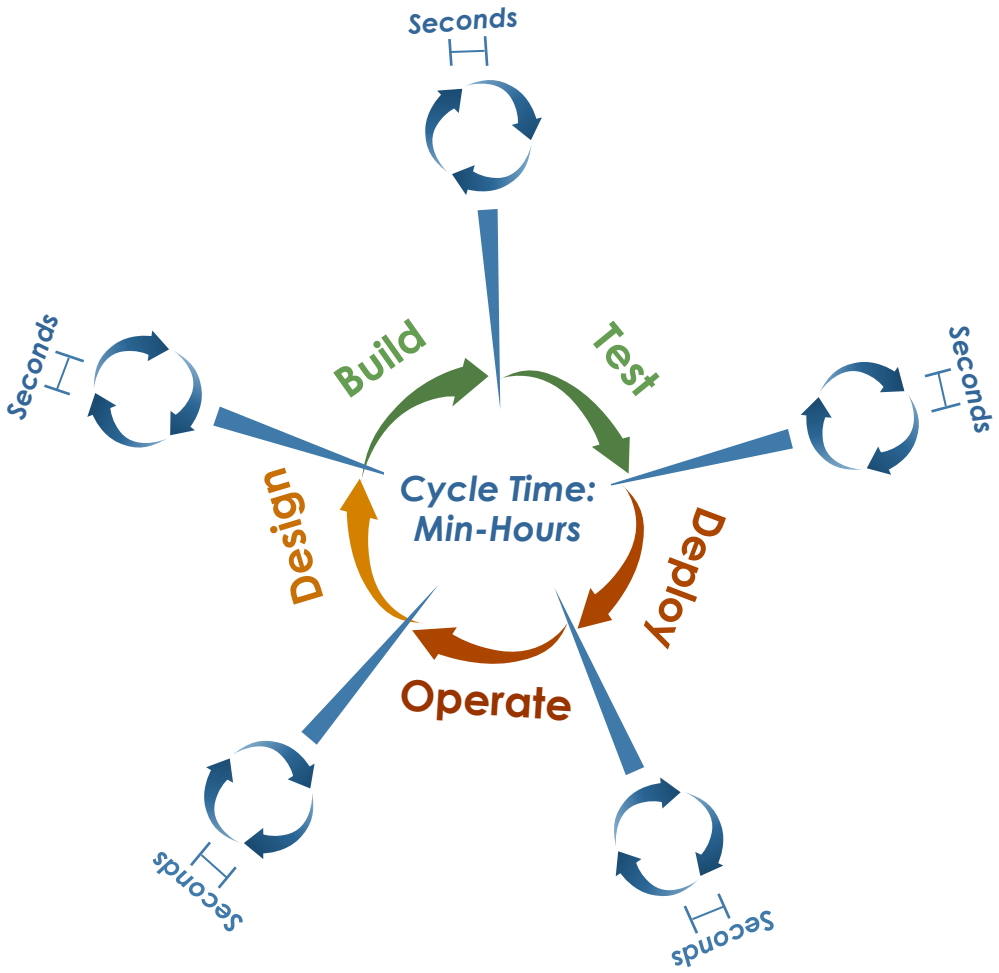
  if you show me an easy fix, I will take it.

Govern

"Actions have to be taken within a set of constraints, and they must conform to certain standards."

Across the lifecycle

CYCLE TIME SYNERGY



Continuous Governance for Continuous Delivery

- No Interruption
- Entire Lifecycle
- Solve Early
- Avoid Rework

Go Fast ***AND*** Sleep at Night

Sonatype

The ability to govern in an automated way clears roadblocks

Monitor

"As experience with solving problems is obtained, greater awareness of other areas that might be affected needs to be created."

Monitor process improvements and refine

Know where components are used to you can respond

Applications don't age like wine,

THEY ROT LIKE MILK

System.exit(0);

Questions?

Sonatype