RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

The Game of Hide and Seek, Hidden Risks in Modern Software Development

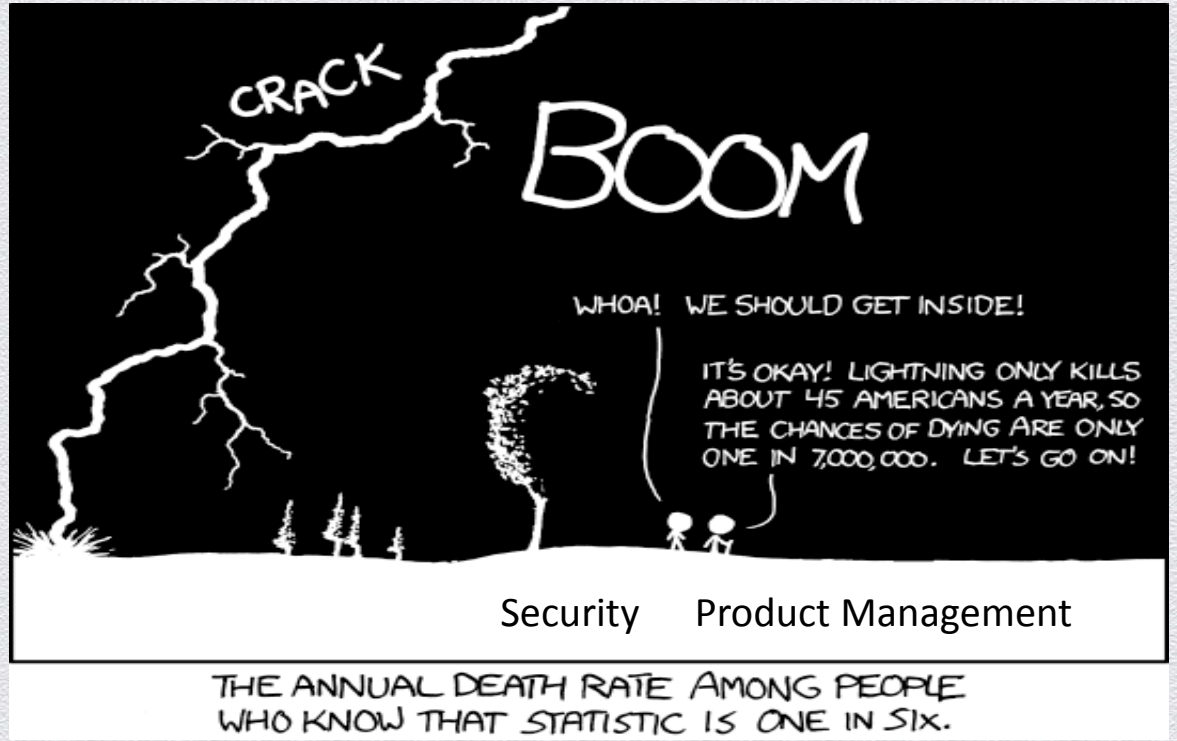
SESSION ID: ASEC-R02

Ryan Berg
CSO
Sonatype
@ryanberg00

Agenda

- The changing dynamics surrounding application security
- Why this is a supply chain problem
- What should you be doing, but likely aren't
- Q&A

The Language of Security is Risk



http://xkcd.com/795/

What is Risk?

What does the snail tell us?



"…WE OWE A DUTY OF REASONABLE CARE TO OUR NEIGHBOR"

Lord Atkin: Donoghue v. Stevenson (1932)

You Built It, Your Responsible

“…a manufacturer of products, which he sells in such a form as to show that he intends them to reach the ultimate consumer in the form in which they left him with no reasonable possibility of intermediate examination, and with knowledge that the absence of reasonable care in the preparation or putting up of products will result in an injury to the consumer's life or property, owes a duty to the consumer to take that reasonable care.”

What is Risk?

United States v. Carroll Towing Co.
159 F.2d 169 (2d. Cir. 1947)

The cost of Doing nothing can't be ignored

"…IF THE PROBABILITY BE CALLED P; THE INJURY, L; AND THE BURDEN, B; LIABILITY DEPENDS UPON WHETHER B IS LESS THAN L MULTIPLIED BY P: I.E., WHETHER B < PL".

Translation: If the Cost of Protecting Against Harm is less than the Cost of the Damage Multiplied by the Likelihood of the Damage, then there is **negligence**.

Risk = probability x impact

Modern software development

HAS CHANGED

Application security

HASN'T CHANGED ENOUGH

Modern software development

HAS CHANGED

Application security

HASN'T CHANGED ENOUGH

Sonatype

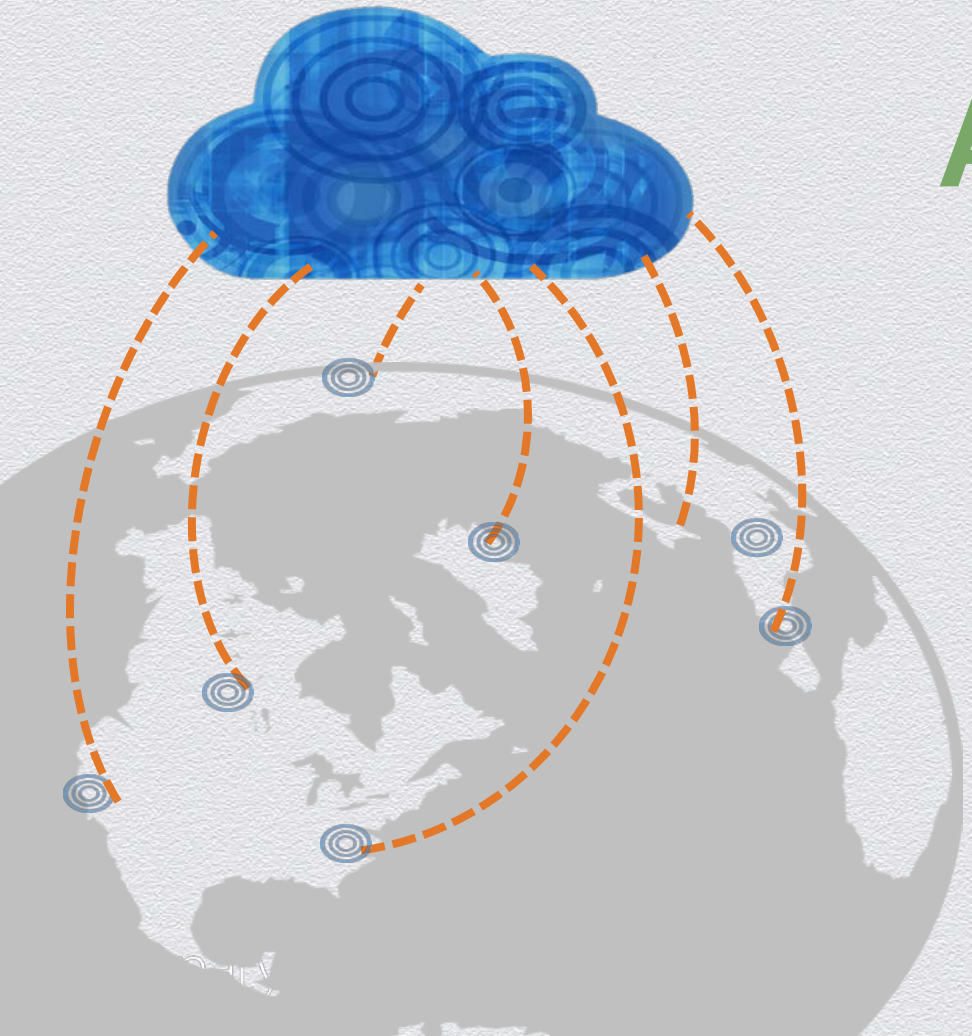
#RSAC

RSACONFERENCE2014

Modern software development **HAS CHANGED**

Application security

HASN'T CHANGED ENOUGH

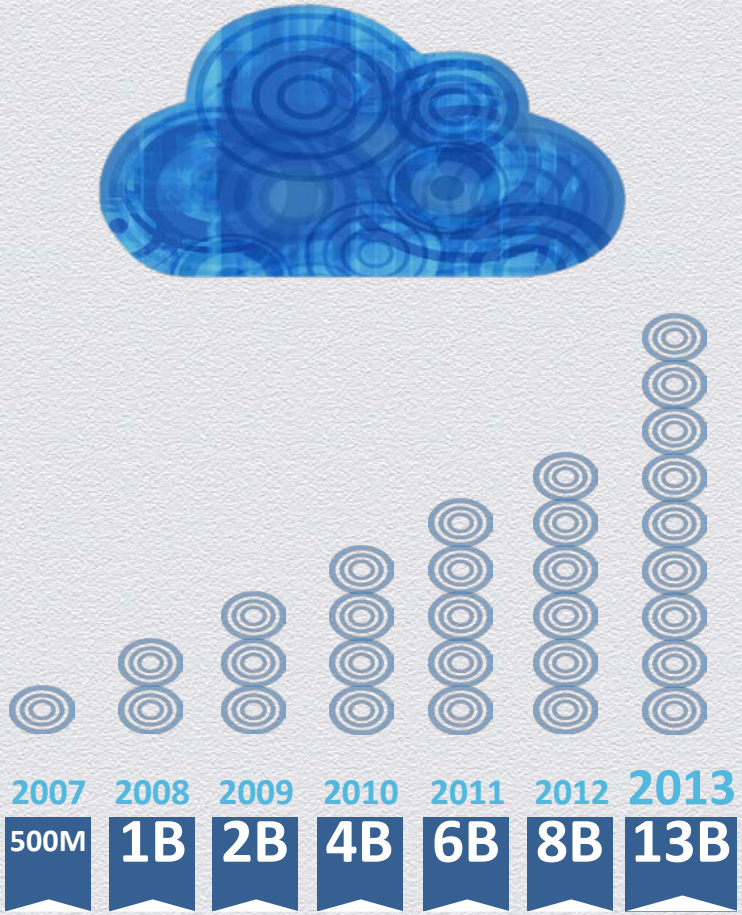


APPLICATIONS

are assembled using
third party “components,”
most of which are open source

In fact, **90%**

of a typical application
is open source



Open source usage is

EXPLODING

Yesterday's source code is today's

OPEN SOURCE

Sonatype

#RSAC

RSACONFERENCE2014

Creating today's software

SUPPLY CHAIN

COMPONENT SELECTION → DEVELOPMENT → BUILD AND DEPLOY → PRODUCTION

Sonatype

#RSAC

RSACONFERENCE2014

Do you know who your

SUPPLIERS ARE?

COMPONENT SELECTION → DEVELOPMENT → BUILD AND DEPLOY → PRODUCTION

Sonatype

#RSAC

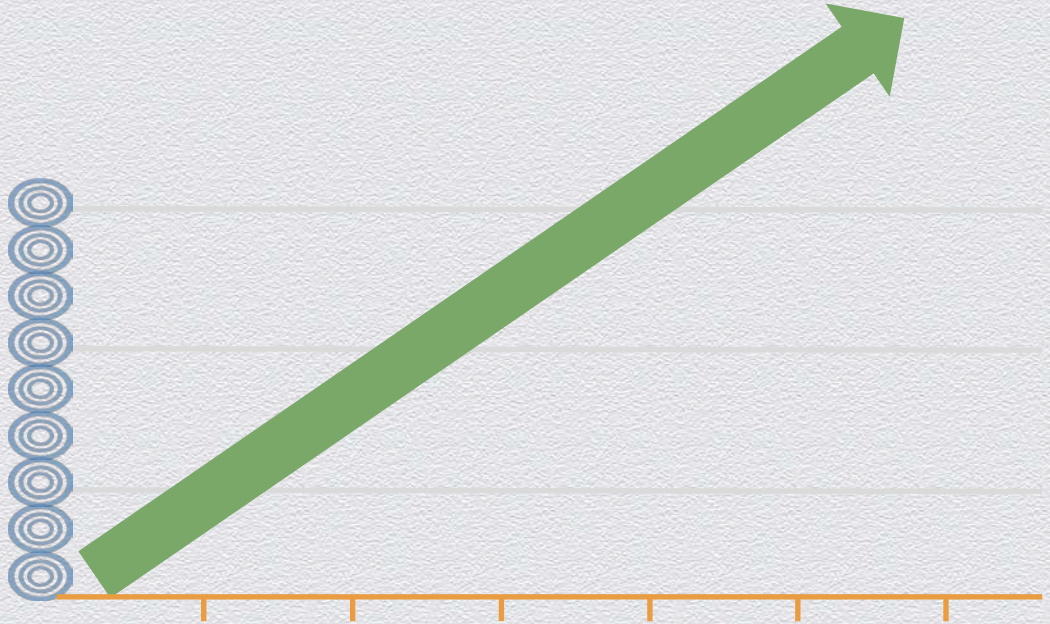
RSACONFERENCE2014

OPEN SOURCE:

QUALITY

INNOVATION

EFFICIENCY



Sonatype

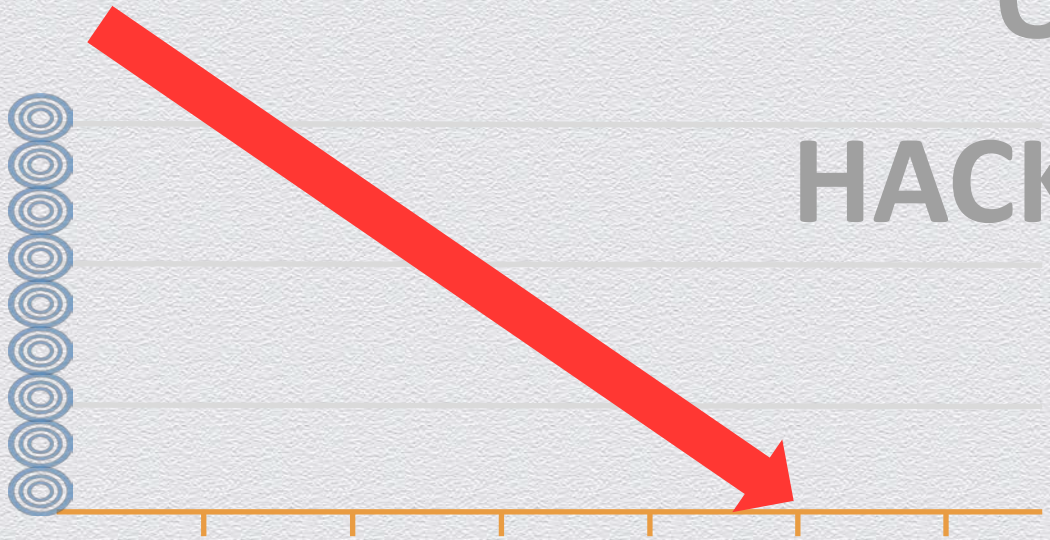
#RSAC

RSACONFERENCE2014

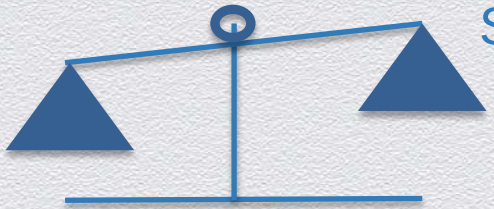
NO CONTROLS.

OPEN ACCESS.

HACKER TARGETS.



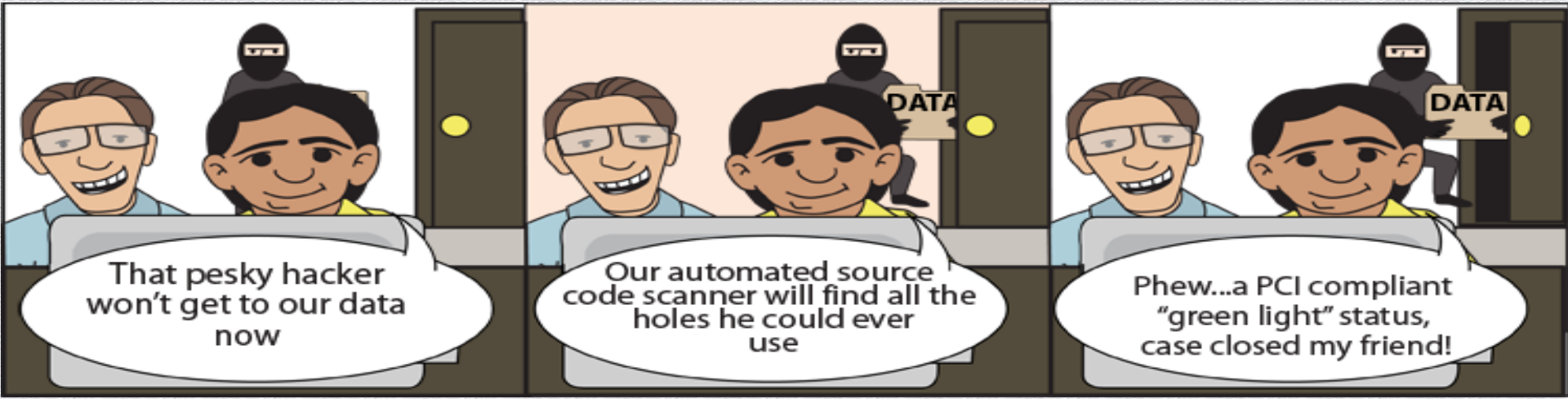
Security spans the Enterprise



Security concerns are across the Enterprise

Development	Operations	Security
Features	Performance	Security
Usability	Reliability/Scalability	Compliance
Performance	Compliance	Everything Else
Reliability/Scalability	Security	
Maintainability	Maintainability	
Security	Features/Usability	
Compliance		

Haven't We Learned Compliant Does Not Mean Secure, Often the Opposite



A disproportionate spend against the risk

Prevention	Detection	Monitoring
Firewall	IDS	SIEM
Encryption	SAST	DAM
IPS	DAST	RAST
WebApp Firewall (WAF)		

Evolution of Spend

A Sea Change in Application Development

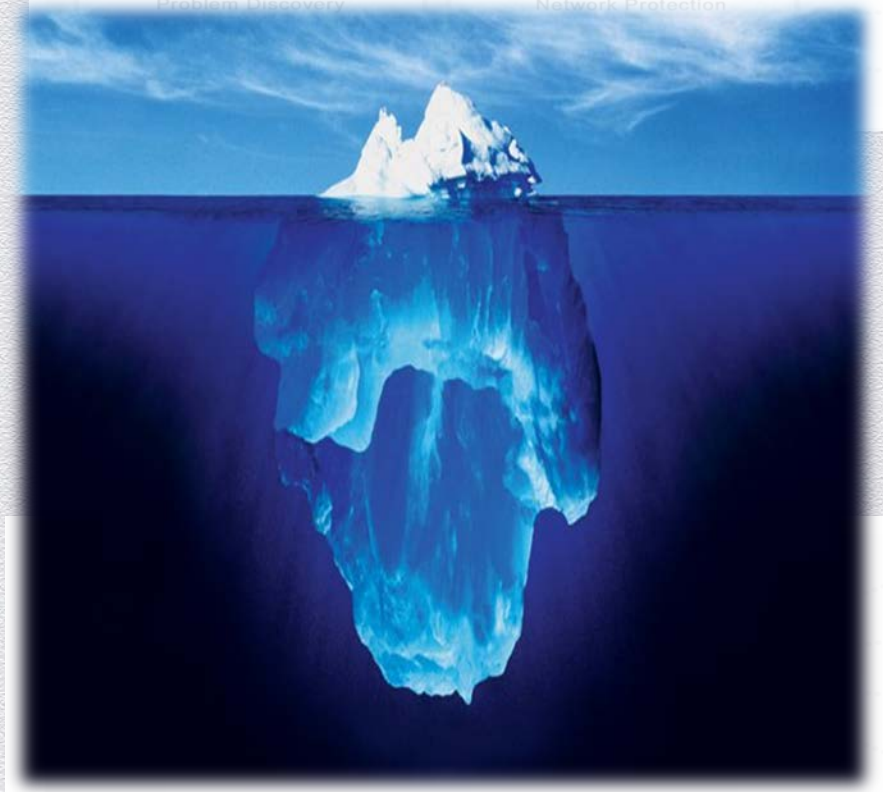
Written

Assembled **90%**

Source: 2012 / 2013 Sonatype analysis of more than 1,000 enterprise applications

What me worry, tis' just a bit of floating ice

Components are a hidden risk



Presentation Layer

Business Logic

Component Layer

Proprietary Components

3rd Party Components
(Libraries, Frameworks, Utilities & Other Components)

Database

Operating System

Firmware

Network

Sonatype

What are you doing to **ADDRESS THIS RISK?**

What are you doing to **ADDRESS THIS RISK?**

FOSS Review Board

Golden repository

Scans post development

Approval workflow

FOSS Review Board

NOTHING?

Golden repository

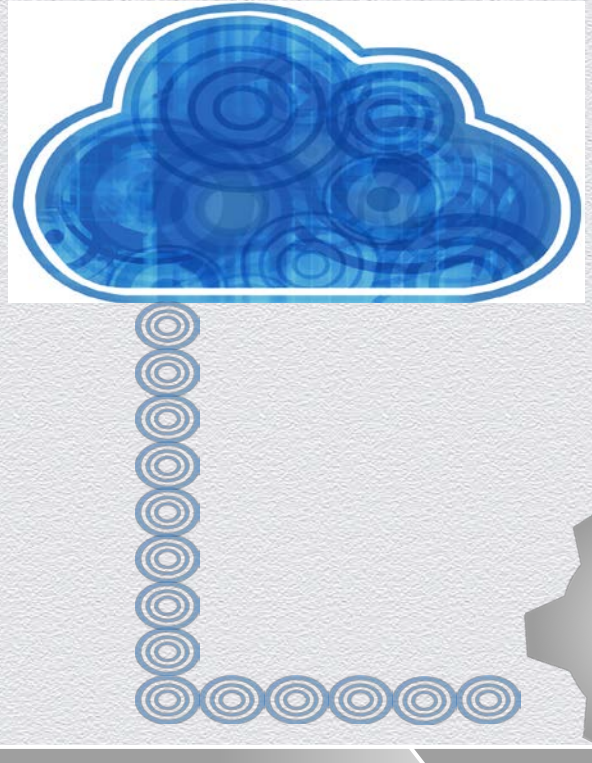
Scans post development

Approval workflow

Sonatype

#RSAC

RSACONFERENCE2014

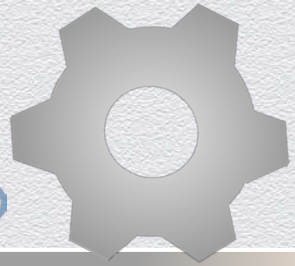


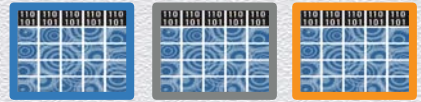
If you're not using secure

COMPONENTS

you're not securing your

APPS

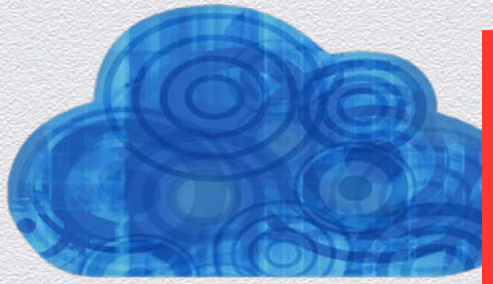




COMPONENT SELECTION → DEVELOPMENT → BUILD AND DEPLOY → PRODUCTION

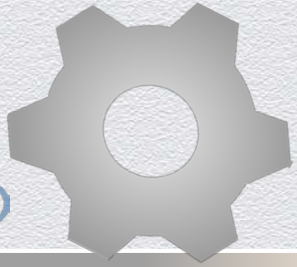
Sonatype

Today's approaches AREN'T WORKING

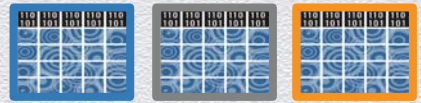


90% of repositories have 1+ critical vulnerability !

46m vulnerable components downloaded !



71% of apps have 1+ critical or severe vulnerability !

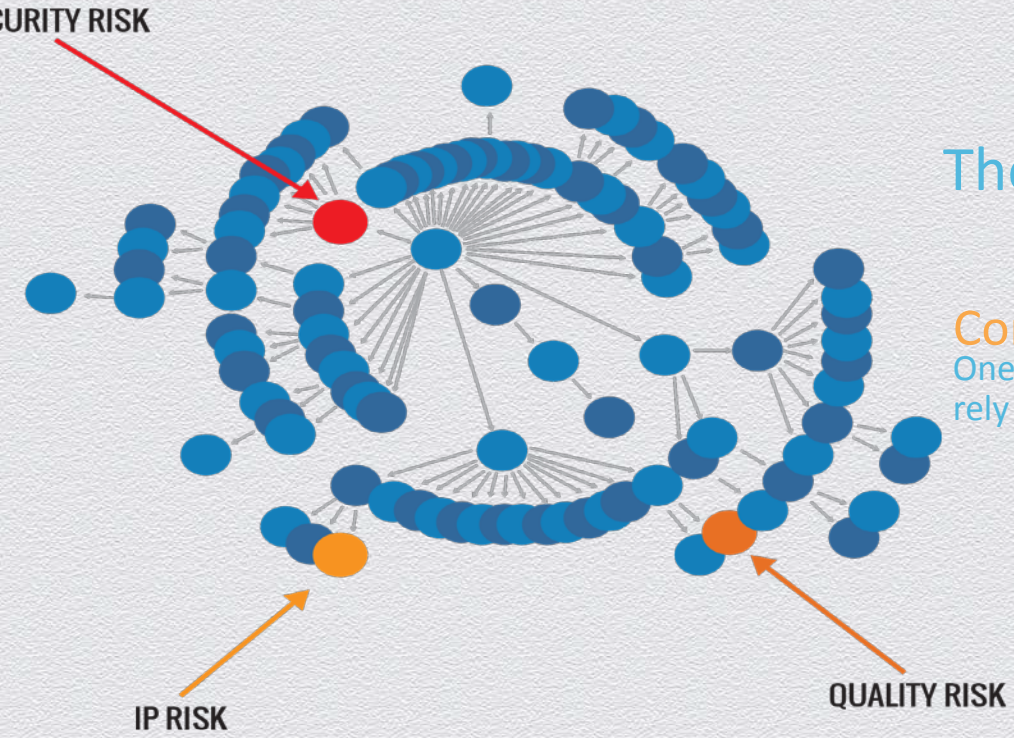


COMPONENT SELECTION | DEVELOPMENT | BUILD AND DEPLOY | PRODUCTION

Sonatype

#RSAC

RSACONFERENCE2014



WHY?

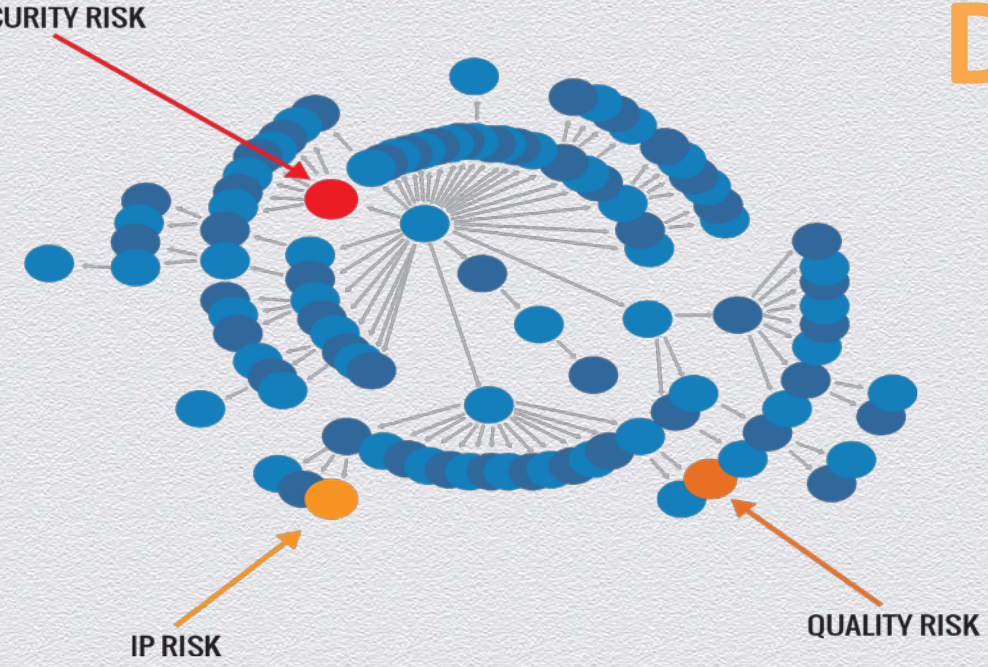
The problem is too complex to manage manually.

Complexity
One component may rely on 100s of others

Diversity
- 40,000 Projects
- 200M Classes
- 400K Components

Volume
Typical enterprise consumes 1,000s of components monthly

Change
Typical component is updated 4X per year



Manual processes

DON'T WORK

Automation should

ENFORCE POLICIES

Humans should manage

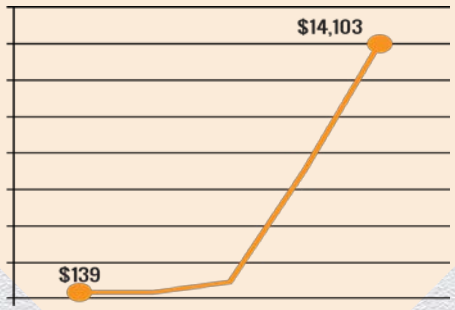
EXCEPTIONS

Sonatype

WHY

is this important?

To reduce cost per defect



!

To achieve compliance

PCI Security Standards Council

NIST

OWASP
The Open Web Application Security Project

SANS

EUROPEAN UNION

FINANCIAL SERVICES Information Sharing and Analysis Center

!

To manage risk

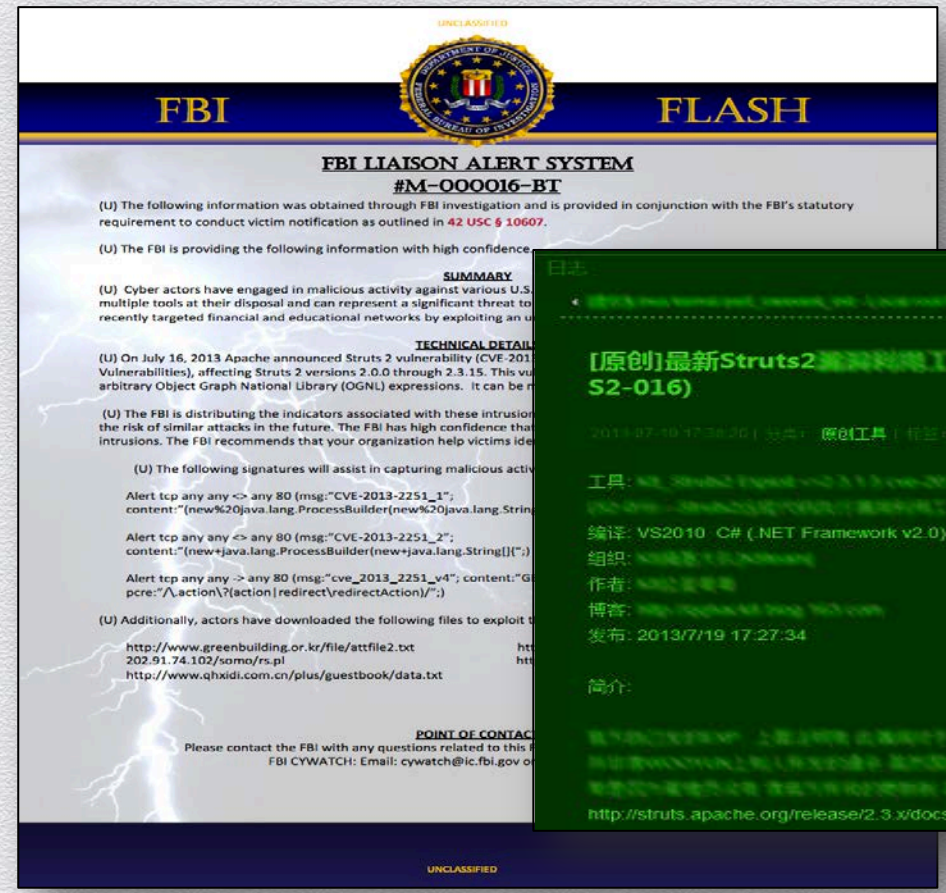
Struts

!

For Example: CVE-2013-2251

- Network exploitable
- Medium access complexity
- No authentication required for exploit
- Allows unauthorized disclosure of information;
  allows unauthorized modification; allows disruption of service

Hackers have first mover advantage



UNCLASSIFIED

FBI FLASH

FBI LIAISON ALERT SYSTEM
#M-000016-BT

(U) The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

(U) The FBI is providing the following information with high confidence.

SUMMARY

(U) Cyber actors have engaged in malicious activity against various U.S. multiple tools at their disposal and can represent a significant threat to recently targeted financial and educational networks by exploiting an u

TECHNICAL DETAIL

(U) On July 16, 2013 Apache announced Struts 2 vulnerability (CVE-201 Vulnerabilities), affecting Struts 2 versions 2.0.0 through 2.3.15. This vu arbitrary Object Graph National Library (OGNL) expressions. It can be r

(U) The FBI is distributing the indicators associated with these intrusion the risk of similar attacks in the future. The FBI has high confidence tha intrusions. The FBI recommends that your organization help victims ide

(U) The following signatures will assist in capturing malicious activ

Alert tcp any any <> any 80 (msg:"CVE-2013-2251_1"; content:"(new%20java.lang.ProcessBuilder(new%20java.lang.Strin

Alert tcp any any <> any 80 (msg:"CVE-2013-2251_2"; content:"(new+java.lang.ProcessBuilder(new+java.lang.String[](";)

Alert tcp any any -> any 80 (msg:"cve_2013_2251_v4"; content:"G pcre:"/\.action\?(action|redirect\redirectAction)/";)

(U) Additionally, actors have downloaded the following files to exploit t

http://www.greenbuilding.or.kr/file/attfile2.txt
202.91.74.102/somo/rs.pl
http://www.qhxidi.com.cn/plus/guestbook/data.txt

POINT OF CONTAC

Please contact the FBI with any questions related to this F
FBI CYWATCH: Email: cywatch@ic.fbi.gov o

UNCLASSIFIED

日志

[原创]最新Struts2 Struts2 Exploit <=2.3.1.5 cve-2013-2251 (S2-016)

原创工具 | struts2漏洞 struts2-exp

订阅 字号

工具:
编译: VS2010 C# (.NET Framework v2.0)
组织:
作者:
博客:
发布: 2013/7/19 17:27:34

简介:

http://struts.apache.org/release/2.3.x/docs/s2-016.html

Sonatype

#RSAC

RSACONFERENCE2014

THE ANTI-PATTERNS

TURN OFF THE LIGHTS

LOCK THE DOORS

Sonatype

RSACONFERENCE2014

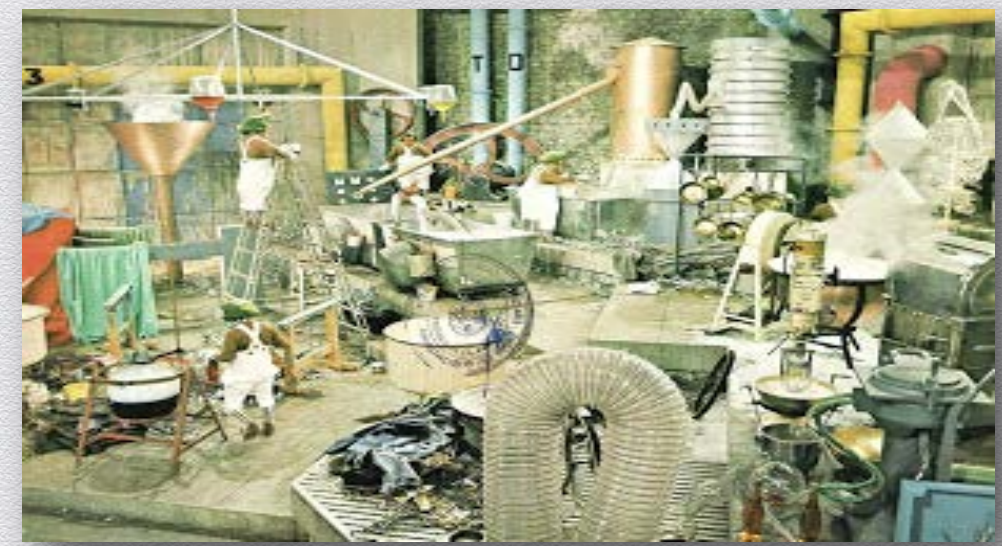
POINT FINGERS

THESE ARE NOT MY DROIDS

EVERYTHING IS A NAIL

Success Requires Discipline

The Problem is Not Problem Discovery



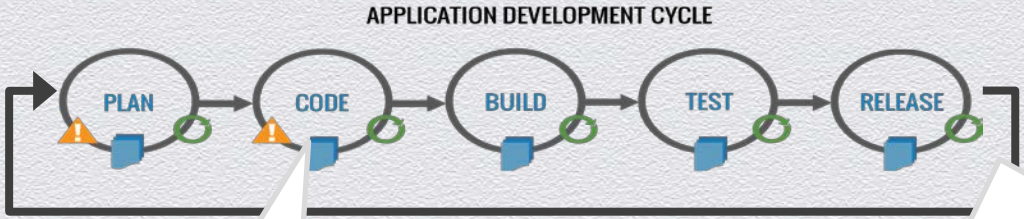
- When our software development ecosystem looks like this it is easy to find problems
- The real challenge is to develop at scale and deliver continuous value continuously when everything else is a mess

The problem is no longer like this

It’s Starting to Look More Like This

Time for a

FRESH APPROACH?



Developer friendly – makes it easy to find and fix problems early.

Visibility and control. Automated and integrated policy enforcement throughout the software lifecycle.

Proactive and ongoing for continued trust.

Got questions?

Get the

ANSWERS.

- What production applications are at risk?
- What problems are most critical?
- What components are being used? Where are they?
- Which components have known security vulnerabilities?
- What are our license obligations?
- Do our applications comply with our policies?
- How can we choose the best components **from the start**?

Building A Better Bridge

Between Dev, Ops and Security

- Need to recognize that the priorities are different
- Tooling needs to adopt the practice of the practitioner not the other way around
- A Tool is not a process and a process is not a tool learn to leverage both.

Building A Better Bridge Between Dev, Ops and Security

- Need to recognize that the priorities are different
- Tooling needs to adopt the practice of the practitioner not the other way around
- A Tool is not a process and a process is not a tool learn to leverage both.

Go Fast.
Be Secure.

Build security in from the start

Enforce policy in the tools you already use

Reduce risk by automating governance throughout the lifecycle

Reduce cost by fixing early in the process

React to new threats by knowing what they are and where to fix them

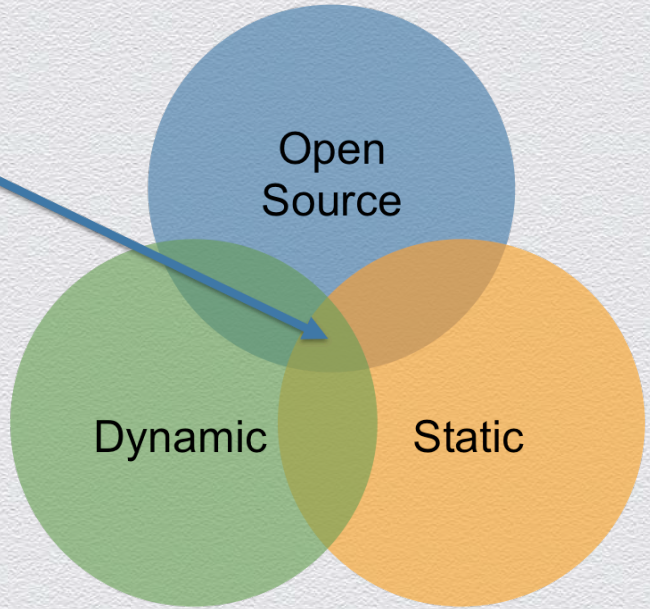
Go fast by using tools your developers already know

Announcing a

NEW BREED

of On-Demand Application Security

Sonatype



Thank You

@ryanberg00

LEARN MORE

Sonatype:
South Hall #2327

HP Fortify on Demand:
North Hall #3401

www.sonatype.com/fortify

Sonatype

#RSAC

RSACONFERENCE2014