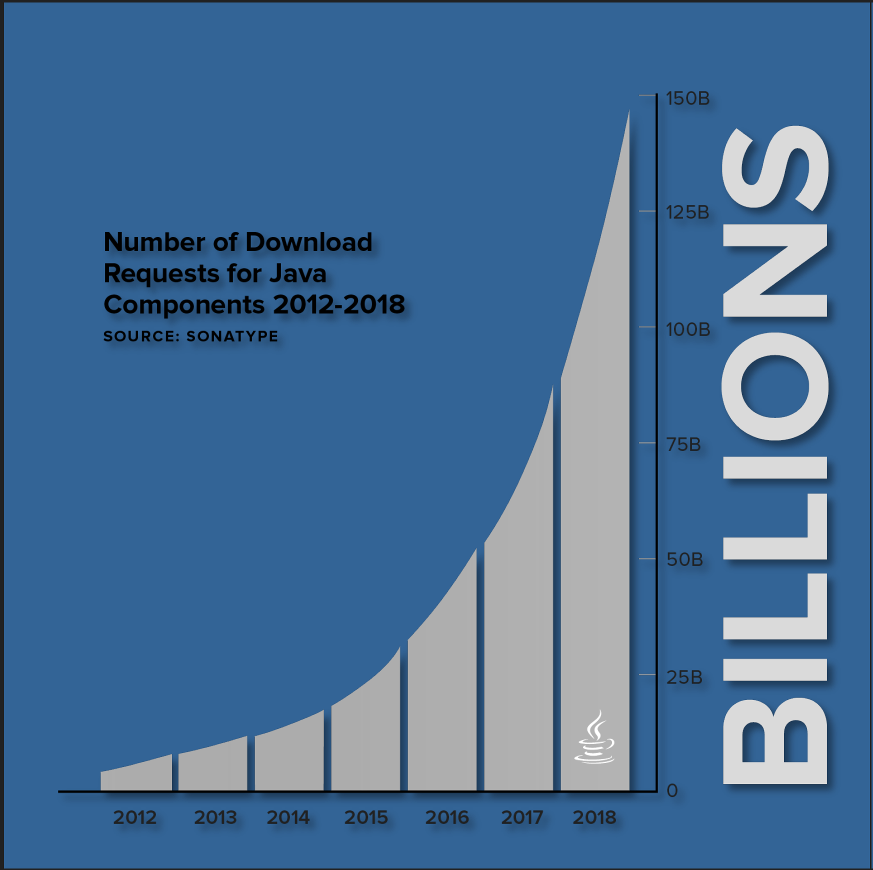
sonatype

Automate or Die

Anthony Baer abaer@sonatype.com

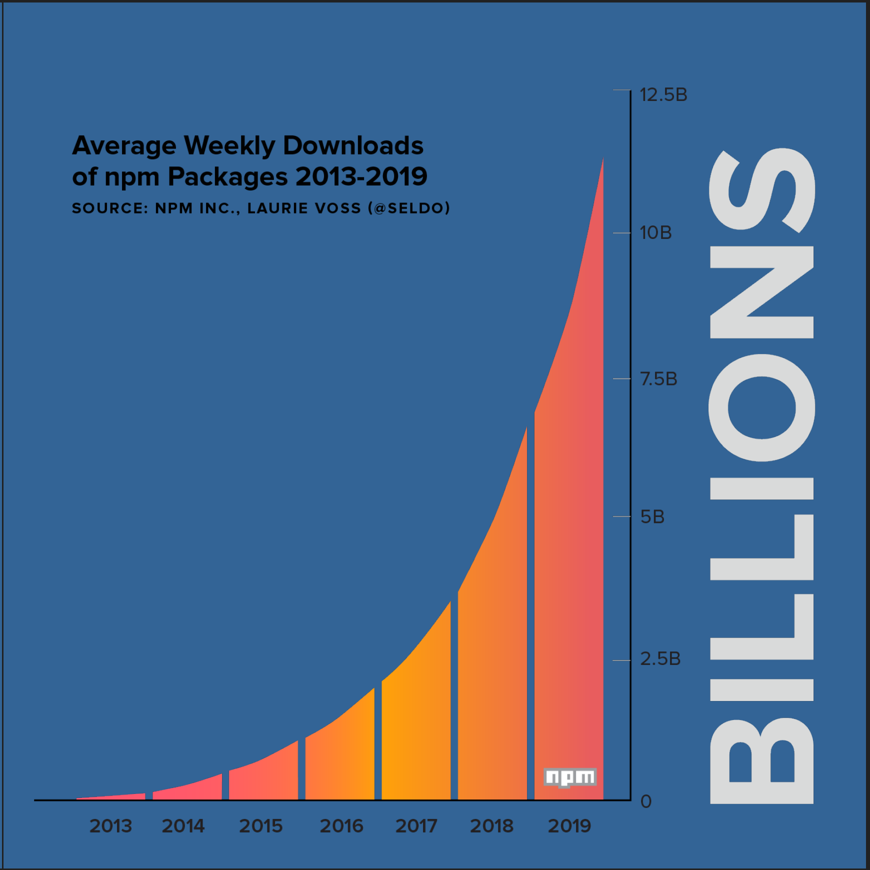
March 5, 2020

OSS download volumes



Number of Download Requests for Java Components 2012-2018

SOURCE: SONATYPE



Average Weekly Downloads of npm Packages 2013-2019

SOURCE: NPM INC., LAURIE VOSS (@SELDO)

Source: Sonatype

It's no secret... developers use open source software.

Still, there are questions around how it should be managed—and for good reason. Here's why:

- Open source components are not created equal. Some are vulnerable from the start, while others go bad over time.
- Usage has become more complex. With tens of billions of downloads, it's increasingly difficult to manage libraries and direct dependencies.
- Transitive dependencies: if you are using dependency management tools like Maven (Java), Bower (JavaScript), Bundler (Ruby), etc., then you are automatically pulling in third party dependencies—a liability that you can't afford.

How do you manage open source risk at scale?
Through an automated open source governance policy.

of the components in most modern applications are open source.

500 billion
download requests of Java, npm, PyPi, and RubyGems were recorded in 2018.

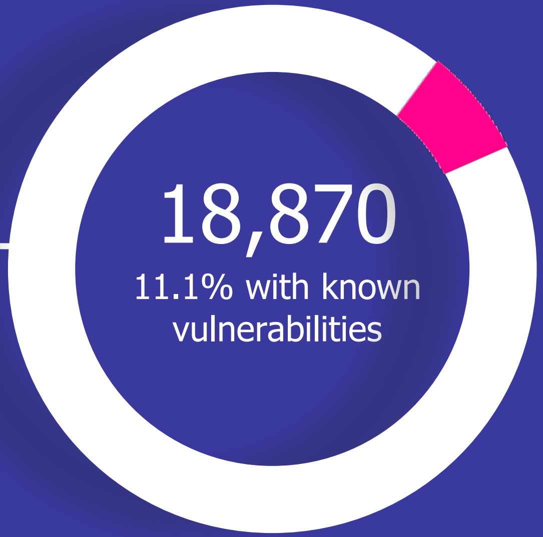
300,000+
open source components are downloaded annually by the average company.

170,000

java component downloads annually

3,500

unique



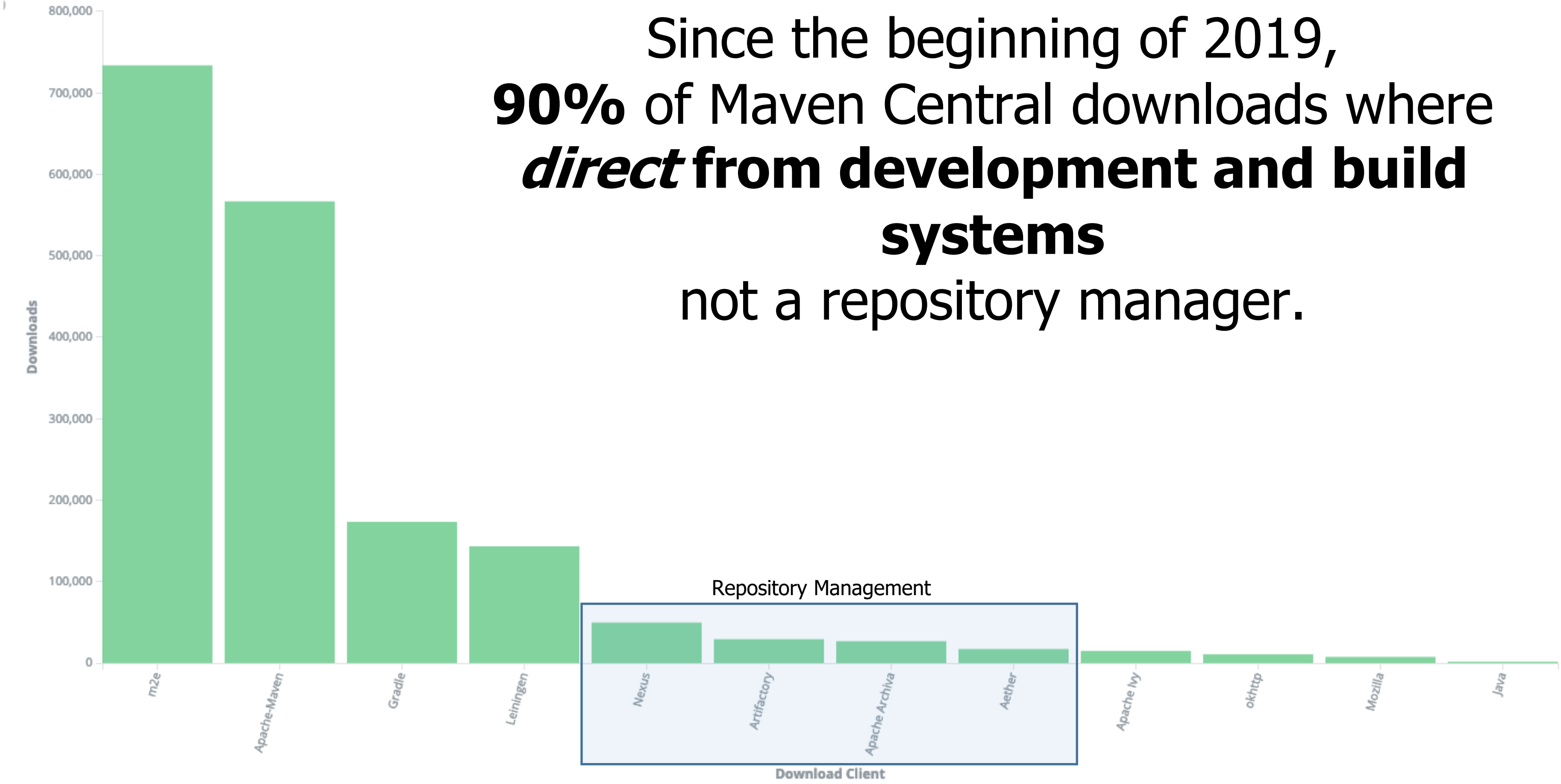
18,870

11.1% with known vulnerabilities

sonatype

@weekstweets

Since the beginning of 2019,
90% of Maven Central downloads where
direct **from development and build systems**
not a repository manager.



Repository Management

60,660

JavaScript packages downloaded annually per developer

30,330

51% with known vulnerabilities

DevSecOps: Why is open source policy critical?

1 in 10

open source component downloads contain a known security vulnerability.

71%

increase in verified or suspected breaches between 2014 and 2019.

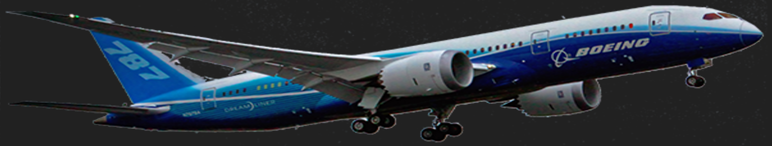
1 in 4

organizations experienced at least one open source breach in the last 12 months.

38%

of organizations have no open source governance policy or ignore it.

We are not the first **INDUSTRY** to face a supply chain **CHALLENGE**



2013 CVE-2013-2251

STRUTS

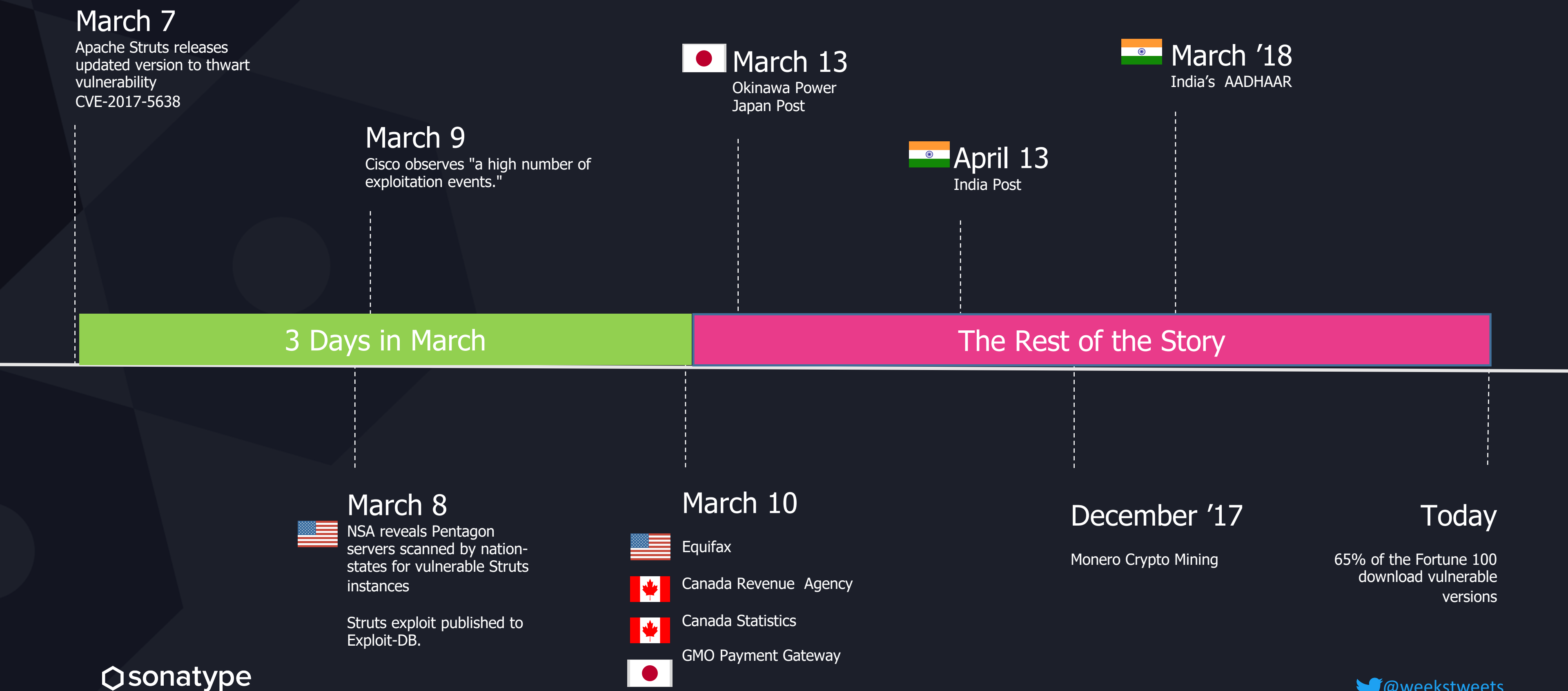
- Network exploitable
- Medium access complexity
- No authentication required for exploit
- Allows unauthorized disclosure of information
- Allows unauthorized modification
- Allows disruption of service

2014

CVE-2014-0160

CVE-2014-6271

Equifax Was Not Alone



3 Days in March

The Rest of the Story

March 7

Apache Struts releases updated version to thwart vulnerability
CVE-2017-5638

March 8

NSA reveals Pentagon servers scanned by nation-states for vulnerable Struts instances

Struts exploit published to Exploit-DB.

March 9

Cisco observes "a high number of exploitation events."

March 10

Equifax

Canada Revenue Agency

Canada Statistics

GMO Payment Gateway

March 13

Okinawa Power
Japan Post

April 13

India Post

December ’17

Monero Crypto Mining

March ’18

India’s AADHAAR

Today

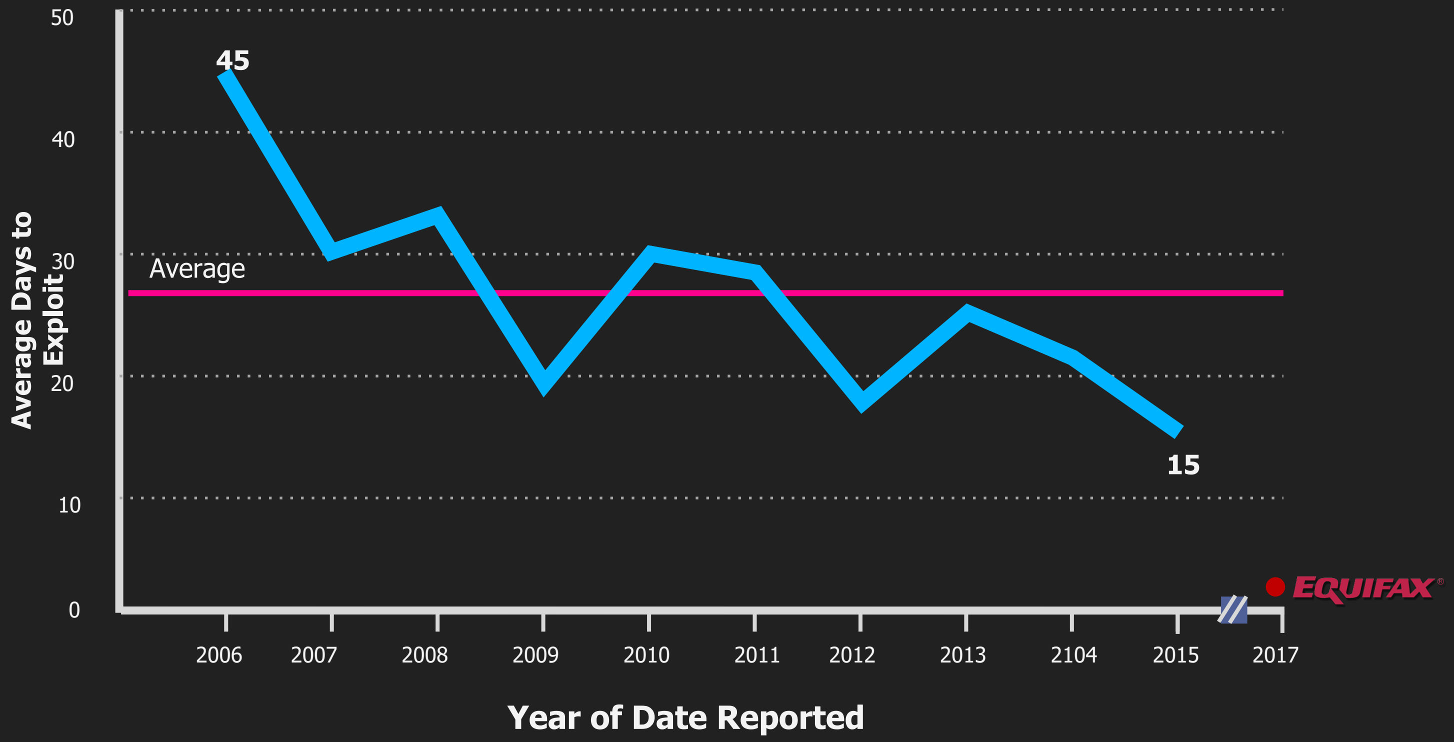
65% of the Fortune 100 download vulnerable versions

sonatype

@weekstweets

TIME TO **RESPOND BEFORE** EXPLOIT

Source: Adapted from IBM X-Force / Analysis by Gartner Research (September 2016)



Known Vulnerabilities Aren’t the Only Problem

Organized Cybercrime is the most profitable type of crime

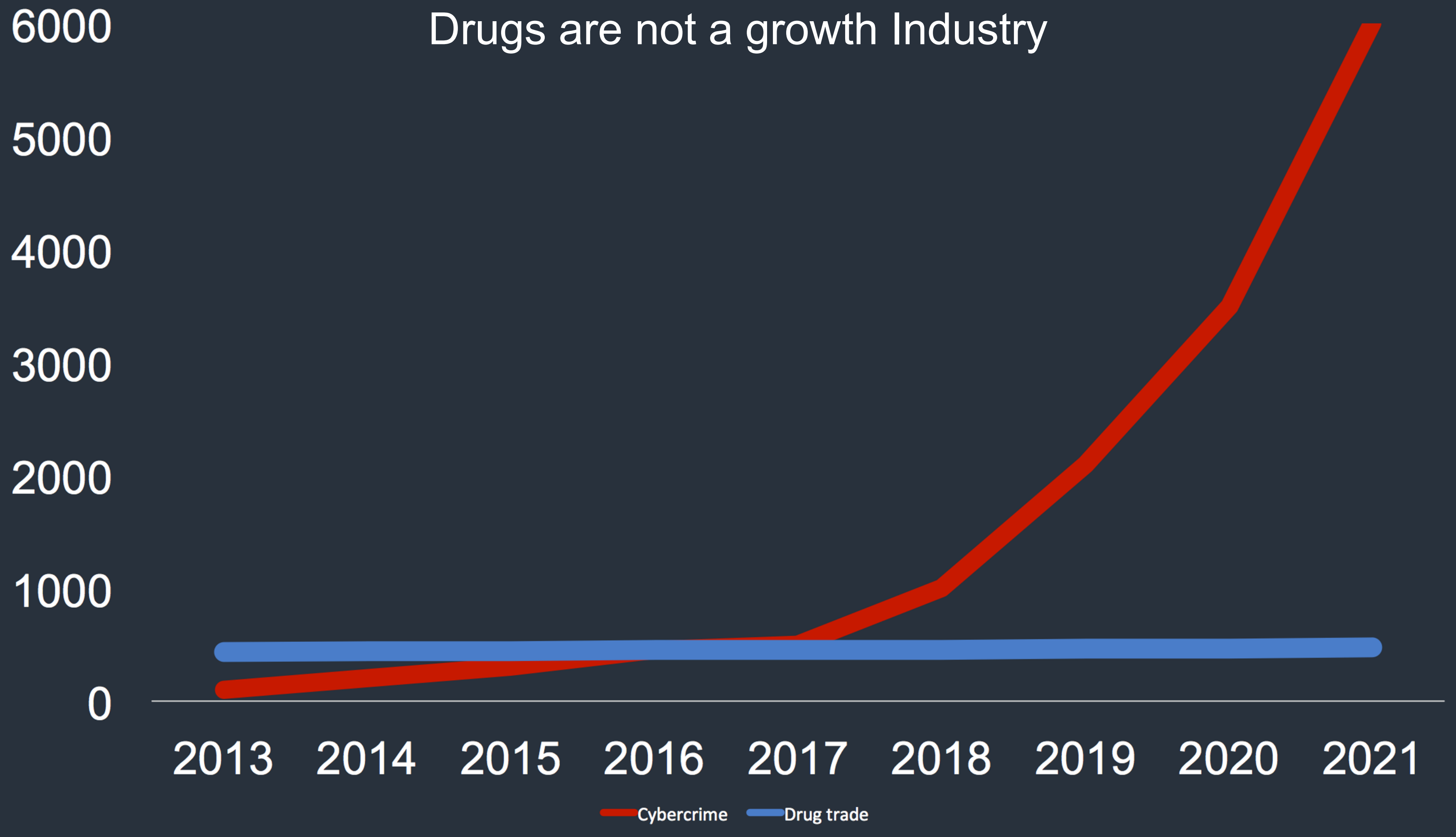
In 2016 Cybercrime was estimated to be worth

450 Billion Dollars

In 2016 The illicit drug trade was estimated to be worth

435 Billion Dollars

Drugs are not a growth Industry

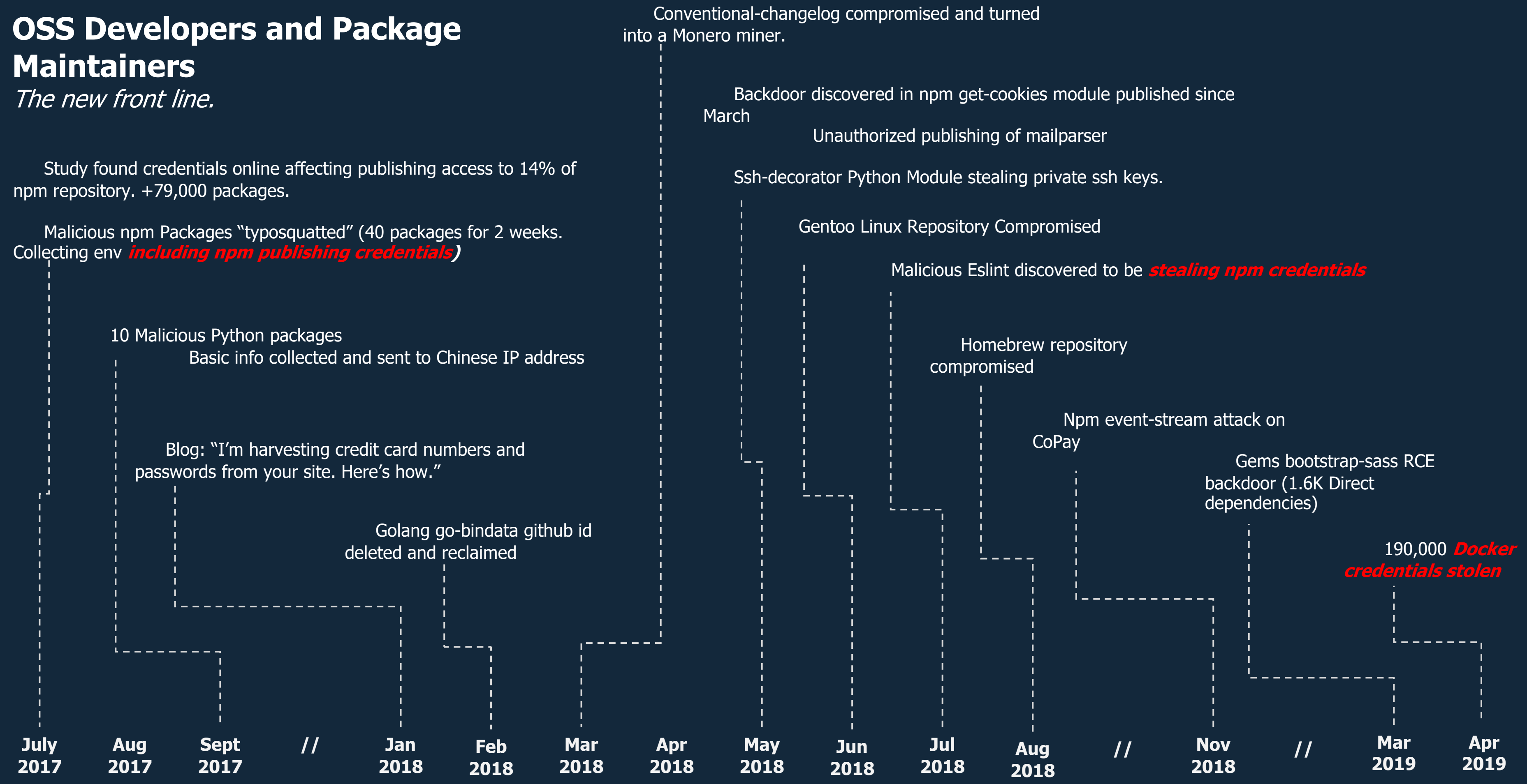


That’s about $800 for every person on the planet

Slide Credit: Steven Pool @spool167

OSS Developers and Package Maintainers

The new front line.



Study found credentials online affecting publishing access to 14% of npm repository. +79,000 packages.

Malicious npm Packages “typosquatted” (40 packages for 2 weeks. Collecting env ***including npm publishing credentials)***

10 Malicious Python packages
Basic info collected and sent to Chinese IP address

Blog: “I’m harvesting credit card numbers and passwords from your site. Here’s how.”

Golang go-bindata github id deleted and reclaimed

Conventional-changelog compromised and turned into a Monero miner.

Backdoor discovered in npm get-cookies module published since March

Unauthorized publishing of mailparser

Ssh-decorator Python Module stealing private ssh keys.

Gentoo Linux Repository Compromised

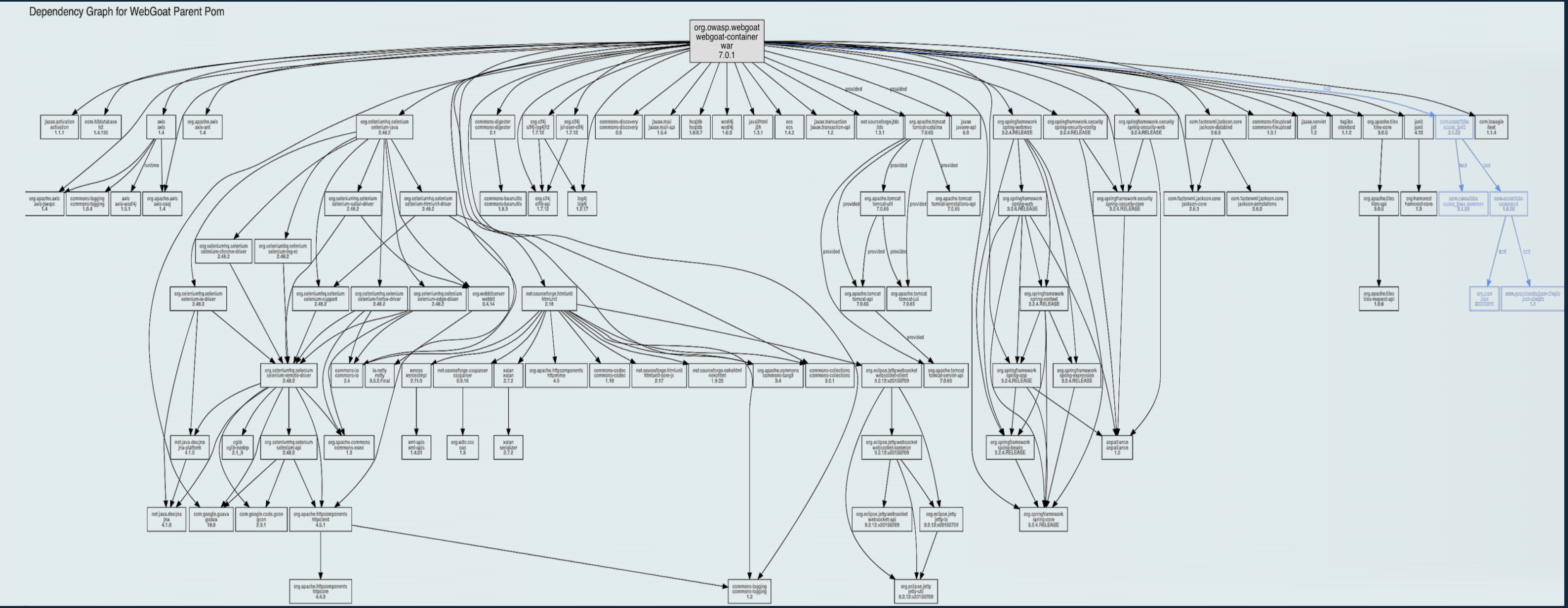
Malicious Eslint discovered to be ***stealing npm credentials***

Homebrew repository compromised

Npm event-stream attack on CoPay

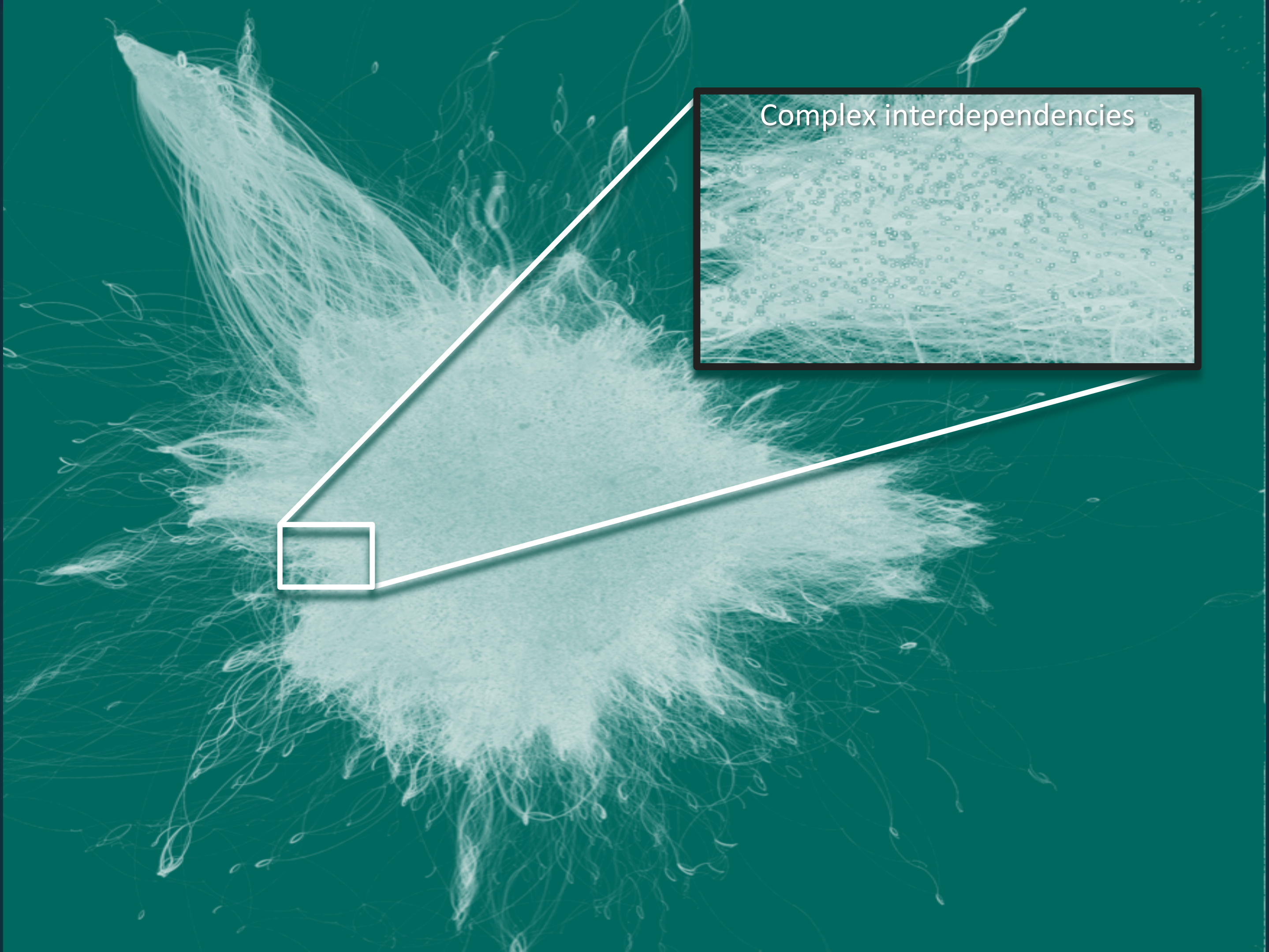
Gems bootstrap-sass RCE backdoor (1.6K Direct dependencies)

190,000 ***Docker credentials stolen***



Dependency Graph for WebGoat Parent Pom

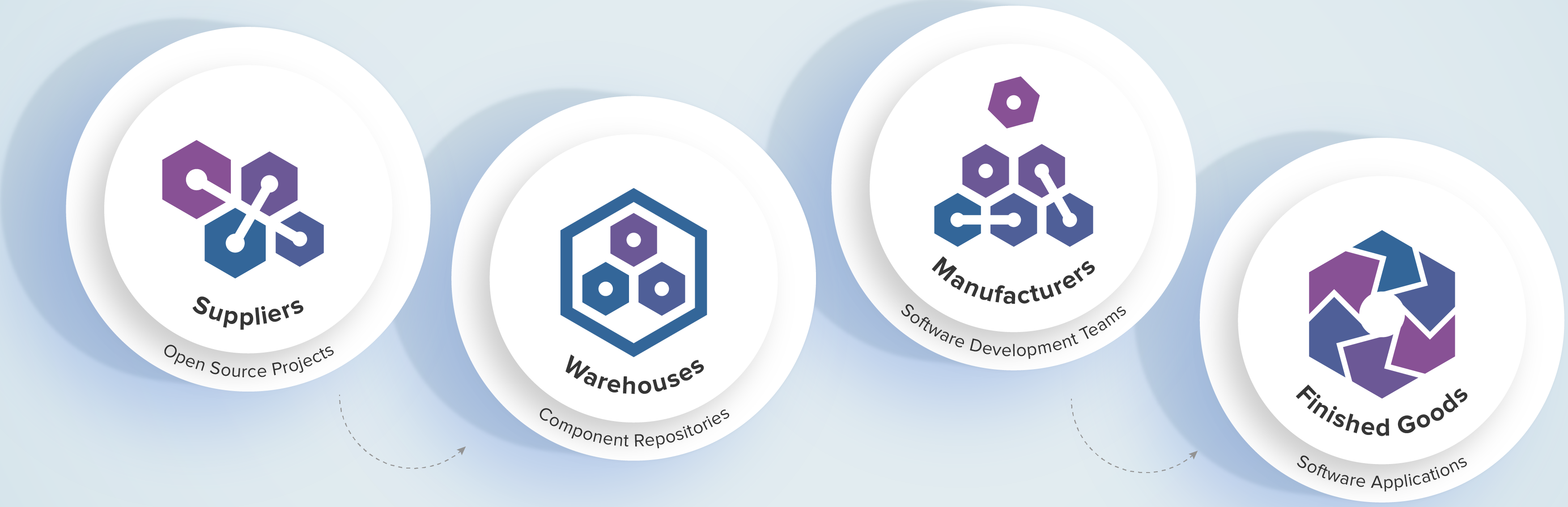
org.owasp.webgoat webgoat-container war 7.0.1
javax.activation activation 1.1.1
com.h2database h2 1.4.190
axis axis 1.4
org.apache.axis axis-ant 1.4
org.seleniumhq.selenium selenium-java 2.48.2
commons-digester commons-digester 2.1
org.slf4j slf4j-log4j12 1.7.12
org.slf4j jcl-over-slf4j 1.7.12
commons-discovery commons-discovery 0.5
javax.mail javax.mail-api 1.5.4
hsqldb hsqldb 1.8.0.7
wsdl4j wsdl4j 1.6.3
java2html j2h 1.3.1
ecs ecs 1.4.2
javax.transaction javax.transaction-api 1.2
net.sourceforge.jtds jtds 1.3.1
org.apache.tomcat tomcat-catalina 7.0.65
javax javaee-api 6.0
org.springframework spring-webmvc 3.2.4.RELEASE
org.springframework.security spring-security-config 3.2.4.RELEASE
org.springframework.security spring-security-web 3.2.4.RELEASE
com.fasterxml.jackson.core jackson-databind 2.6.3
commons-fileupload commons-fileupload 1.3.1
javax.servlet jstl 1.2
taglibs standard 1.1.2
org.apache.tiles tiles-core 3.0.5
junit junit 4.12
com.saucelabs sauce_junit 2.1.20
com.lowagie itext 1.1.4
provided
provided
test
runtime
org.apache.axis axis-jaxrpc 1.4
commons-logging commons-logging 1.0.4
axis axis-wsdl4j 1.5.1
org.apache.axis axis-saaj 1.4
org.seleniumhq.selenium selenium-safari-driver 2.48.2
org.seleniumhq.selenium selenium-htmlunit-driver 2.48.2
commons-beanutils commons-beanutils 1.8.3
org.slf4j slf4j-api 1.7.12
log4j log4j 1.2.17
provided
org.apache.tomcat tomcat-util 7.0.65
provided
provided
org.apache.tomcat tomcat-annotations-api 7.0.65
org.springframework spring-web 3.2.4.RELEASE
org.springframework.security spring-security-core 3.2.4.RELEASE
com.fasterxml.jackson.core jackson-core 2.6.3
com.fasterxml.jackson.core jackson-annotations 2.6.0
org.apache.tiles tiles-api 3.0.5
org.hamcrest hamcrest-core 1.3
test
test
com.saucelabs sauce_java_common 2.1.20
com.saucelabs saucerest 1.0.22
org.seleniumhq.selenium selenium-chrome-driver 2.48.2
org.seleniumhq.selenium selenium-leg-rc 2.48.2
provided
provided
provided
test
test
org.seleniumhq.selenium selenium-ie-driver 2.48.2
org.seleniumhq.selenium selenium-support 2.48.2
org.seleniumhq.selenium selenium-firefox-driver 2.48.2
org.seleniumhq.selenium selenium-edge-driver 2.48.2
org.webbitserver webbit 0.4.14
net.sourceforge.htmlunit htmlunit 2.18
org.apache.tomcat tomcat-api 7.0.65
org.apache.tomcat tomcat-juli 7.0.65
org.springframework spring-context 3.2.4.RELEASE
org.apache.tiles tiles-request-api 1.0.6
org.json json 20090211
com.googlecode.json-simple json-simple 1.1
provided
org.seleniumhq.selenium selenium-remote-driver 2.48.2
commons-io commons-io 2.4
io.netty netty 3.5.2.Final
xerces xercesImpl 2.11.0
net.sourceforge.cssparser cssparser 0.9.16
xalan xalan 2.7.2
org.apache.httpcomponents httpmime 4.5
commons-codec commons-codec 1.10
net.sourceforge.htmlunit htmlunit-core-js 2.17
net.sourceforge.nekohtml nekohtml 1.9.22
org.apache.commons commons-lang3 3.4
commons-collections commons-collections 3.2.1
org.eclipse.jetty.websocket websocket-client 9.2.12.v20150709
org.apache.tomcat tomcat-servlet-api 7.0.65
org.springframework spring-aop 3.2.4.RELEASE
org.springframework spring-expression 3.2.4.RELEASE
net.java.dev.jna jna-platform 4.1.0
cglib cglib-nodep 2.1_3
org.seleniumhq.selenium selenium-api 2.48.2
org.apache.commons commons-exec 1.3
xml-apis xml-apis 1.4.01
org.w3c.css sac 1.3
xalan serializer 2.7.2
org.eclipse.jetty.websocket websocket-common 9.2.12.v20150709
org.springframework spring-beans 3.2.4.RELEASE
aopalliance aopalliance 1.0
net.java.dev.jna jna 4.1.0
com.google.guava guava 18.0
com.google.code.gson gson 2.3.1
org.apache.httpcomponents httpclient 4.5.1
org.eclipse.jetty.websocket websocket-api 9.2.12.v20150709
org.eclipse.jetty jetty-io 9.2.12.v20150709
org.springframework spring-core 3.2.4.RELEASE
org.apache.httpcomponents httpcore 4.4.3
commons-logging commons-logging 1.2
org.eclipse.jetty jetty-util 9.2.12.v20150709


Complex interdependencies

With the right tools, many of these problems are solvable

Everyone has a software supply chain.

(even if you don’t call it that)



Suppliers

Open Source Projects

Warehouses

Component Repositories

Manufacturers

Software Development Teams

Finished Goods

Software Applications

sonatype

What is software supply chain management?

A new **(yet proven)** way of thinking.

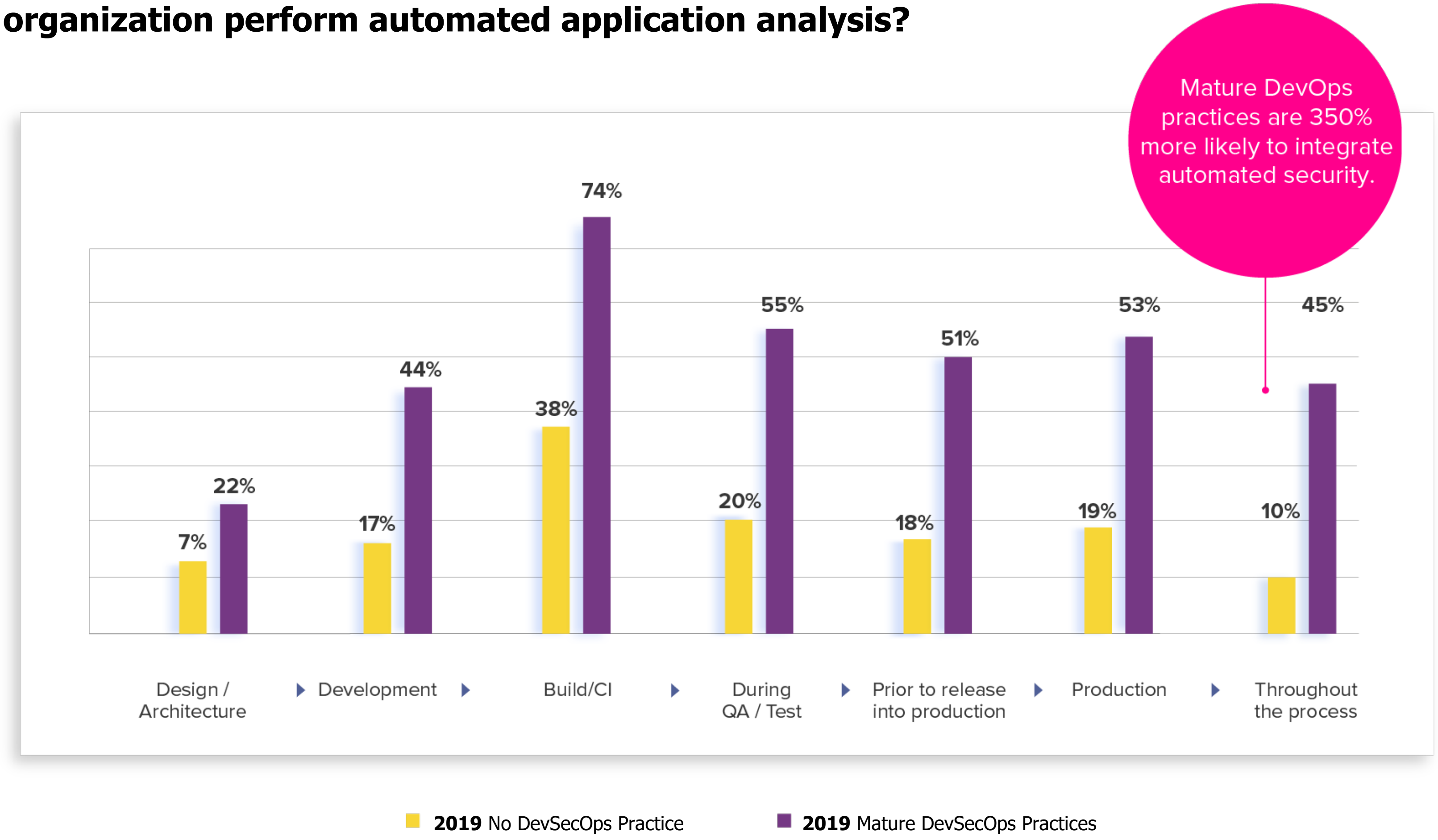
1. Source parts from fewer and better suppliers.
2. Use only the highest quality parts.
3. Never pass known defects downstream.
4. Continuously track location of every part.

W. Edwards Deming

100:1

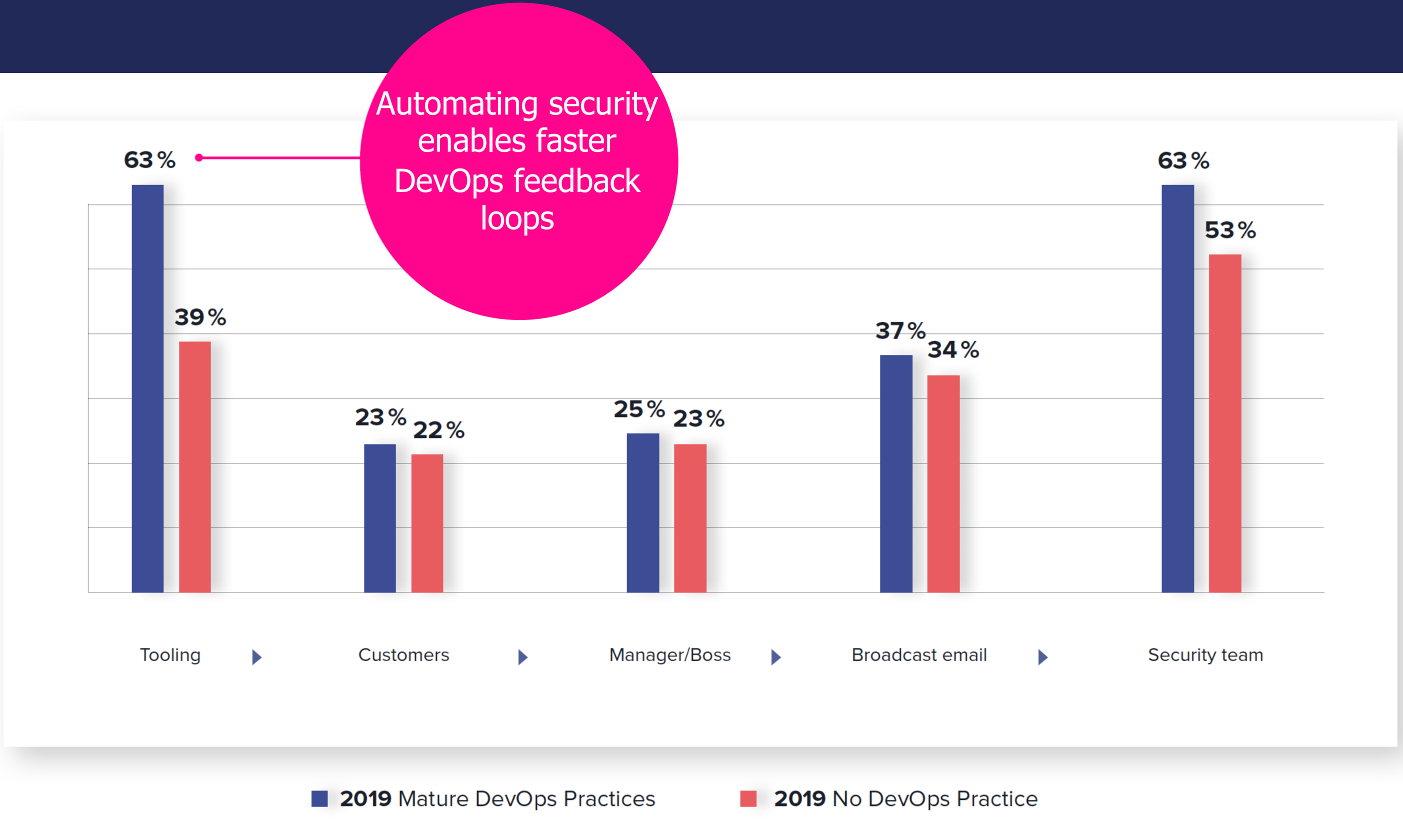
developers outnumber application security

At what point in the development process does your organization perform automated application analysis?



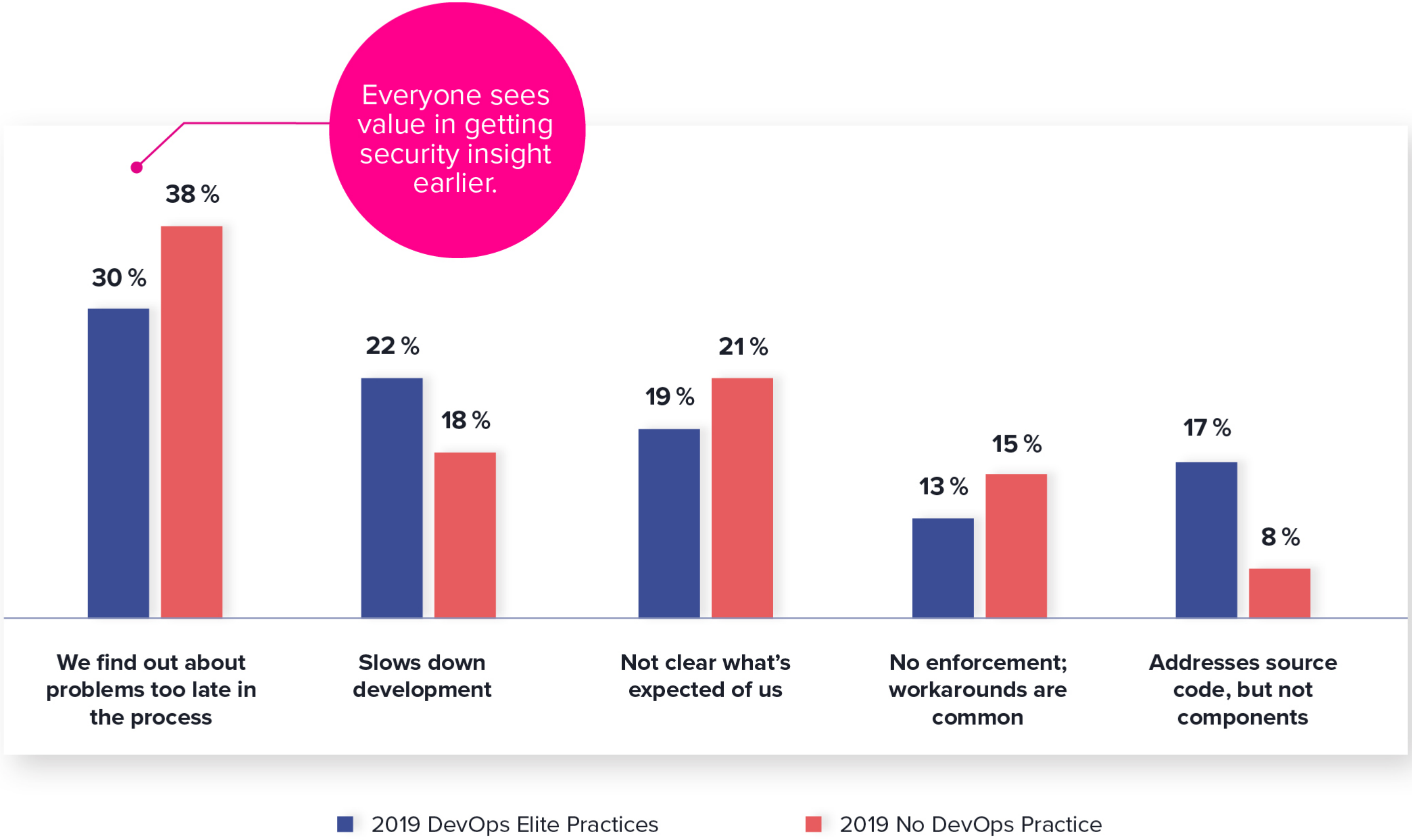
Mature DevOps practices are 350% more likely to integrate automated security.

How are you informed of InfoSec and AppSec issues?



Automating security enables faster DevOps feedback loops

Rank the top challenges with your application security processes.



Everyone sees value in getting security insight earlier.

1

Solve your supply chain problems

2

Solve your own quality problems – trust but verify

3

Create discipline – every day it gets a little bit easier

Thank you!

Anthony Baer abaer@sonatype.com

sonatype