SKILUP DAYS

by: DevOps Institute
ADVANCING THE HUMANS OF DEVOPS

Matt Stanchek
Fortify on Demand Architect
Micro Focus
matt.stanchek@microfocus.com

A JDBC Library
And the Day I Felt Like Jack Ryan

Matt Stanchek
Fortify on Demand Architect

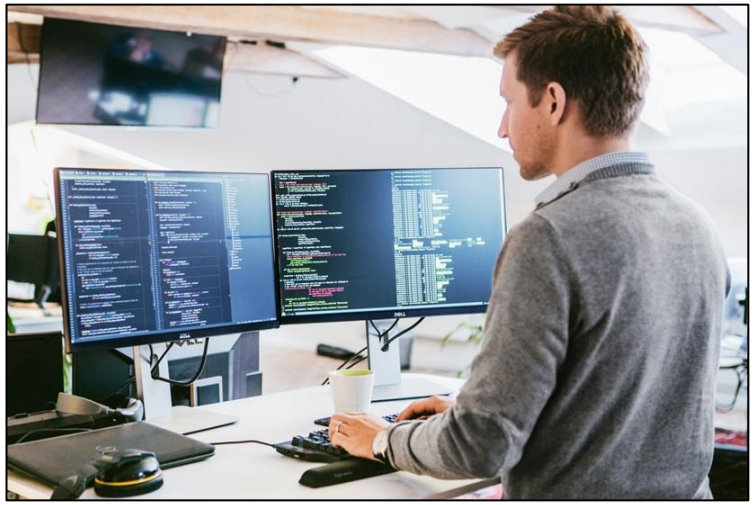
About Me

- 15 or so years as “IT guy”, developer, tech lead before moving into security
- Implemented AppSec tooling and automation at multiple organizations
- Dad, car guy, sci-fi fan
- Fortify on Demand Architect

matt.stanchek@microfocus.com

Booting up DevSecOps

Once upon a time...



New DevOps processes and patterns were emerging

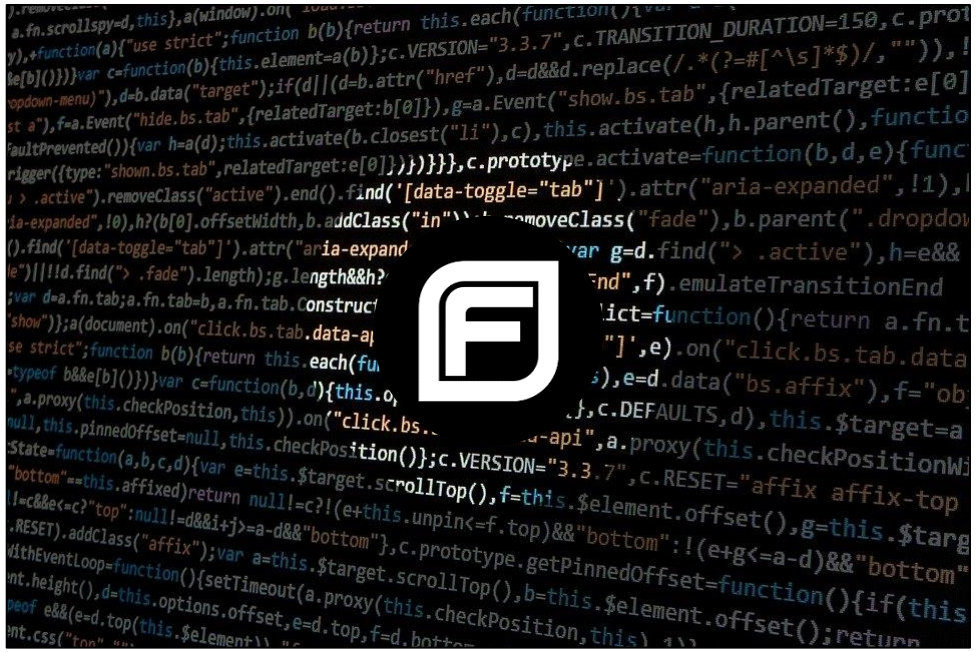
Meanwhile, new Application Security practices were starting

DevOps

- Build and test automation
- Centralized repository management
- Best practices

Security

- Scan automation
- Centralized results management
- Best practices




DID WE JUST BECOME BEST FRIENDS?
YUP!

DevSecOps

Communication

Collaboration

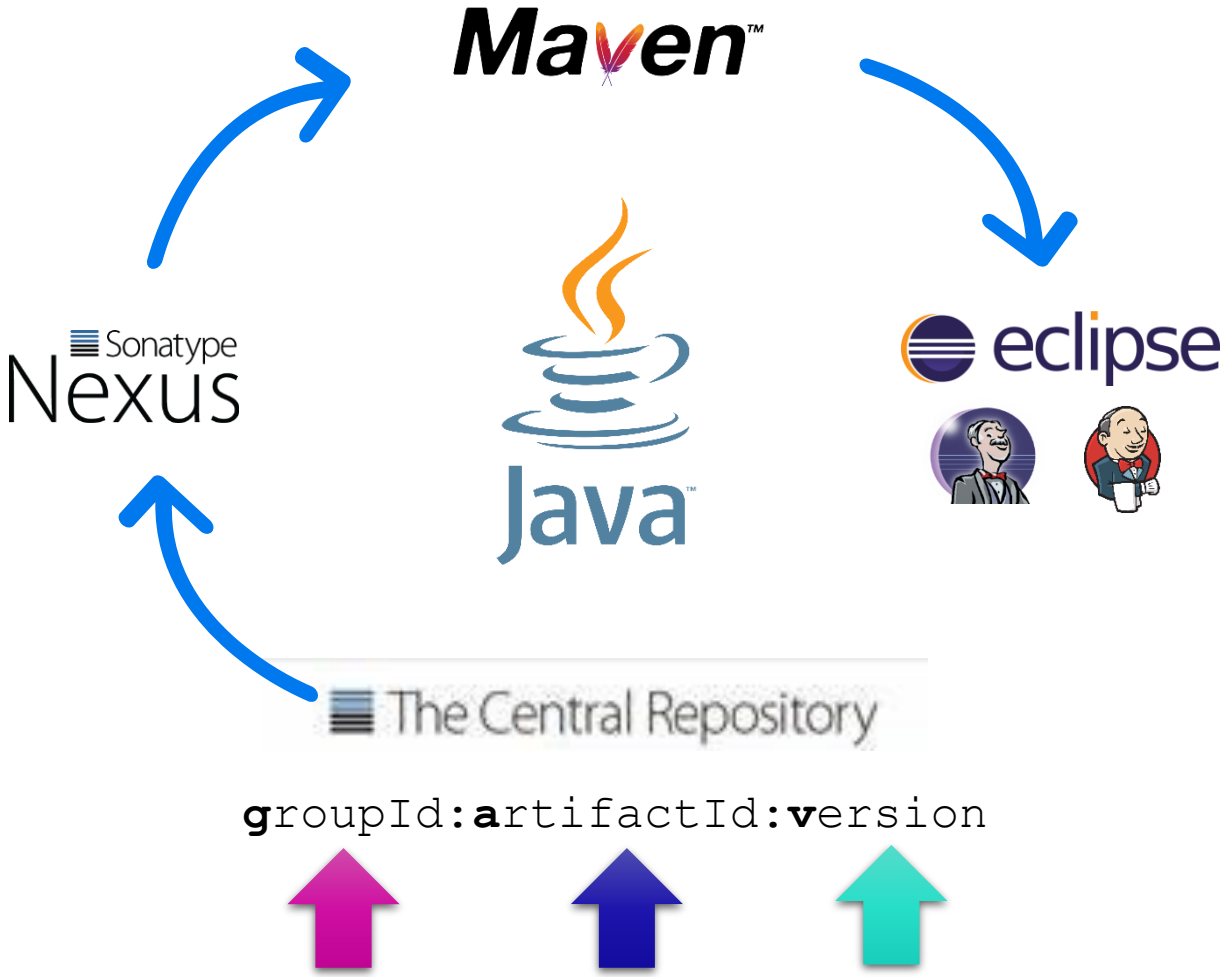
Culture

Open Source Software

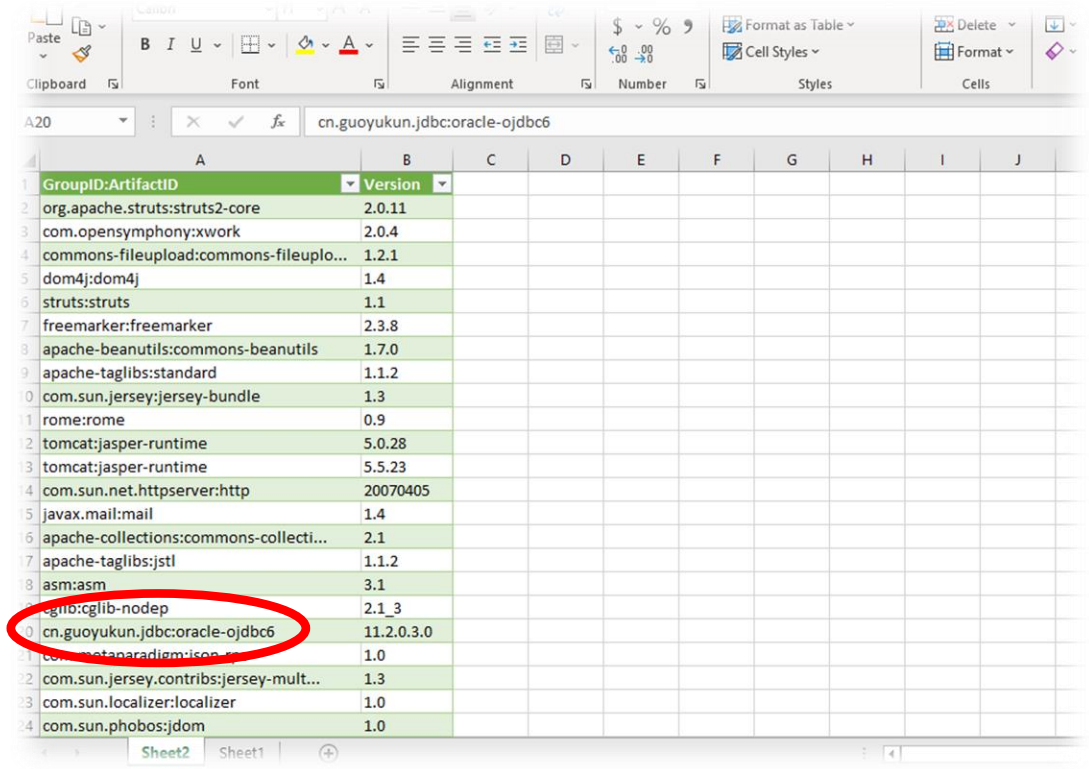
As the risks of using Open Source Software were being recognized, the DevOps folks asked for Security to review its usage

It became my second job

Java Ecosystem



cn.guoyukun

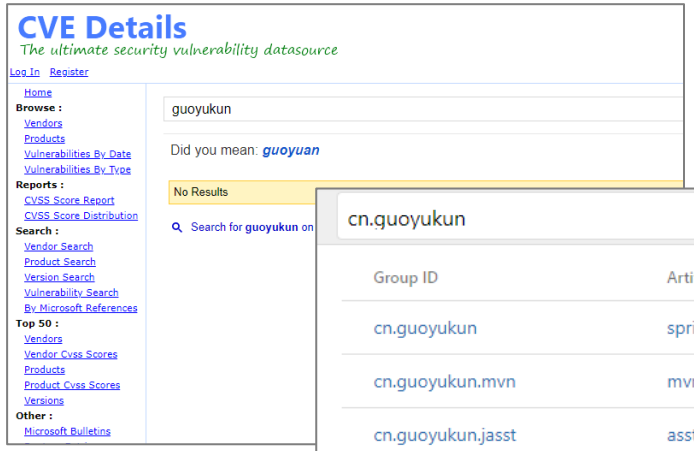


GroupID:ArtifactID	Version
org.apache.struts:struts2-core	2.0.11
com.opensymphony:xwork	2.0.4
commons-fileupload:commons-fileuplo...	1.2.1
dom4j:dom4j	1.4
struts:struts	1.1
freemarker:freemarker	2.3.8
apache-beanutils:commons-beanutils	1.7.0
apache-taglibs:standard	1.1.2
com.sun.jersey:jersey-bundle	1.3
rome:rome	0.9
tomcat:jasper-runtime	5.0.28
tomcat:jasper-runtime	5.5.23
com.sun.net.httpserver:http	20070405
javax.mail:mail	1.4
apache-collections:commons-collecti...	2.1
apache-taglibs:jstl	1.1.2
asm:asm	3.1
cglib:cglib-nodep	2.1_3
cn.guoyukun.jdbc:oracle-ojdbc6	11.2.0.3.0
[illegible]	1.0
com.sun.jersey.contribs:jersey-mult...	1.3
com.sun.localizer:localizer	1.0
com.sun.phobos:jdom	1.0

The process started off with developers submitting a list of Open Source components they wanted to use for their projects

I would take a look and assess the risk by researching known vulnerabilities and some other factors

Research



Research didn’t turn up any known vulnerabilities

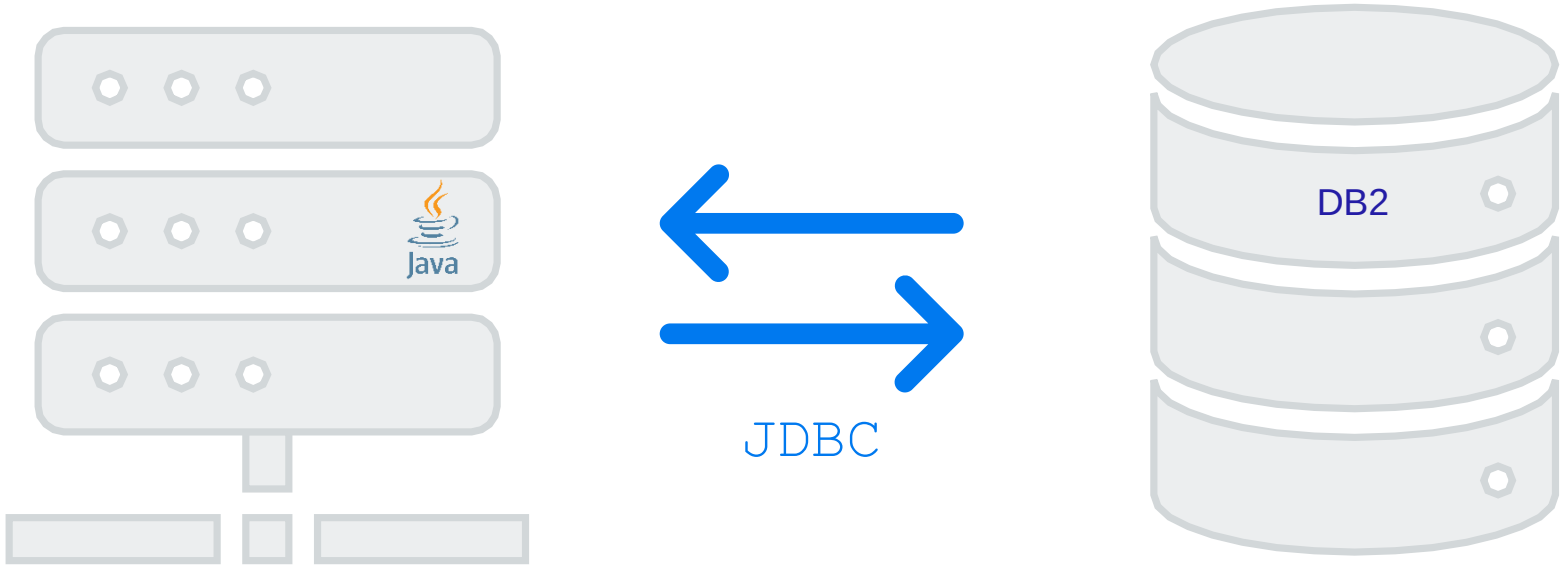
cn.guoyukun

Group ID	Artifact ID	Latest Version		Updated
cn.guoyukun	spring-leman	1.0.5	(6)	14-Jun-201
cn.guoyukun.mvn	mvn-basic	0.0.3	(3)	28-Jul-201
cn.guoyukun.jasst	asst-parent	0.0.1	(1)	28-Apr-20
cn.guoyukun.mvn	basic-web	0.0.1	(1)	23-Dec-20
cn.guoyukun	protocol-extends	0.1	(1)	23-Aug-20
cn.guoyukun	pdm2pdf	0.0.1	(1)	05-Aug-20
cn.guoyukun	leman-jdbc-extend	1.0.5	(1)	14-Jun-201
cn.guoyukun	leman-schema-extend	1.0.5	(5)	14-Jun-201
cn.guoyukun	leman-core-extend	1.0.5	(1)	14-Jun-2016
cn.guoyukun.crack	soupui-pro-crack	5.1.1	(3)	22-Aug-2014
cn.guoyukun.jasst	asst-test	0.0.1	(1)	28-Apr-2014

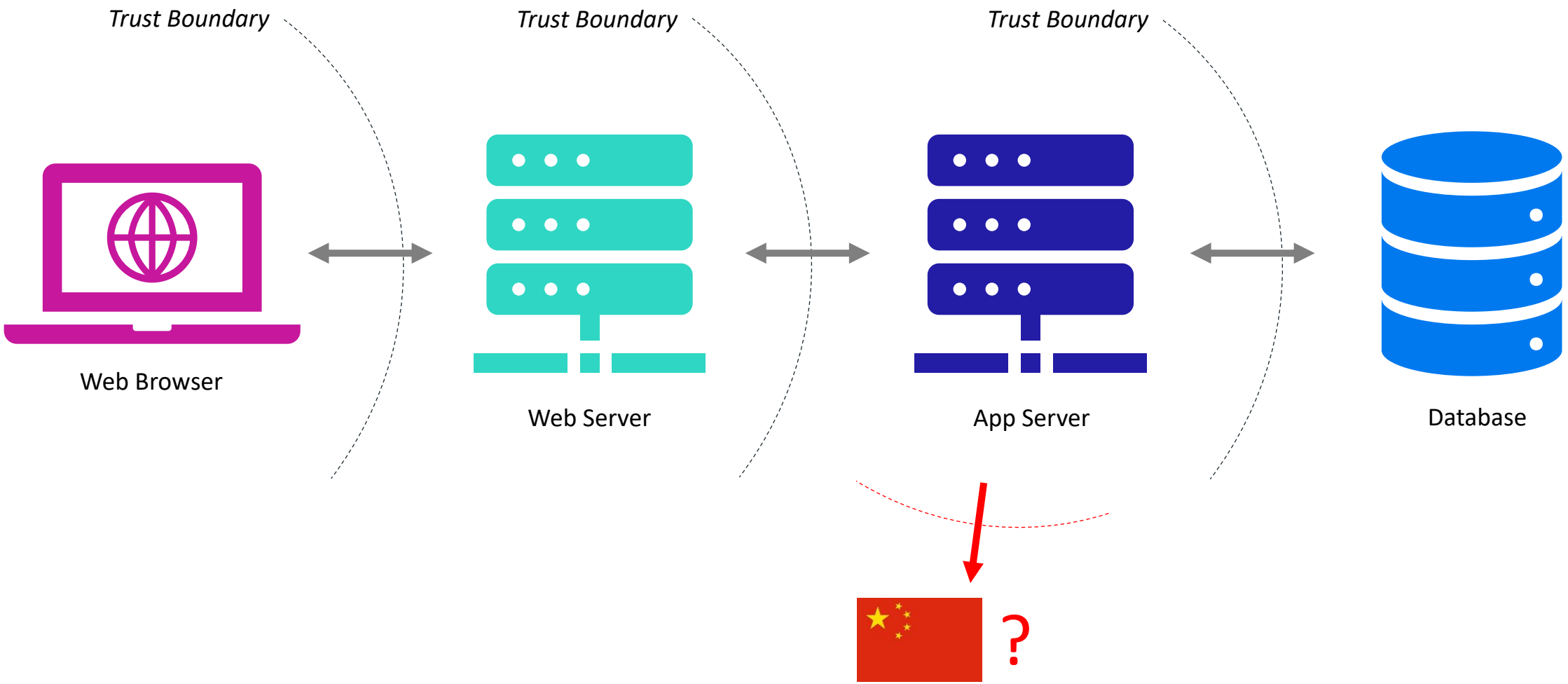
Items per page: 20

But there were some warning signs

Java Database Connectivity



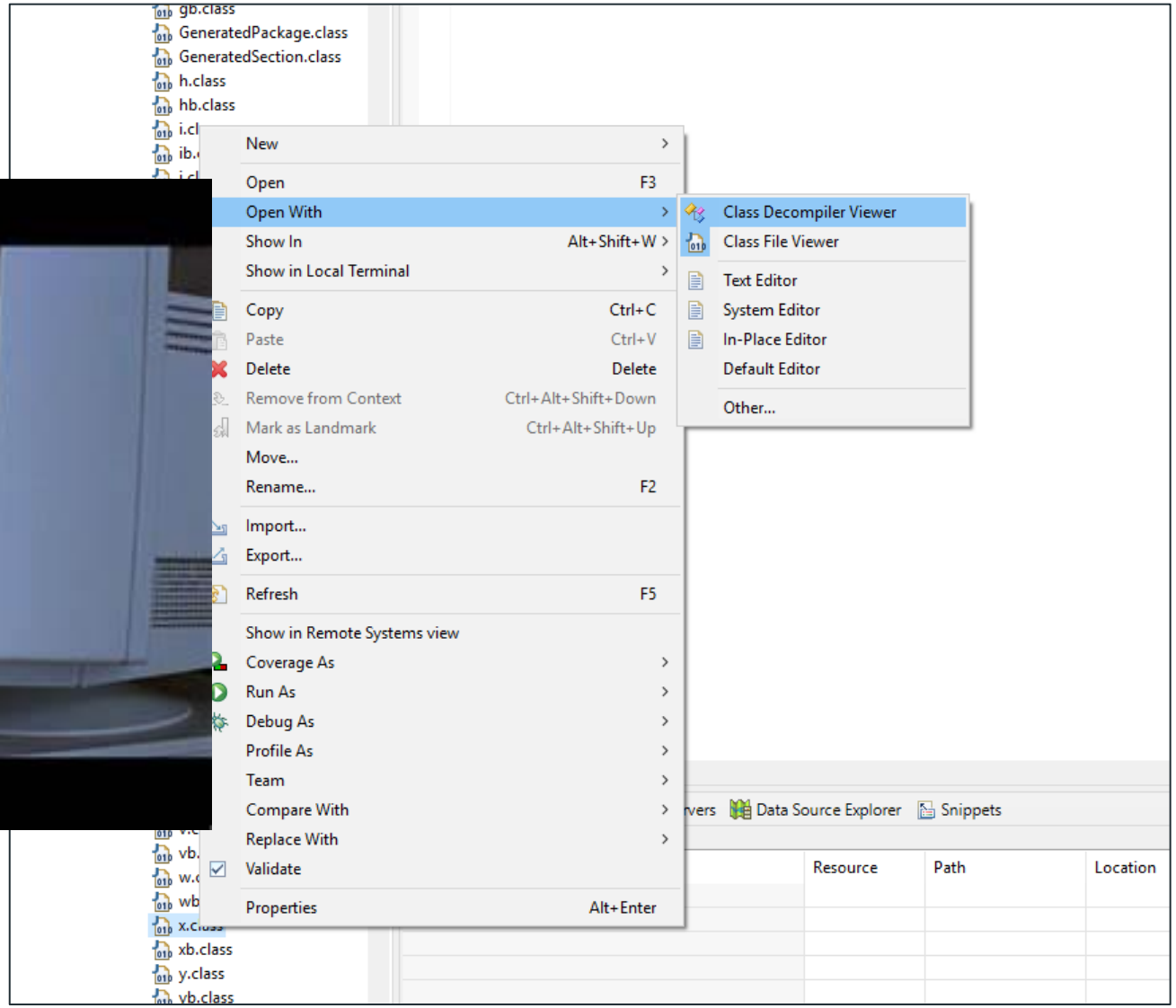
Trust Boundaries



Different File Sizes, Different Contents?

Name	Type	Size
db2jcc.jar	JAR File	2,808 KB
db2jcc-1.4.2.jar	JAR File	3,272 KB

Try Something New



Through The Looking Glass

```java
6   package
7
8
9   class x
10  {
11
12      x(int i, int j, int k, int l, int i1, int j1, int k1,
13              int l1)
14      {
15          a = i;
16          b = j;
17          c = k;
18          d = l;
19          e = i1;
20          f = j1;
21          g = k1;
22          h = l1;
23      }
24
25      public void a(int i, int j, int k, int l, int i1, int j1, int k1,
26              int l1)
27      {
28          a = i;
29          b = j;
30          c = k;
31          d = l;
32          e = i1;
33          f = j1;
34          g = k1;
35          h = l1;
36      }
```

```java
6   package
7
8   import java.io.IOException;
9   import java.net.*;
10  import java.security.PrivilegedExceptionAction;
11
12  public class x
13      implements PrivilegedExceptionAction
14  {
15
16      public x(InetAddress inetaddress, int i, int j)
17      {
18          a = null;
19          a = inetaddress;
20          b = i;
21          c = j;
22      }
23
24      public Object run()
25          throws UnknownHostException, IOException
26      {
27          Socket socket = new Socket();
28          socket.connect(new InetSocketAddress(a, b), c * 1000);
29          socket.setTcpNoDelay(true);
30          socket.setKeepAlive(true);
31          socket.setSoTimeout(c * 1000);
32          return socket;
33      }
34
35      private InetAddress a;
36      private int b;
```

I Think I Found Something

“I’m just an analyst!”

Confirmation & Validation

Both Oracle and IBM confirmed the jar files available via Maven Central were counterfeit

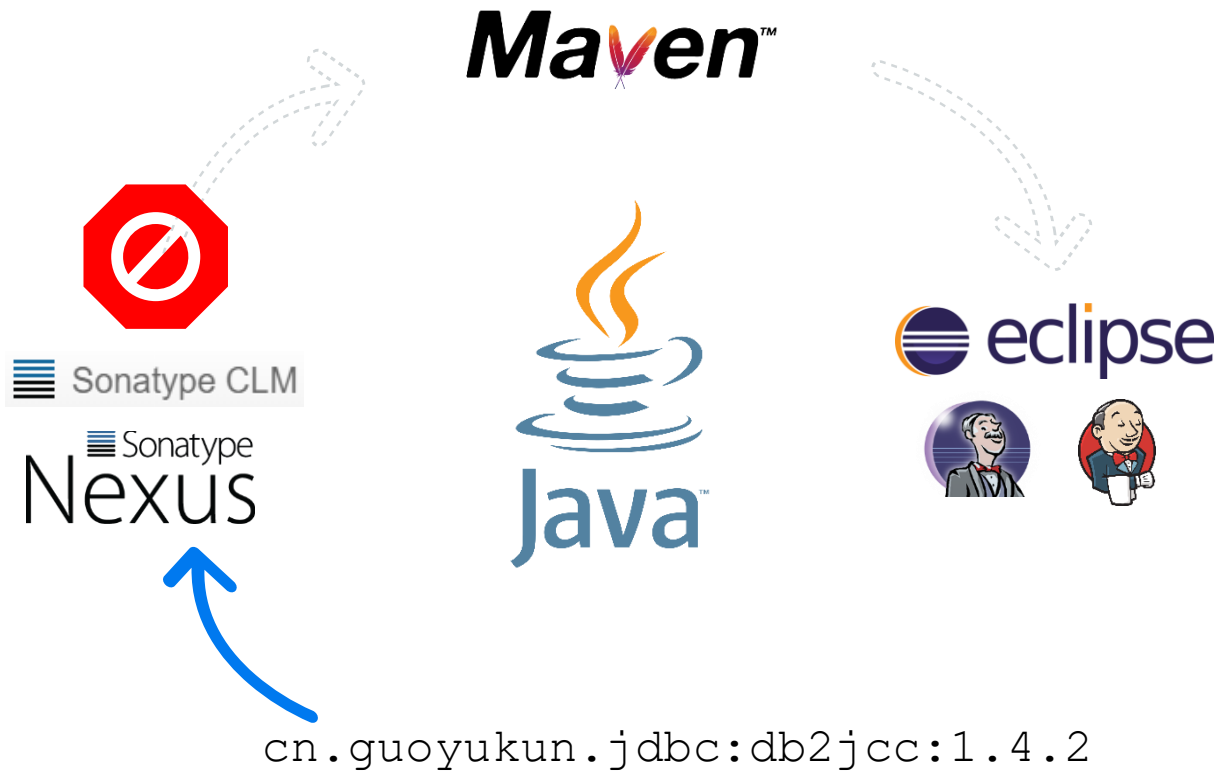
But Why?

Cleanup

The really super folks at Sonatype agreed to remove the counterfeit, potentially dangerous, libraries from Central

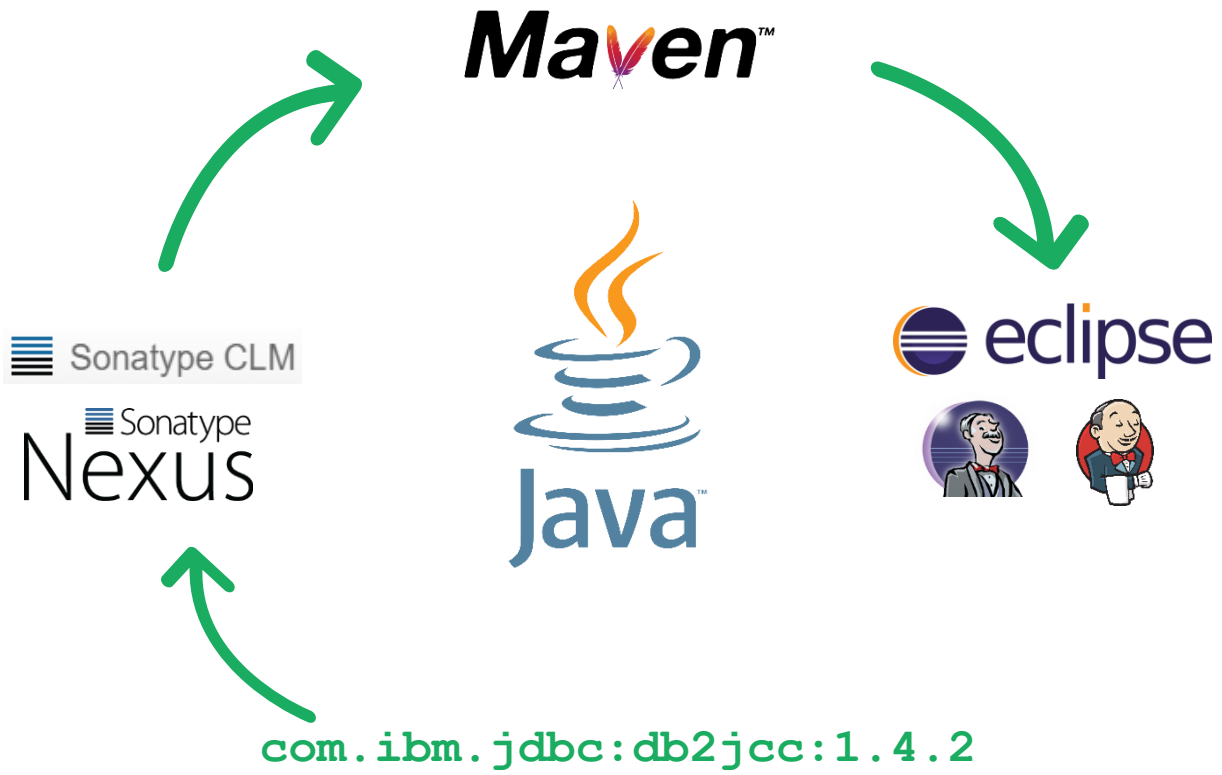
A DevSecOps Win

- Build servers were permitted to only retrieve components from the internal repo proxy
- The internal repo proxy had policies in place to ban components with cn.guoyukun GAVs



Lessons Learned

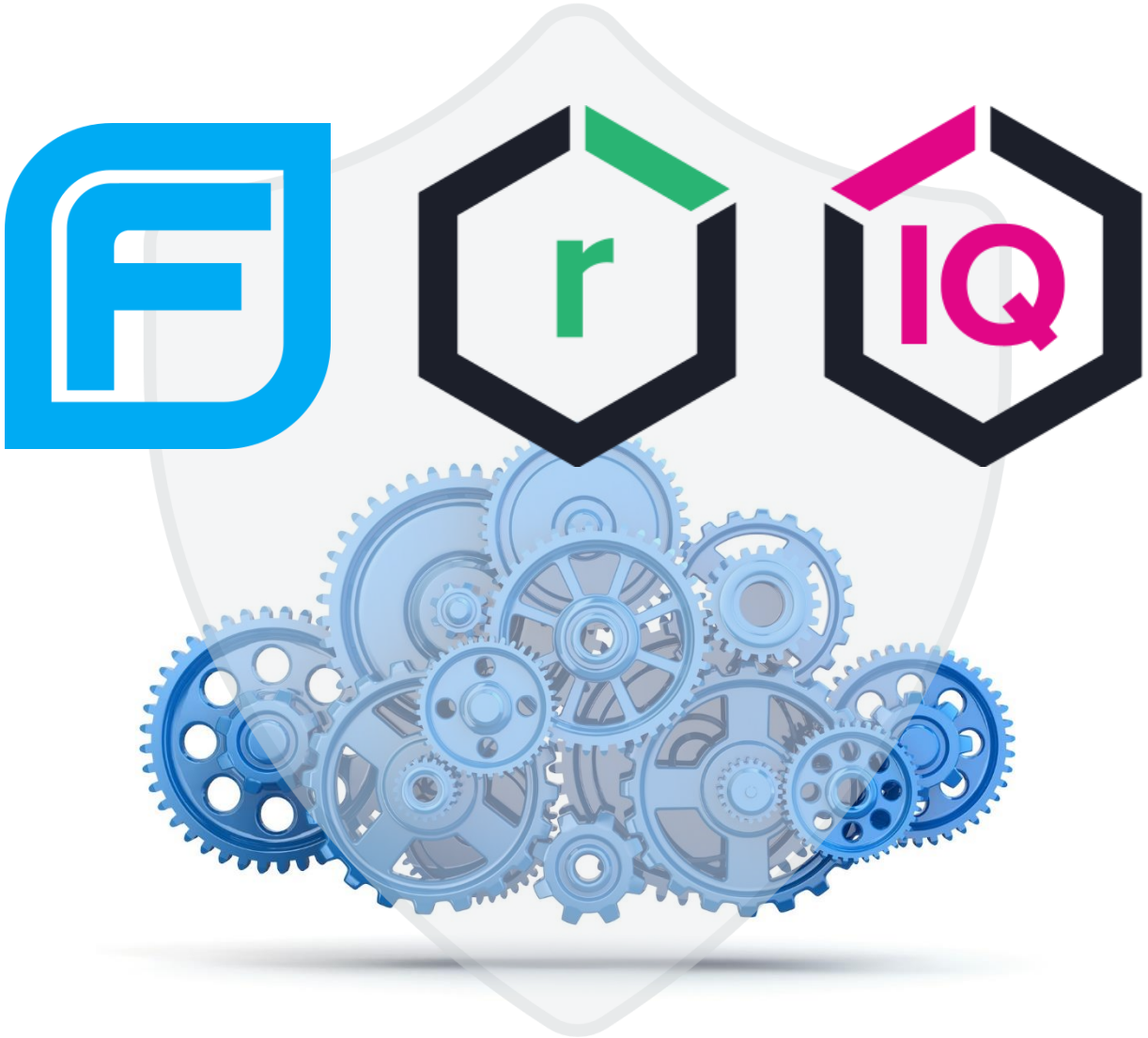
- We worked together to make the vendors' driver files readily available to the organization
- The development team started using the official drivers



Automating Visibility & Policy Enforcement

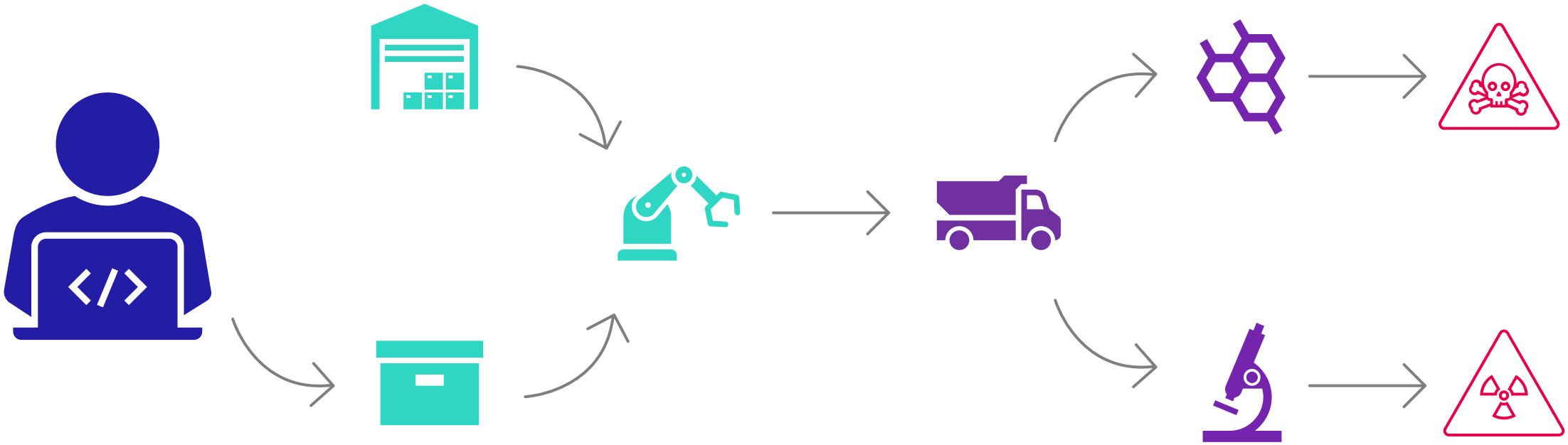
Modern policy creation and enforcement don't have to involve heroic acts

(or movie star good looks)



It can be built right into the DevSecOps toolchain

Static Analysis + Software Composition Analysis



What To Look For

APPLICATIONS DASHBOARD REPORTS ADMINISTRATION

sinister > dev

Open Source Components

57 Components Identified

69 Security Issues
Affecting 14 components

COMPONENT	VERSION	TYPE	KNOWN PUBLIC VULNERABILITIES				
			CRITICAL	HIGH	MEDIUM	LOW	
org.apache.struts:struts2-core	2.0.11	maven	12	5	11	0	Apache-
com.opensymphony:xwork	[illegible]	[illegible]	0	3	6	1	Apache Apache- BSD-3-C OpenSy See-Lice
commons-fileupload:commons-fileuplo...	1.2.1	maven	1	3	1	1	Apache-
dom4j:dom4j	1.4	maven	1	1	0	0	Apache- BSD
struts:struts	1.1	maven	0	6	1	0	
freemarker:freemarker	2.3.8	maven	0	1	1	0	Apache- Gene

Check Out My Demo!

DevSecOps Checklist

- ✓ Relentlessly automate
- ✓ Make it easy
- ✓ Understand trust boundaries
- ✓ Be open
- ✓ Auditable activities

Thank You.

MICRO FOCUS®

THANK YOU!

Meet me in the Network
Chat Lounge for questions

SKILUP DAYS
by: DevOps Institute
ADVANCING THE HUMANS OF DEVOPS