Securing Software Supply Chains

Why 3 Days Might Be Your New Normal for DevSecOps

Cameron Townshend
Solution Architect, APJ, Sonatype
Since 2000, 52% of Fortune 500 have been replaced.

Established business leaders are also under attack…
THE POSSIBILITY OF SUCH DAMAGE.

Apache Software Foundation (Apache Lucene Core,
Closure Library, Kaeli, OpenFst, SwiftProtobuf, Xerces)
Apache License Version 2.0, January 2004
TERMS AND CONDITIONS FOR USE, REPRODUCTION,
AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use,
reproduction, and distribution as defined by Sections 1
through 9 of this document.
"Licenser" shall mean the copyright owner or entity
authorized by the copyright owner that is granting the
License.
"Legal Entity" shall mean the union of the acting entity and
all other entities that control, are controlled by, or are
under common control with that entity. For the purposes
of this definition, "control" means (i) the power, direct or
indirect, to cause the direction or management of
the affairs, or (ii) ownership of fifty percent (50%) or
more of the outstanding shares, or (iii) a mutual
arrangement or participations between the original
contracting parties.

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, **1945**
Gene Kim, 2013
Lots of learning

Requirements Gathering -> Development -> Test and Quality Assurance -> Release

Minimal learning

Some learning

*Source: Amazon*
59,000 data breaches have been reported to GDPR regulators since May 2018.

Source: DLA Piper, February 2019
Business applications are under attack…

51% Of enterprises suffered at least one breach in last 12 months.

43% Of enterprise attacks are perpetrated by external actors.

68% Of external attacks target web apps and known vulnerabilities.

Forrester: Best Practices for Deploying And Managing Enterprise Password Managers – Jan 2018
Everyone has a software supply chain.
(even if you don’t call it that)
Demand drives 15,000 new releases every day
Automation accelerates OSS downloads

Download Requests for Java Components 2008-2018 are a proxy for the popularity of automated software development.

Source: Sonatype’s 2018 State of the Software Supply Chain Report
85% of your code is sourced from external suppliers
170,000 Java component downloads annually
3,500 unique

source: 2018 State of the Software Supply Chain Report
60,660 JavaScript packages downloaded per developer per year

source: npm, 2018
Not all parts are created equal.
We are not “building quality in”.
2016 Java Downloads

source: 2019 State of the Software Supply Chain Report

source: 2017 State of the Software Supply Chain Report
We are not “building quality in”.

10.3%

2018
Java

source: 2019 State of the Software Supply Chain Report
We are not “building quality in”.

51%

2018 npm

source: 2018 npm
Defects targets per million for 6-sigma
170,000 java component downloads annually

3,500 unique

18,870 11.1% with known vulnerabilities
60,660 JavaScript packages downloaded annually per developer

30,936 51% with known vulnerabilities
Developers continue to believe security is important but don’t have enough time to spend on it.

- 50% in 2017
- 48% in 2018
- 48% in 2019
Social normalization of deviance

“People within the organization become so much accustomed to a deviant behavior that they don't consider it as deviant, despite the fact that they far exceed their own rules for elementary safety.”

Diane Vaughan
Breaches increased 71% from 2014 to 2019.

- In 2014, 14% suspect or have verified a breach related to open source components.
- In 2019, 24% suspect or have verified a breach related to open source components, making it 1 in 4 breached.

Source: DevSecOps Community Survey 2014 and 2019
The speed of exploits has compressed 93%

Sources: Gartner, IBM, Sonatype
Quickly identify who is faster than their adversaries
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

March 9
Cisco observes “a high number of exploitation events.”

March 10
Equifax

March 13
Okinawa Power

March ’18
India’s AADHAAR

The Rest of the Story

March 10
Canada Revenue Agency
Canada Statistics
GMO Payment Gateway

December ’17
Monero Crypto Mining

Today
65% of the Fortune 100 download vulnerable versions

Equifax was not alone
Complete software bill of materials (SBOM)

- 2019 No DevOps Practice: 19%
- 2019 Mature DevOps Practices: 50%

Source: 2019 DevSecOps Community Survey
18,126 organizations downloading vulnerable versions of Struts
DevSecOps challenge: automate faster than evil.
1.3 million vulnerabilities in OSS components undocumented
No corresponding CVE advisory in the public NVD database

Source: www.recordedfuture.com/chinese-vulnerability-reporting/, Sonatype
The new battlefront
Software Supply Chain Attacks

1. 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).

2. 10 Malicious Python packages
   Basic info collected and sent to Chinese IP address

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

4. Golang go-bindata github id deleted and reclaimed.

5. Conventional-changelog compromised and turned into a Monero miner.

   Unauthorized publishing of mailparser.

7. ssh-decorator Python Module stealing private ssh keys.

8. Gentoo Linux Repository Compromised.

9. Malicious Eslint discovered to be stealing npm credentials.

10. Homebrew repository compromised.

11. npm event-stream attack on CoPay.
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.
Which application security tools are used?

- **Web Application Firewall**: 70% (2019 No DevSecOps Practice), 85% (2019 Mature DevSecOps Practices)
- **Container and Application Security**: 60% (2019 No DevSecOps Practice), 91% (2019 Mature DevSecOps Practices)
- **Open source governance**: 56% (2019 No DevSecOps Practice), 84% (2019 Mature DevSecOps Practices)
- **Static Application Analysis**: 55% (2019 No DevSecOps Practice), 77% (2019 Mature DevSecOps Practices)
- **Dynamic Application Analysis**: 40% (2019 No DevSecOps Practice), 70% (2019 Mature DevSecOps Practices)
How are you informed of InfoSec and AppSec issues?

Automating security enables faster DevOps feedback loops
Automation continues to prove difficult to ignore

<table>
<thead>
<tr>
<th>2019 No DevOps Practice</th>
<th>2019 Mature DevOps Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>75% no policy or ignore it</td>
<td>38% no policy or ignore it</td>
</tr>
<tr>
<td>25% YES</td>
<td>62% YES</td>
</tr>
</tbody>
</table>

Source: 2019 DevSecOps Community Survey
Trusted software supply chains are 2x more secure

Source: 2018 State of the Software Supply Chain Report
“I see no prospect in the long run for avoiding liability for insecure code.”

Paul Rozenzweig
Senior Fellow, R Street Institute
2018
The rising tide of regulation and software liability

Source: Sonatype
Note: Organizations listed multiple times introduced new or strengthened policies at different points along the timeline.
1. An up to date inventory of open-source components utilized in the software

2. A process for identifying known vulnerabilities within open source components

3. 360 degree monitoring of open source components throughout the SDLC

4. A policy and process to immediately remediate vulnerabilities as they become known

All Countries Show Poor Cyber Hygiene

Source: Siotetype
“Emphasize performance of the entire system and never pass a defect downstream.”
ctownshend@sonatype.com