anchore

Learn from Log4shell

Using SBOMs for Zero-Day Preparadness

Hello World

Paul Novarese

Senior Solutions Architect

Anchore

pvn@anchore.com

anchore

Agenda

00 Supply Chain Attacks

01 Log4Shell - What Actually Happened

02 Software Bill of Materials

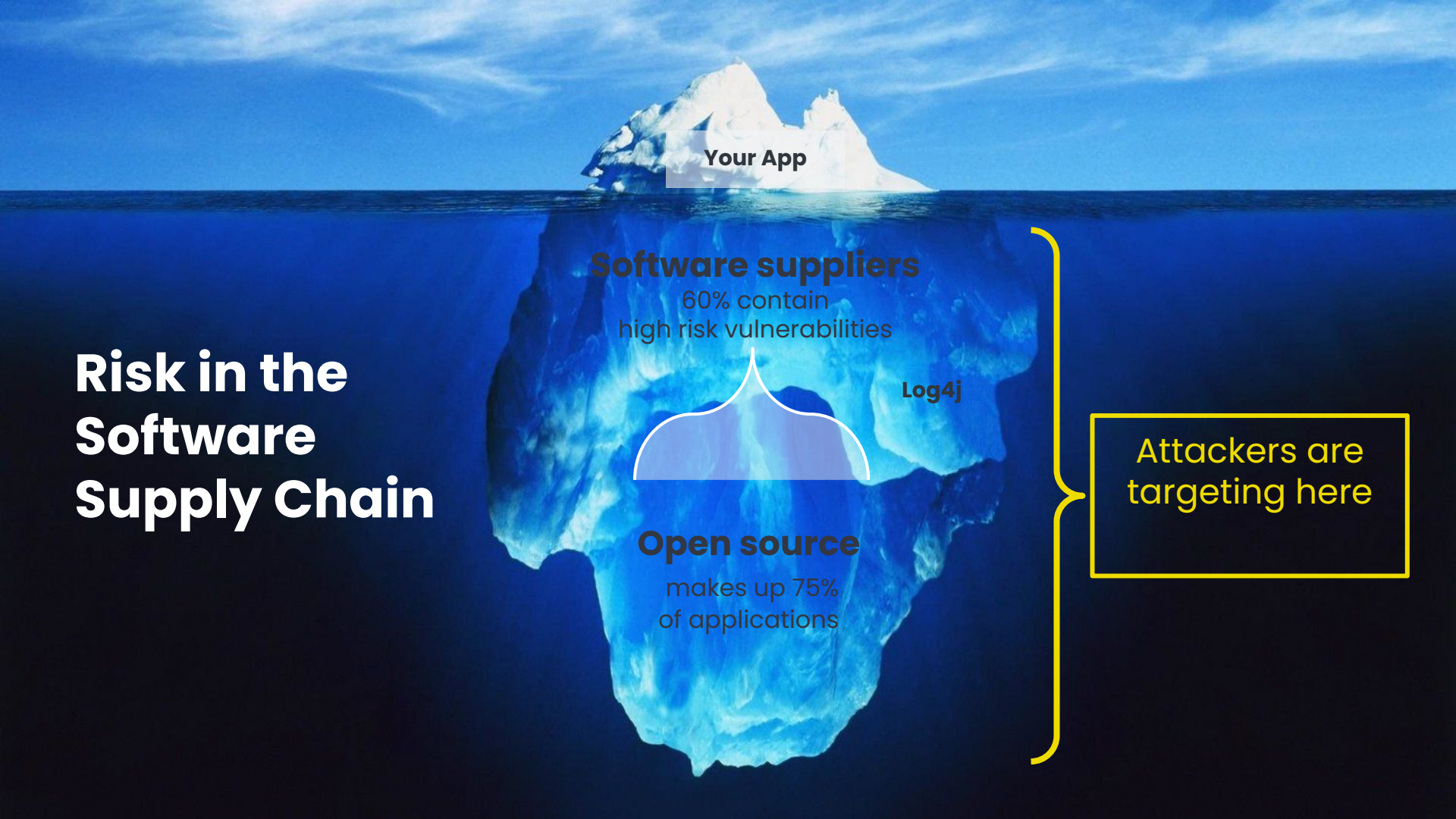
03 Now what?

anchore

anchore

What are Supply Chain Attacks?

Risk in the Software Supply Chain

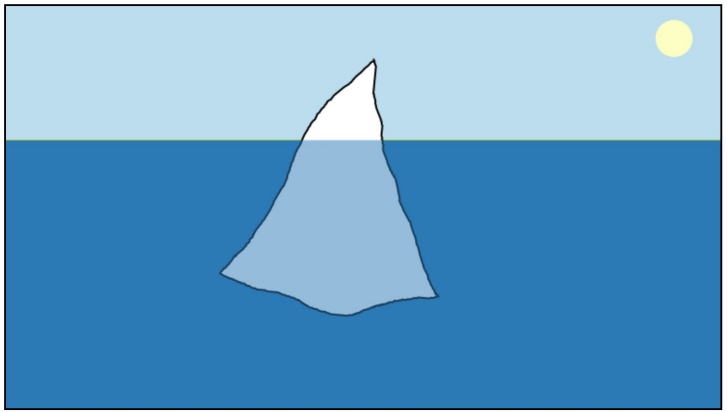



WRONG

Iceberger

Draw an iceberg and see how it will float.

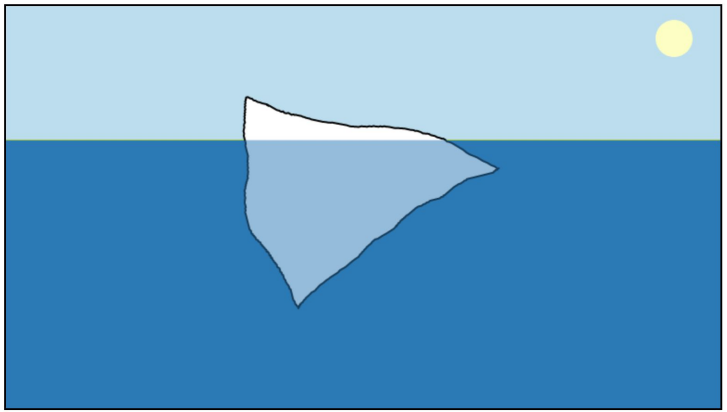
(Inspired by a tweet by @GlacialMeg)



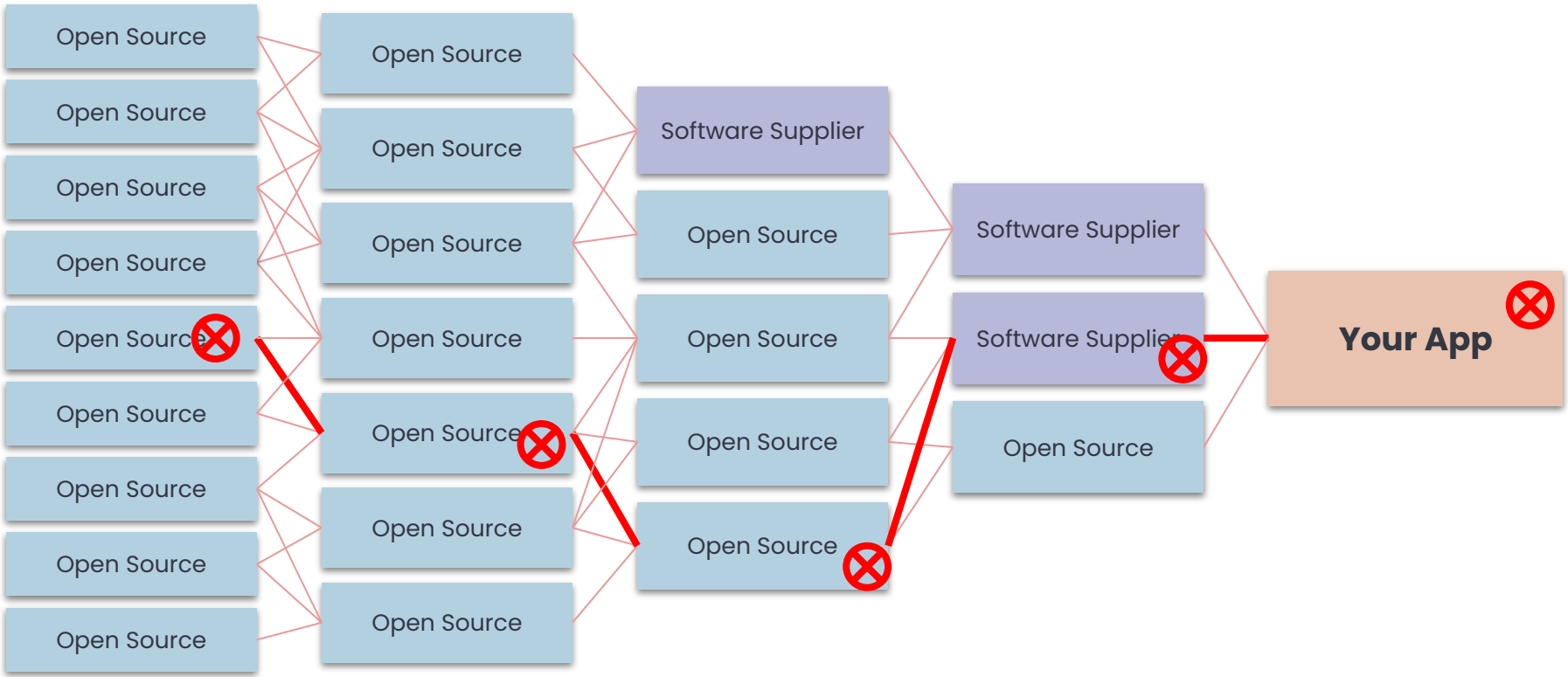
Iceberger

Draw an iceberg and see how it will float.

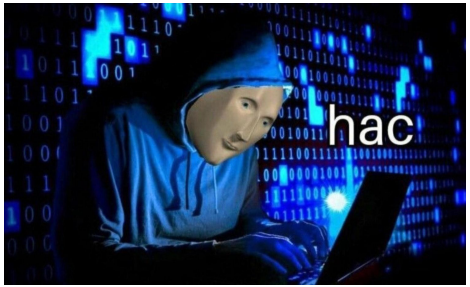
(Inspired by a tweet by @GlacialMeg)



Software Supply Chain: The Funnel



The Reverse Funnel



Compromised Package

Open Source

Open Source

Open Source

Downstream Consumer

Open Source

Open Source

Open Source

Open Source

Downstream Consumer

Open Source

Open Source

Open Source

Open Source

Downstream Consumer

Downstream Consumer

Downstream Consumer

Downstream Consumer

Open Source

Open Source

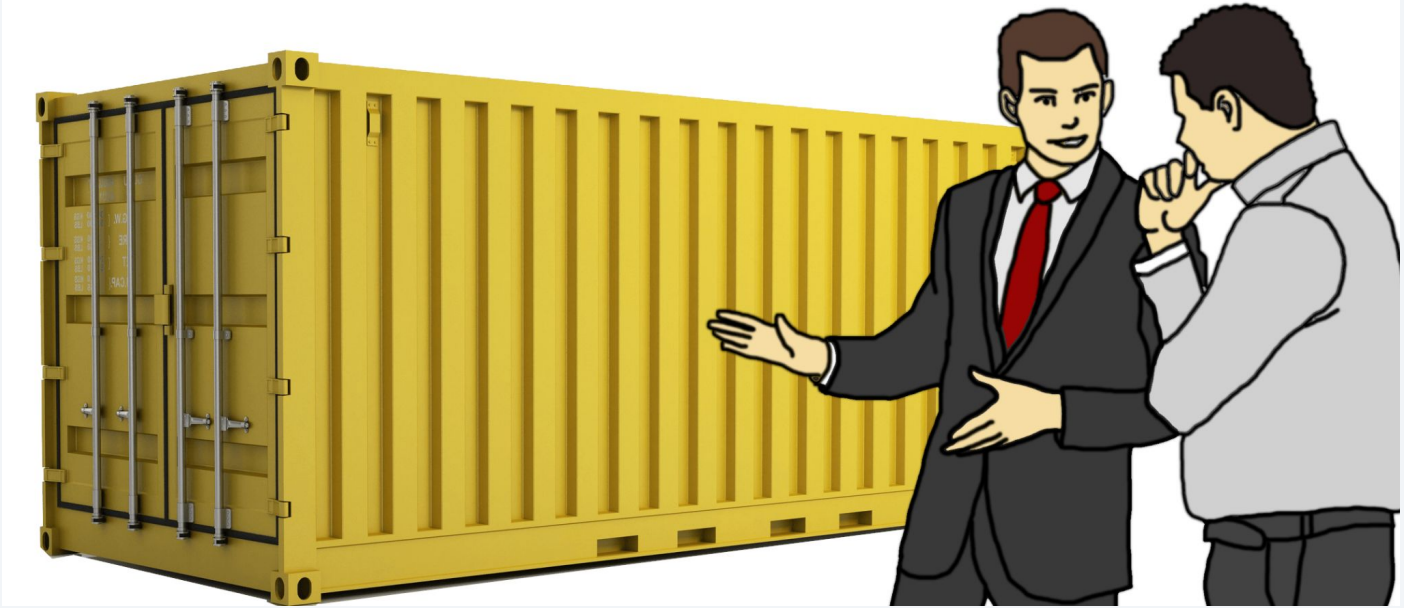
Open Source

Open Source

Open Source

anchore

slaps roof of container this bad boy can fit so many supply chain attacks in it



anchore

Log4Shell Impact

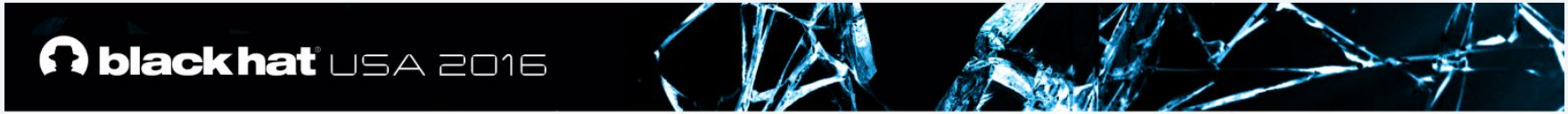
What is log4j? What is log4shell?

What is log4j? What is log4shell?

Log4Shell Timeline

- 2001 - Initial release
- 14 Sep 2013 - Vulnerability is introduced 2.0-beta9
- 3 Aug 2016 - Potential exploit presented at Black Hat

2016-08-03



BlackHat Sound Bytes

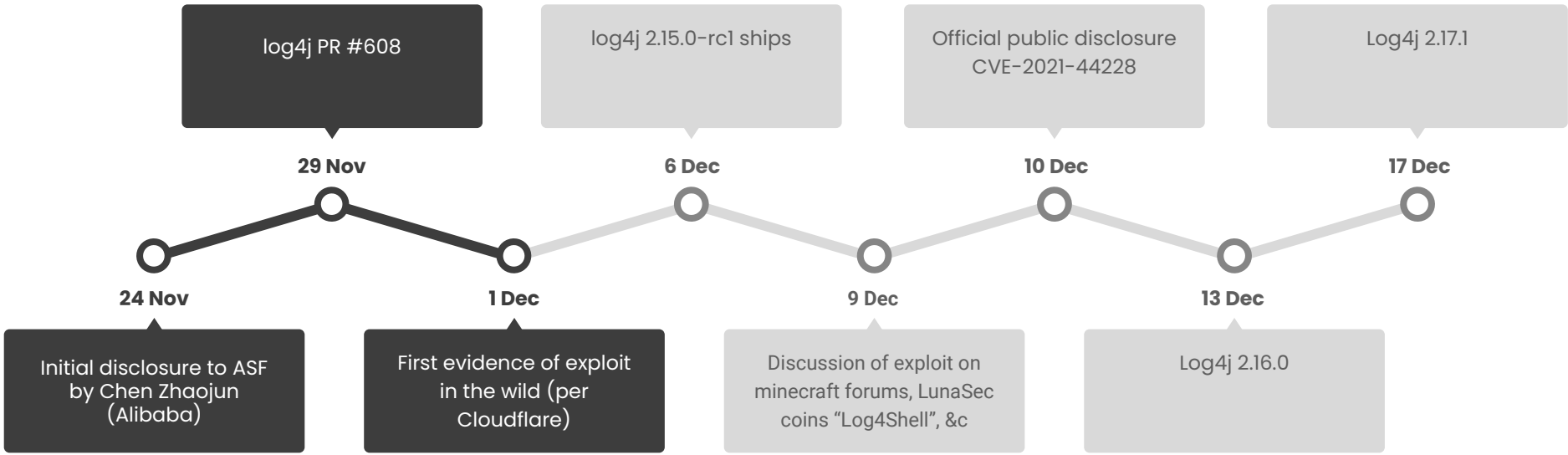
- Audit your Applications for two new vulnerability classes:
  - JNDI Injection
  - LDAP Entry Poisoning
- Carefully protect and periodically audit your LDAP backends; they contain the keys to your kingdom!

Dan Kaminsky
@dakami

Amateurs think about vulnerabilities, professionals think about vectors.

4:04 PM · Aug 12, 2017 · Twitter Web Client

Log4Shell Timeline



anchore

Paul Novarese
Software Supply Chain Security at Anchore
9mo · Edited

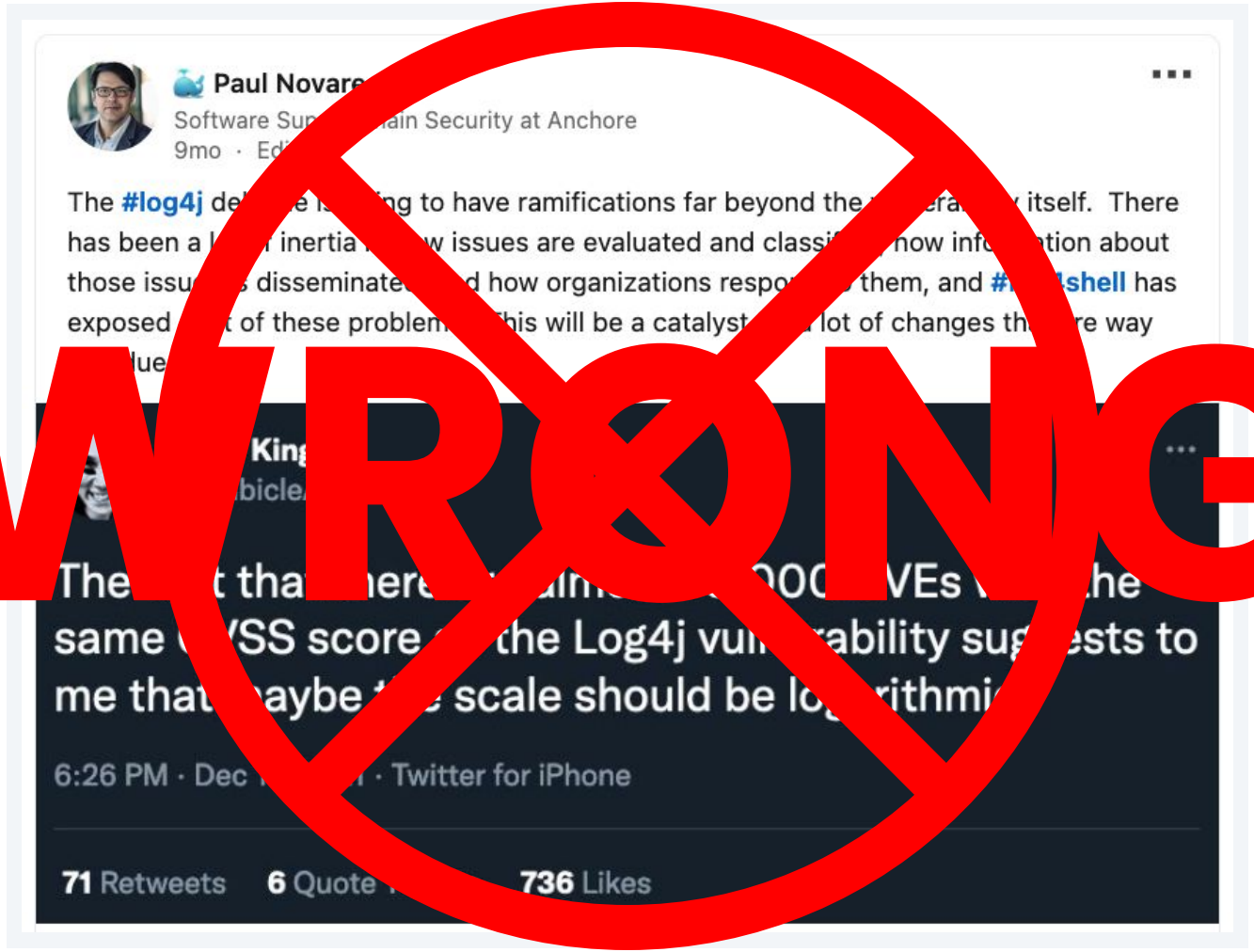
The #log4j debacle is going to have ramifications far beyond the vulnerability itself. There has been a lot of inertia in how issues are evaluated and classified, how information about those issues is disseminated, and how organizations respond to them, and #log4shell has exposed a lot of these problems. This will be a catalyst for a lot of changes that are way overdue.

April King
@CubicleApril

The fact that there are almost 10,000 CVEs with the same CVSS score as the Log4j vulnerability suggests to me that maybe the scale should be logarithmic.

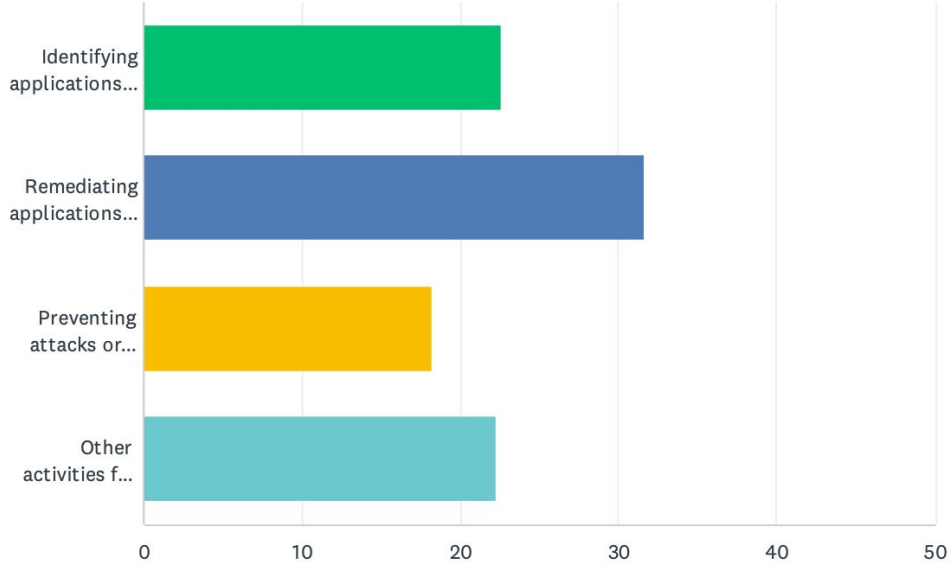
6:26 PM · Dec 11, 2021 · Twitter for iPhone

71 Retweets **6** Quote Tweets **736** Likes


Paul Novare
Software Sup ain Security at Anchore
9mo · Ed
The #log4j de g to have ramifications far beyond the era itself. There
has been a l inertia ow issues are evaluated and classi how info tion about
those issu disseminate d how organizations respo them, and # shell has
exposed t of these problem his will be a catalyst lot of changes th re way
lue
King
bicle
The t tha here aim 000 VEs the
same VSS score the Log4j vul rability sug ests to
me that aybe scale should be lo rithmi
6:26 PM · Dec · Twitter for iPhone
71 Retweets 6 Quote 736 Likes
WRONG

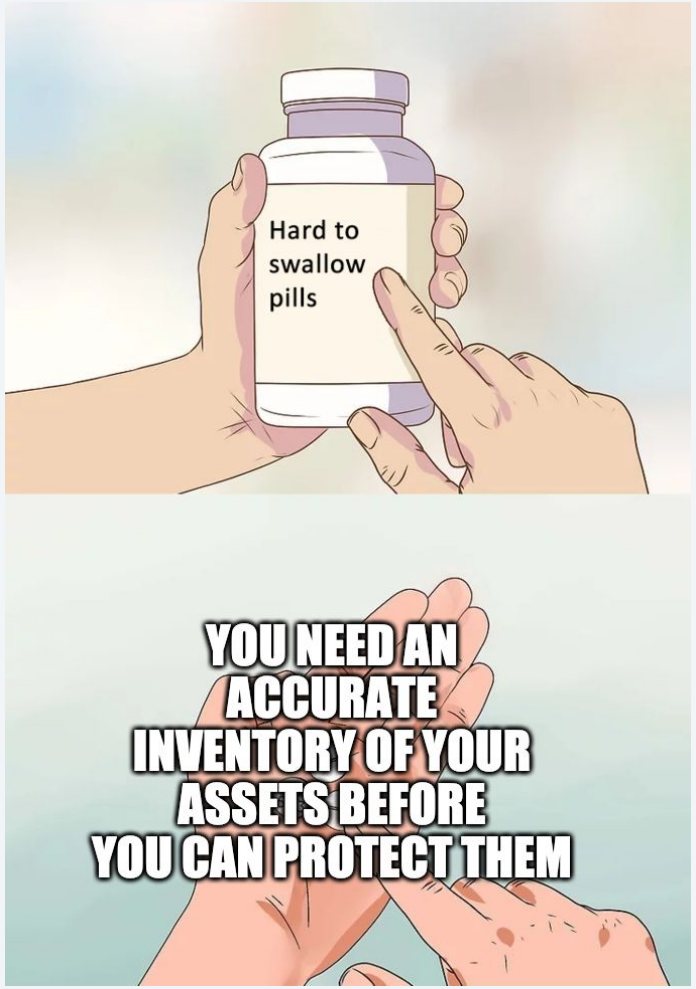
Q12 Estimate how many hours you personally have spent to date on each of the following activities.

Answered: 195 Skipped: 15



anchore

What is a Software Bill of Materials?


Hard to swallow pills
YOU NEED AN ACCURATE INVENTORY OF YOUR ASSETS BEFORE YOU CAN PROTECT THEM

What is an SBOM?

anchore

Beyond CVEs: Overlooked Vectors

01

Software Vulnerabilities

Known vulnerabilities affecting software components that containers and applications depend on - OS packages, direct application dependencies.

02

Malware and Trojan Horses

Malicious code injected into regular application executables during the build process.

03

Software Overrides

Attacks that result in unintentional versions of (typically) dependencies being installed. Name-squatting, max version attacks, typosquatting.

04

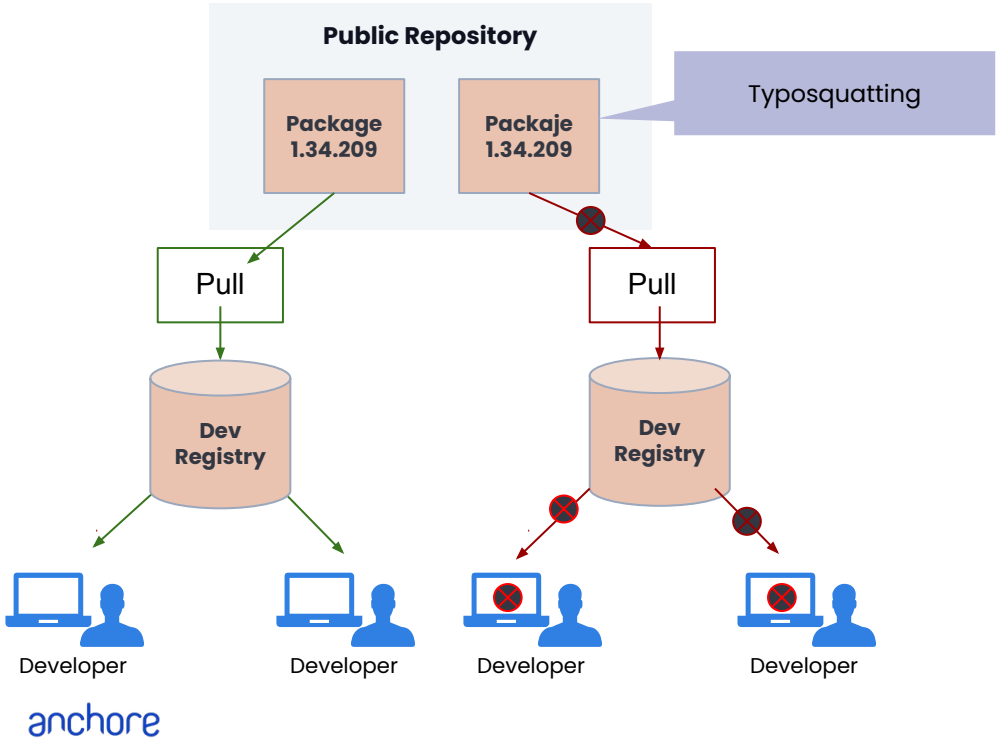
Credentials

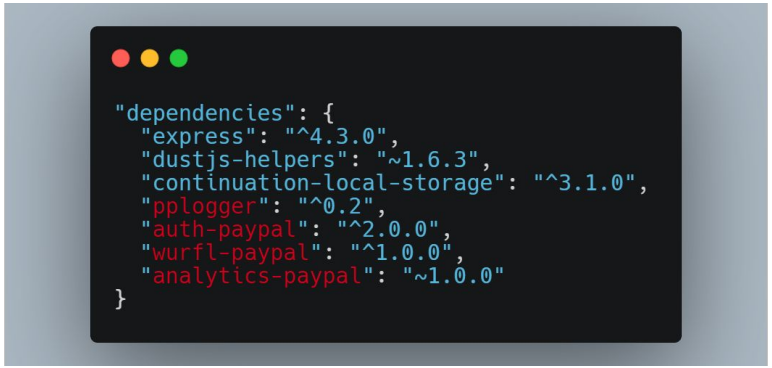
Unintentional inclusion of dev or prod secrets, keys, or other credentials accidentally included in the container.

Software vulnerabilities (often reported as CVEs) are critical to detect and report, but many other build-time attack vectors must also be considered.

anchore

Know What You're Getting





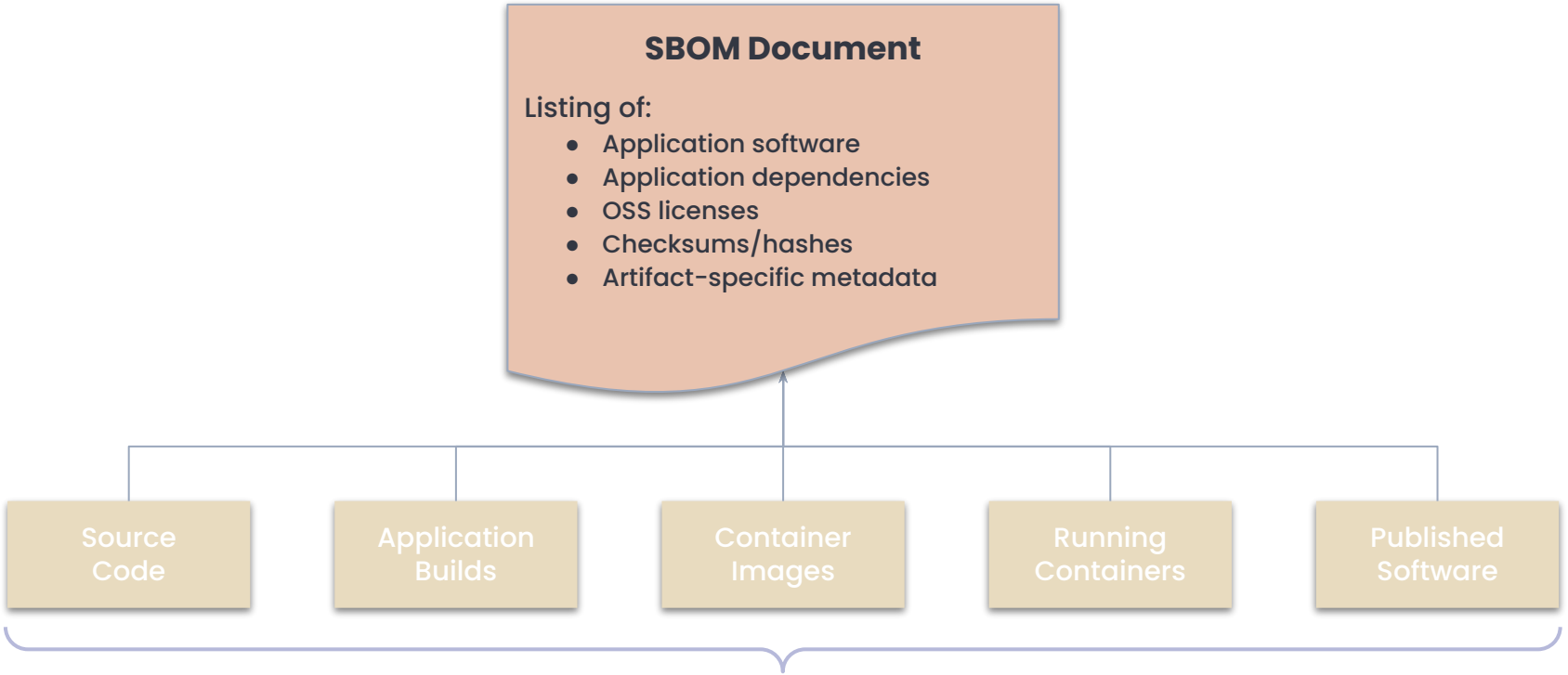
Dependency Confusion

anchore

Addressing the Problem

anchore

What is an SBOM?



Types of artifacts from which SBOMs can be generated

Existing SBOM formats

	SPDX "Software Package Data eXchange"	**CycloneDX**	**SWID** "Software ID"
Organization	SPDX Workgroup (~20 orgs) under the Linux Foundation	A "meritocratic, consensus-based community project" with a Industry Working Group	ISO/IEC Joint Technical Committee Trusted Computing Group
Initial Draft	2010	2017	2009
Formats	RDF, XLS, SPDX, YAML, JSON	XML, JSON	XML, CBOR (CoSWID only)
Spec	spdx.github.io/spdx-spec BS ISO/IEC 5962 - 2020 Draft	github.com/CycloneDX/specification	iso.org/standard/65666.html ISO/IEC 19770-2:2015

Existing SBOM formats: Use Cases

	SPDX "Software Package Data eXchange"	**CycloneDX**	**SWID** "Software ID"
Original use cases	License management	For use with OWASP Dependency-Track	Inventory and change tracking
Unique Features	Extensive support for expressing license details	Extensible format and integrates SPDX license IDs, pURL, and other external identifiers	Deeply integrated into the build and publishing process for a software component
Use cases of latest format versions	• Tracking attributes of multiple software components (e.g. vendor, license, version, etc.) • Generically describe packages, containers, os distributions, archives, etc • Integrity verification of software components and sub-components		

A “good” SBOM describes...

What is being catalogued	Each item uniquely	What did the cataloguing
For example a running system, a machine image, a container image, etc.	Such as each component name, version, UUID, and relationships to other components.	The tool that generated the document with its configuration.

A “great” SBOM also includes...

In scope and out of scope

For example “only these paths were searched” or “only JARS and RPMs are being search for”.

Exceptional conditions

Such as warnings or errors that occur during processing or missing environmental factors

Additional metadata

Such as Java pom properties, key-values, additional RPM DB tag entries, and licenses.

anchore

Introducing Syft

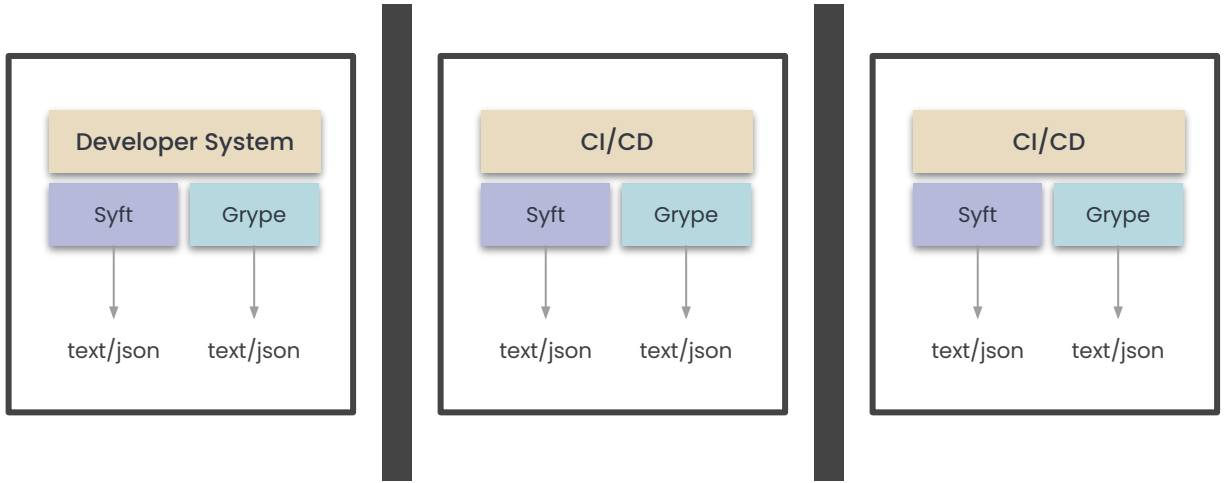
- Syft is an **open source tool that generates SBOMs** from container images and filesystems

- Syft supports **many package ecosystems:**
  - APK, DEB, RPM, Ruby Bundle, Python Wheel/Egg/requirements.txt, JavaScript NPM/Yarn, Java JAR/EAR/WAR, Jenkins plugin JPI/HPI, Go modules, Rust Crate

- Syft also supports **multiple output formats**
  - Syft-Native
  - CycloneDX
  - SPDX

Anchore Open Source

Open Source | Stateless, decentralized tools for developers



Syft
Generates an SBOM for a container image

Grype
Generates a list of CVEs using the SBOM

Open Source

- **Lightweight** tools, written in **Go**
- **API-driven** to run in CI/CD
- **Linux** containers only
- **Local credentials** only
- **Stateless**, no data persistence
- **Siloed,** no centralized control

anchore

anchore

Now What?

How will this improve my life?

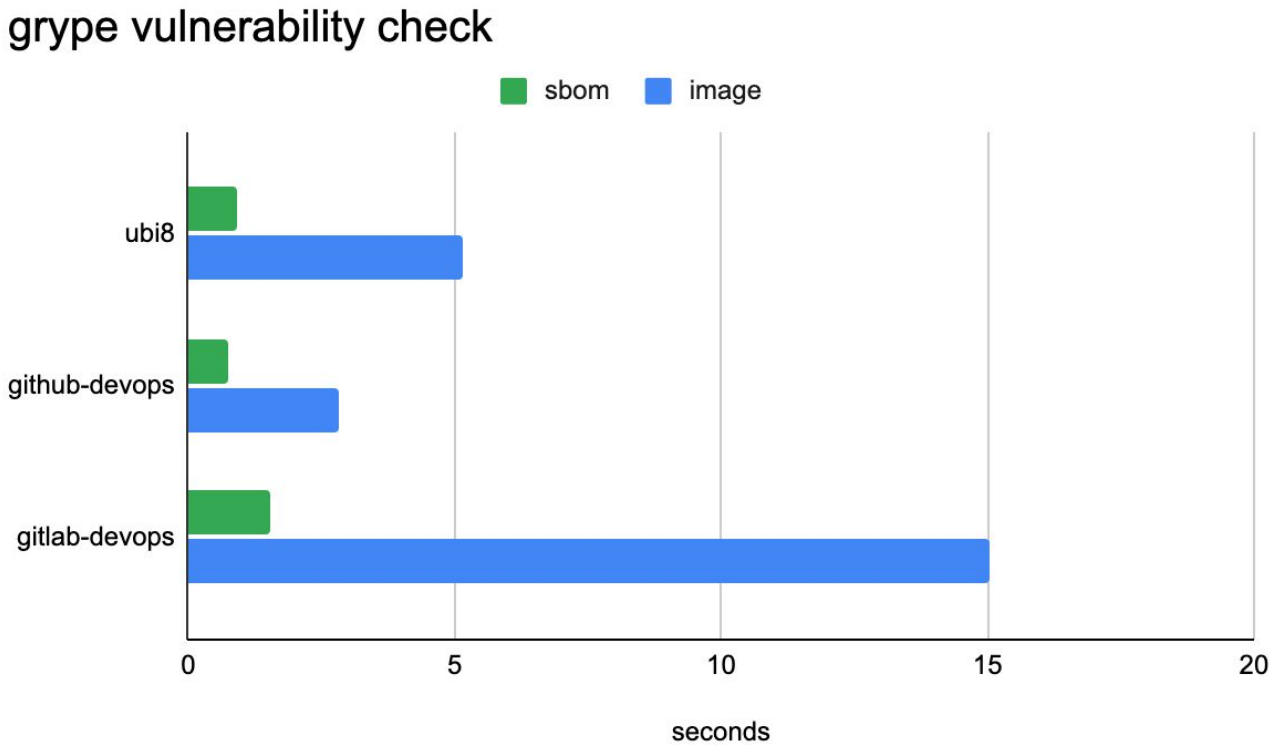
One Last Bad Analogy

How Do SBOMs Actually Help?

anchore

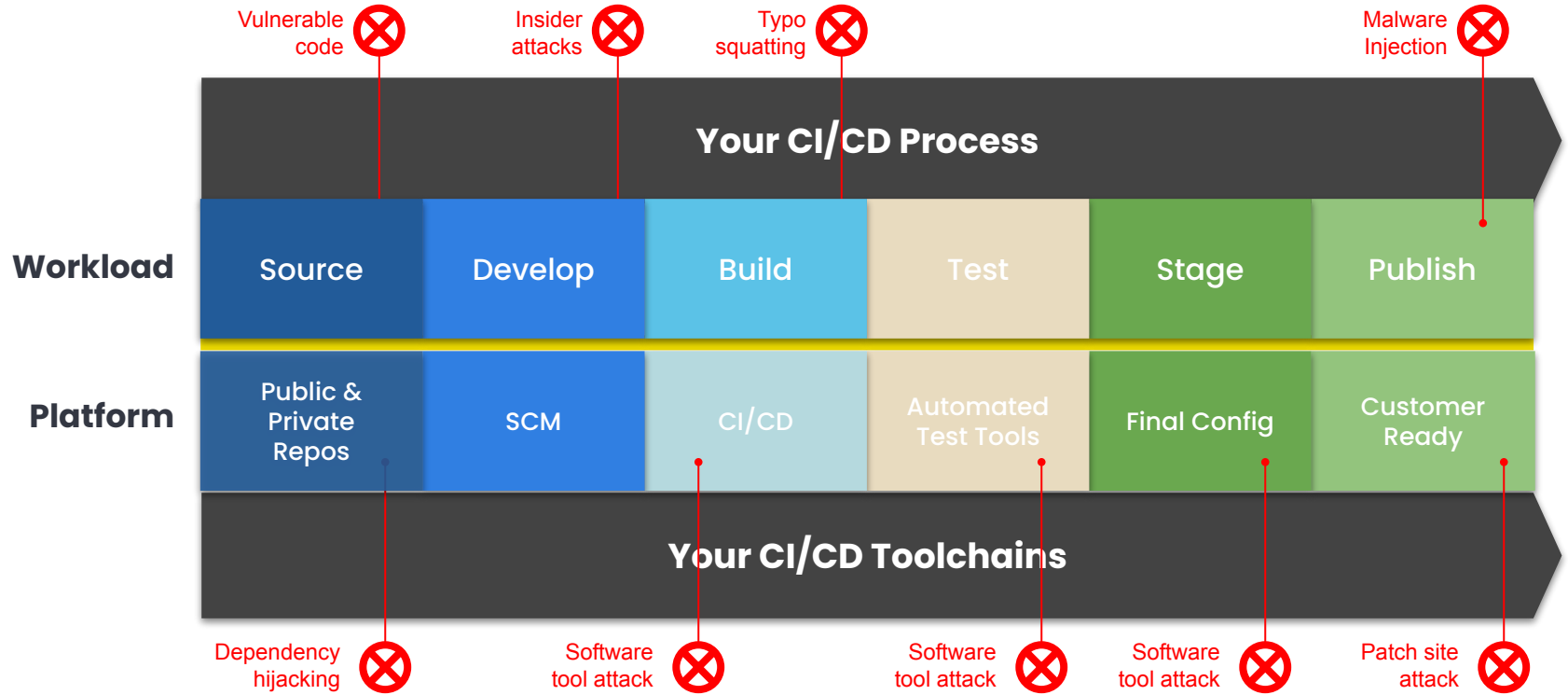
Grype Scan Timing

	ubi8	github -devops	gitlab -devops
sbom	0.917	0.751	1.55
image	5.159	2.839	15.031



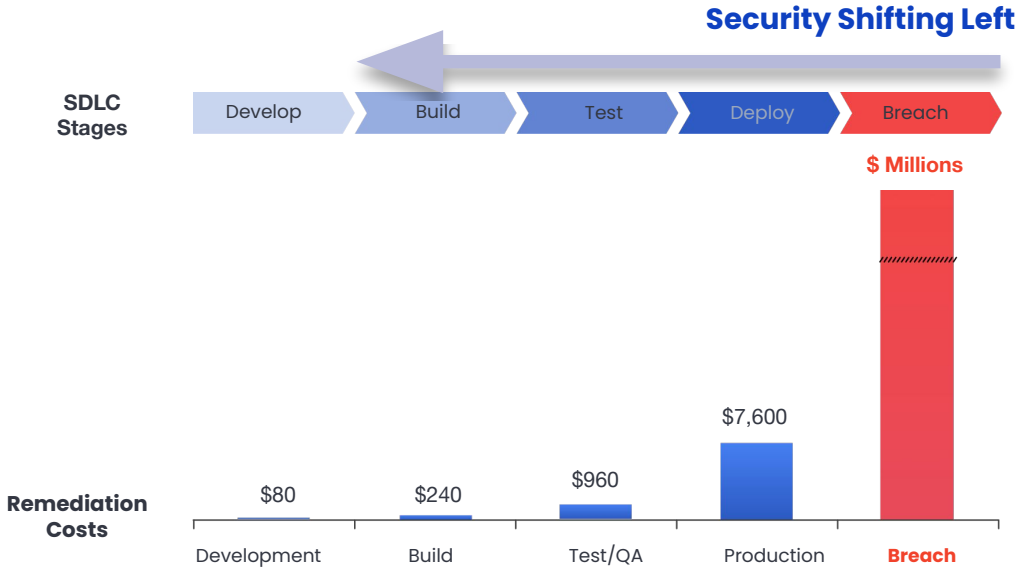
anchore

SBOMs Enable Continuous Evaluation

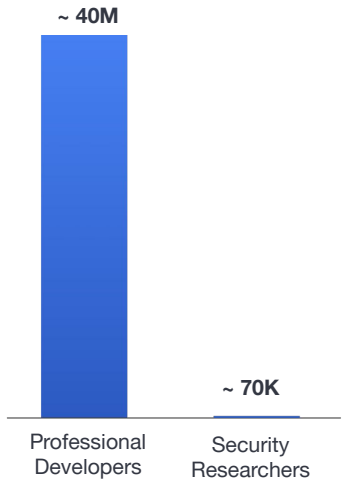


anchore

Shift Security Left



Vastly more cost effective to remediate during development



570x more developers than security researchers

anchore


STOP TALKING
DEMO TIME


LET'S DO
A DEMO
memegenerator.net


I CAN HAS DEMO?


DEMO?
WHAT COULD GO WRONG?


DEMO TIME
memegenerator.net

Paul V. Novarese
@pvn

When I tweak the demo 10 minutes before my presentation

8:41 PM · Aug 26, 2018 · Twitter for iPhone

DIY Demos

- **Create SBOMs, Find log4j, Integrate with Jenkins (Difficulty: Easy)**
  - https://github.com/pvnovarese/2022-10-devopsdays
  - Includes instructions on deploying a disposable Jenkins container

- **Additional Labs (Difficulty: Medium)**
  - https://github.com/pvnovarese/2022-devopsworld
  - Additional Labs

- **Brand new GitHub SBOM Action:**
  - https://github.com/marketplace/actions/anchore-sbom-action

Takeaways

00 Massive shift in how info is spread (mailing lists/CVEs -> twitter/reddit &c)

01 Don’t assume it will be a one-shot fix

02 SBOMs enable continuous vulnerability checks

03 Use SBOMs to reduce time spent identifying and remediating issues

anchore

anchore

Q&A

Download Syft

https://github.com/anchore/syft

Download Grype

https://github.com/anchore/grype

Let us know if you like it by giving us a star on GitHub

Get an invite to our open source community Slack at
https://anchore.com/slack/

Jake Williams
@MalwareJake

Hey infosec: remember that your job is risk reduction, not risk elimination. There's a BIG difference.

9:31 PM · Aug 29, 2021 · Twitter for Android

258 Retweets **26** Quote Tweets **1,677** Likes

Bibliography &c

Dealing with log4shell (detection, mitigation, workarounds):
https://cloudsecurityalliance.org/blog/2021/12/14/dealing-with-log4shell-aka-cve-2021-44228-aka-the-log4j-version-2/

Keeping up with log4shell (post mortem)
https://cloudsecurityalliance.org/blog/2021/12/16/keeping-up-with-log4shell-aka-cve-2021-44228-aka-the-log4j-version-2/

Mysterious tweet hinting at the exploit:
https://twitter.com/sirifu4k1/status/1468951859381485573

Another mysterious tweet:
https://twitter.com/CattusGlavo/status/1469010118163374089

“THE” pull request:
https://github.com/apache/logging-log4j2/pull/608

Cloudflare digs for evidence of pre-disclosure exploits in the wild:
https://twitter.com/eastdakota/status/1469800951351427073

Reading List

Maslow's Hierarchy of Supply Chain Needs: https://www.youtube.com/watch?v=rcP8QHFMwCw

Reflections on Trusting Trust: https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf

Generate sboms with syft and jenkins: https://www.youtube.com/watch?v=nMLveJ_TxAs

Solar Winds post mortem: https://www.lawfareblog.com/solarwinds-and-holiday-bear-campaign-case-study-classroom

SPDX becomes sbom standard:
https://www.linuxfoundation.org/press-release/spdx-becomes-internationally-recognized-standard-for-software-bill-of-materials

Profound Podcast - Episode 10 (John Willis and Josh Corman):
https://www.buzzsprout.com/1758599/8761108-profound-dr-deming-episode-10-josh-corman-captain-america

Creating a trusted container supply chain: https://thenewstack.io/creating-a-trusted-container-supply-chain/

Accuracy and Precision: https://wps.prenhall.com/wps/media/objects/3310/3390101/blb0105.html

Footnotes

Other notes:
Slide 2: https://twitter.com/codinghorror/status/786667942142435329
Slide 7: https://joshdata.me/iceberger.html
Slide 16: https://twitter.com/dakami/status/896477575475642368
Slide 14-15: https://www.blackhat.com/docs/us-16/materials/us-16-Munoz-A-Journey-From-JNDI-LDAP-Manipulation-To-RCE.pdf
Slide 17: https://hypixel.net/threads/psa-there-is-a-fatal-remote-code-execution-exploit-in-minecraft-and-its-by-typing-in-chat.4703238/
Slide 17: https://twitter.com/__r__netsec/status/1469120458083962882
Slide 17: https://twitter.com/eastdakota/status/1469800951351427073
Slide 18-19: https://twitter.com/CubicleApril/status/1469825942684160004
Slide 18-19: https://www.linkedin.com/posts/novarese_log4j-log4shell-activity-6876206319238463488-8bEA
Slide 26: https://en.wikipedia.org/wiki/USA-247
Slide 45: https://twitter.com/malwarejake/status/1432168973970313221

Images used for SBOM generation timing benchmarks:

- registry.access.redhat.com/ubi8:latest
- https://gitlab.com/pvn_test_images/devops-supply-chain
- https://github.com/pvnovarese/devops-supply-chain-demo

Integration of cosign with syft: https://github.com/anchore/syft/issues/510
Add support for Hints in syft: https://github.com/anchore/syft/issues/31

Best Practices for Securing the Software Supply Chain

00 Centralized, secure CI/CD process for all software

01 Build images from trusted sources

02 Automate security testing and policy enforcement

03 Deploy only trusted images into production

anchore