anchore

Learn from Log4shell

Using SBOMs for Zero-Day Preparadness

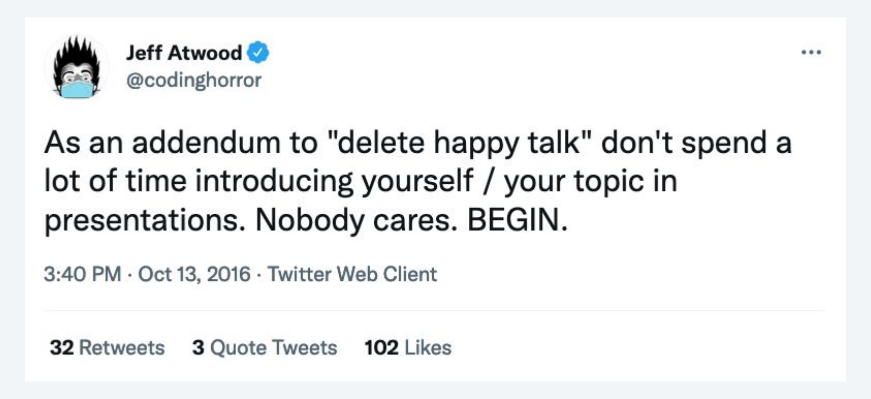
Hello World

Paul Novarese

Senior Solutions Architect

Anchore, Inc.

pvn@anchore.com - @pvn



Jeff Atwood
@codinghorror

As an addendum to "delete happy talk" don't spend a lot of time introducing yourself / your topic in presentations. Nobody cares. BEGIN.

3:40 PM · Oct 13, 2016 · Twitter Web Client

32 Retweets 3 Quote Tweets 102 Likes

anchore

Agenda

00 Supply Chain Attacks

01 Log4Shell - What Actually Happened

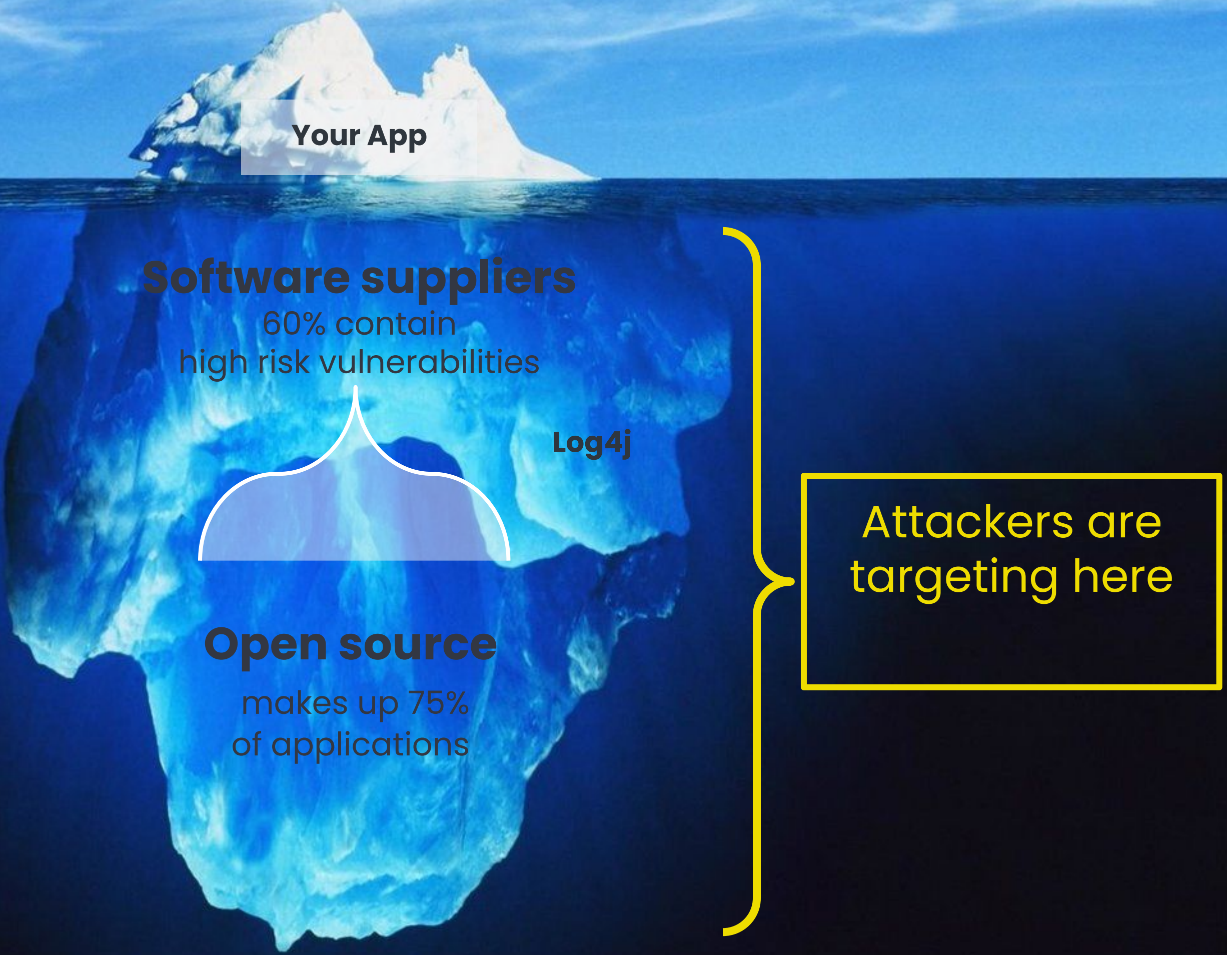
02 Software Bill of Materials

03 Now what?

anchore

What are Supply Chain Attacks?

Risk in the Software Supply Chain



Your App

Software suppliers

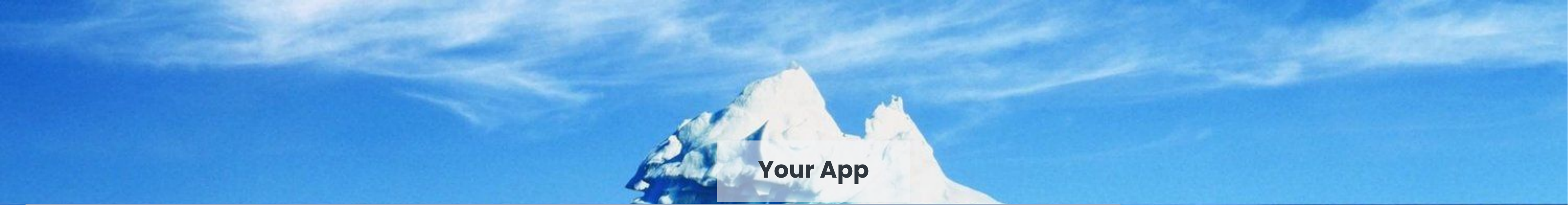
60% contain
high risk vulnerabilities

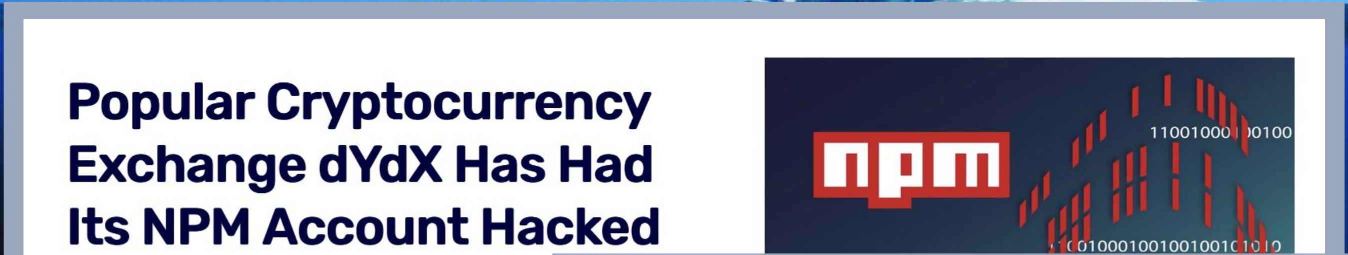
Log4j

Open source

makes up 75%
of applications

Attackers are
targeting here



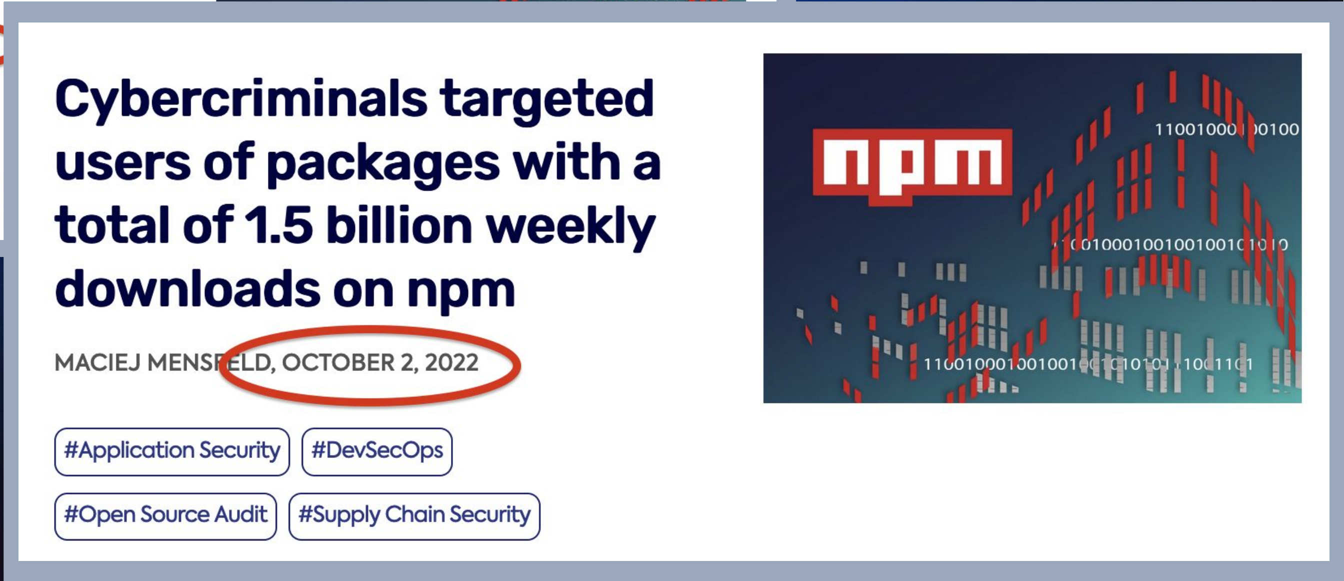


Popular Cryptocurrency Exchange dYdX Has Had Its NPM Account Hacked

MACIEJ MENSFELD, SEPTEMBER 23, 2022

#Application Security #DevSecOps

#Open Source Audit #Supply Chain Security



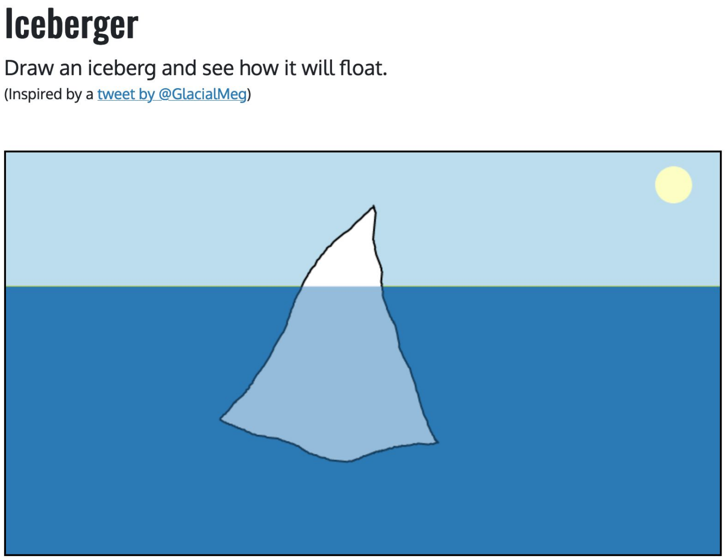
Cybercriminals targeted users of packages with a total of 1.5 billion weekly downloads on npm

MACIEJ MENSFELD, OCTOBER 2, 2022

#Application Security #DevSecOps

#Open Source Audit #Supply Chain Security

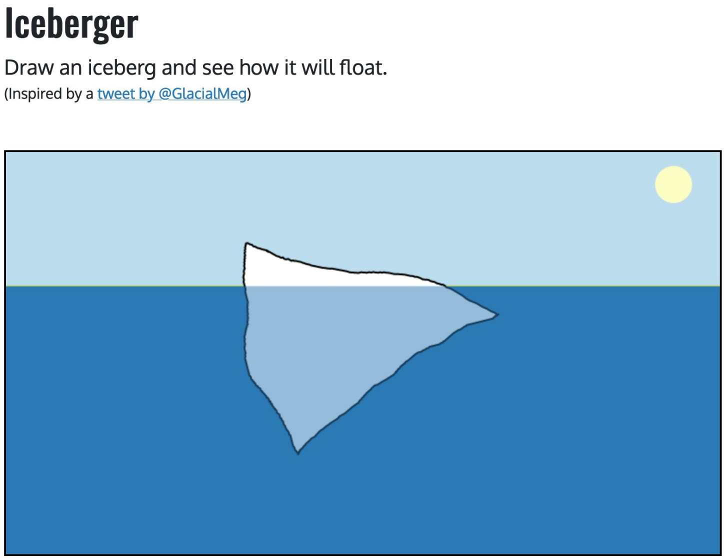
Quick Aside



Iceberger

Draw an iceberg and see how it will float.

(Inspired by a tweet by @GlacialMeg)

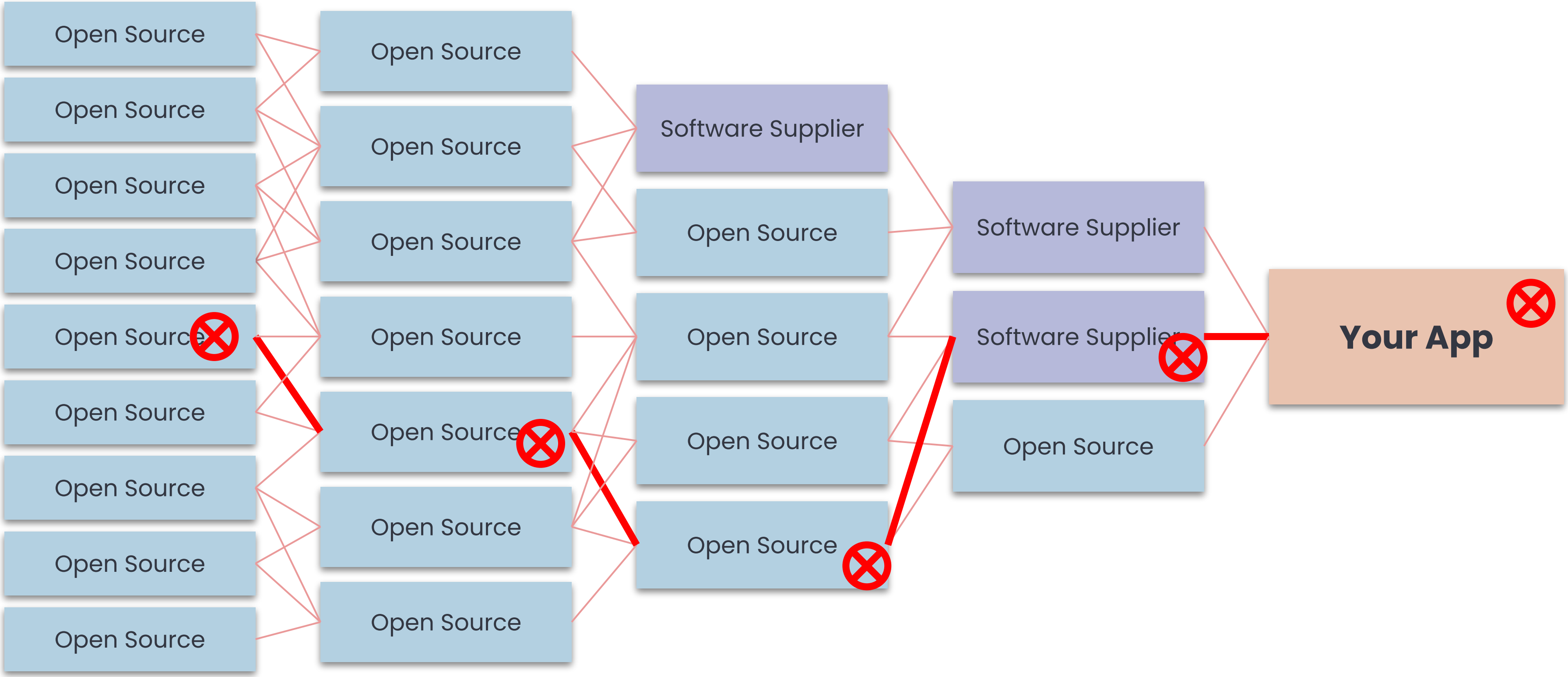


Iceberger

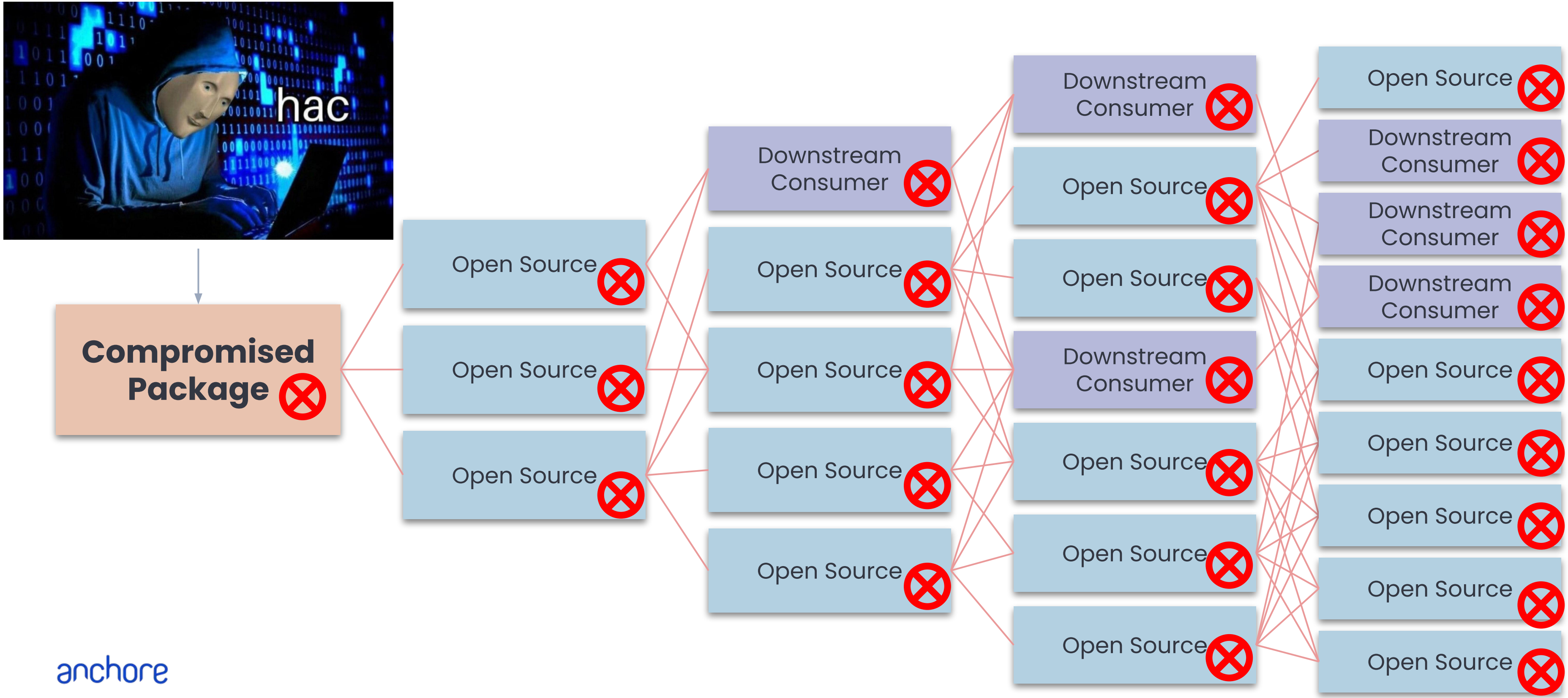
Draw an iceberg and see how it will float.

(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

Downstream Consumer

Open Source

Open Source

Open Source

Open Source

Downstream Consumer

Downstream Consumer

Downstream Consumer

Open Source

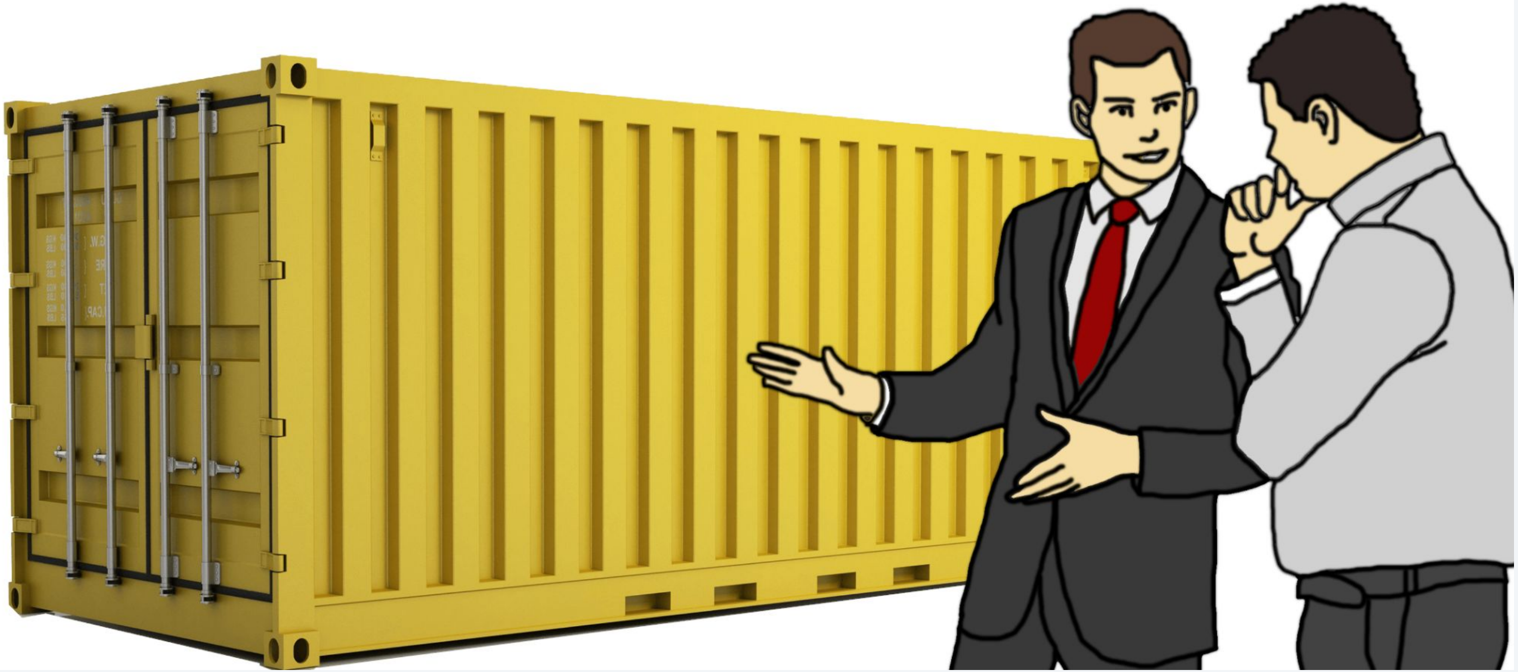
Open Source

Open Source

Open Source

Open Source

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



Log4Shell Impact

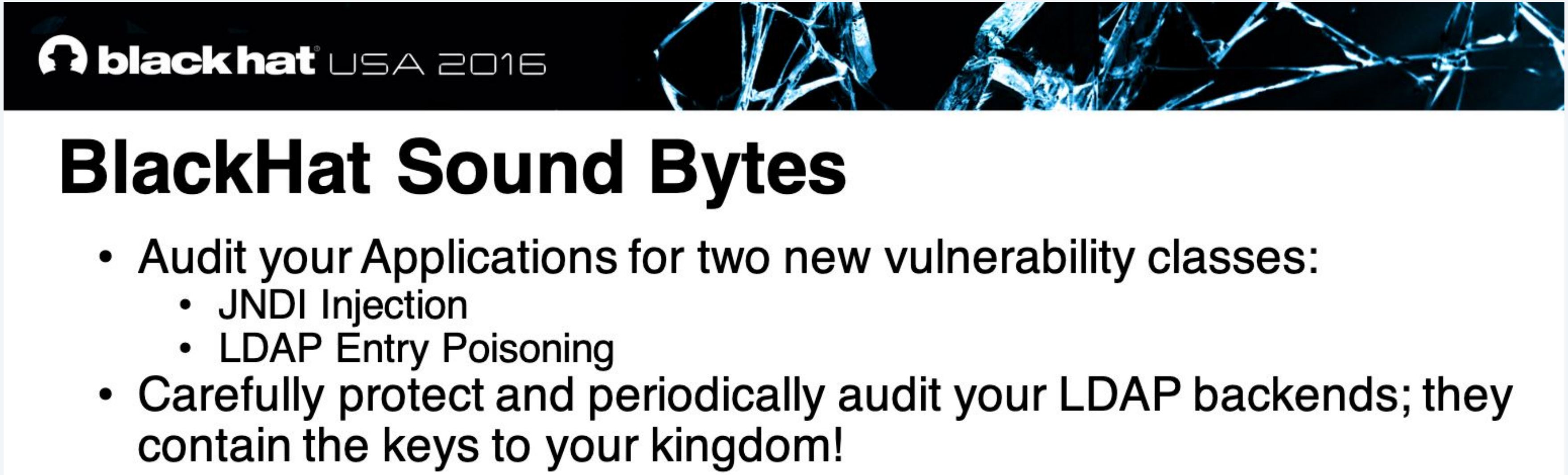
What is log4j? What is log4shell?

What is log4j? What is log4shell?

log4j Timeline

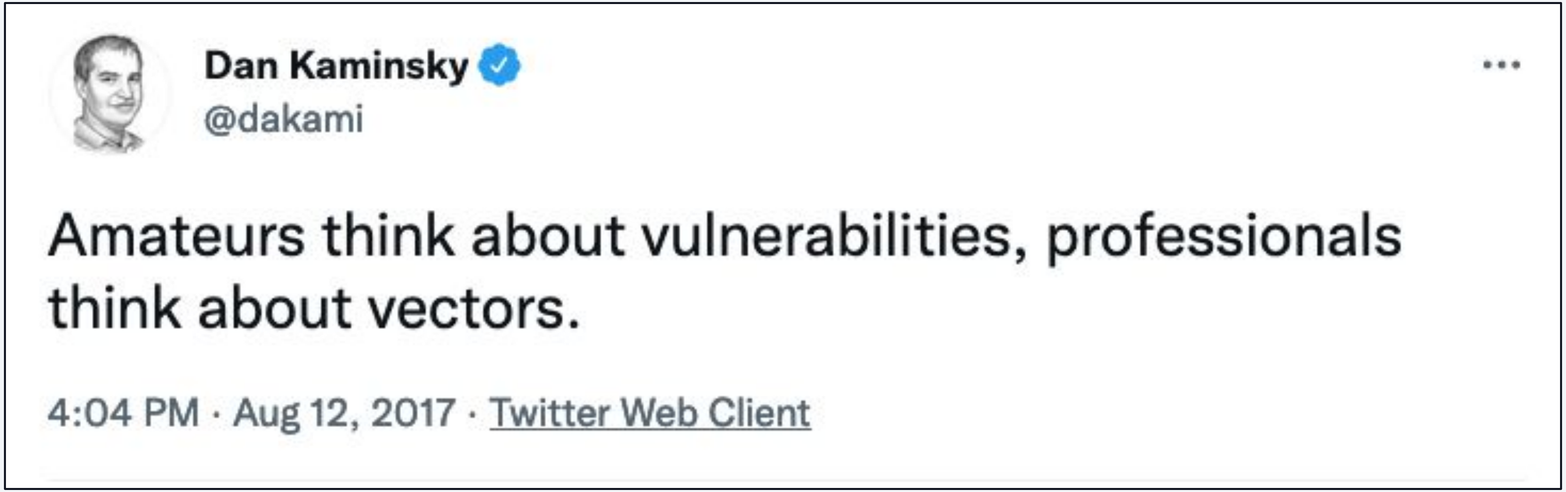
- 2001 - Initial release
- 14 Sep 2013 - Vulnerability is introduced 2.0-beta9
- 3 Aug 2016 - Potential exploit presented at Black Hat

2016-08-03


blackhat USA 2016

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!



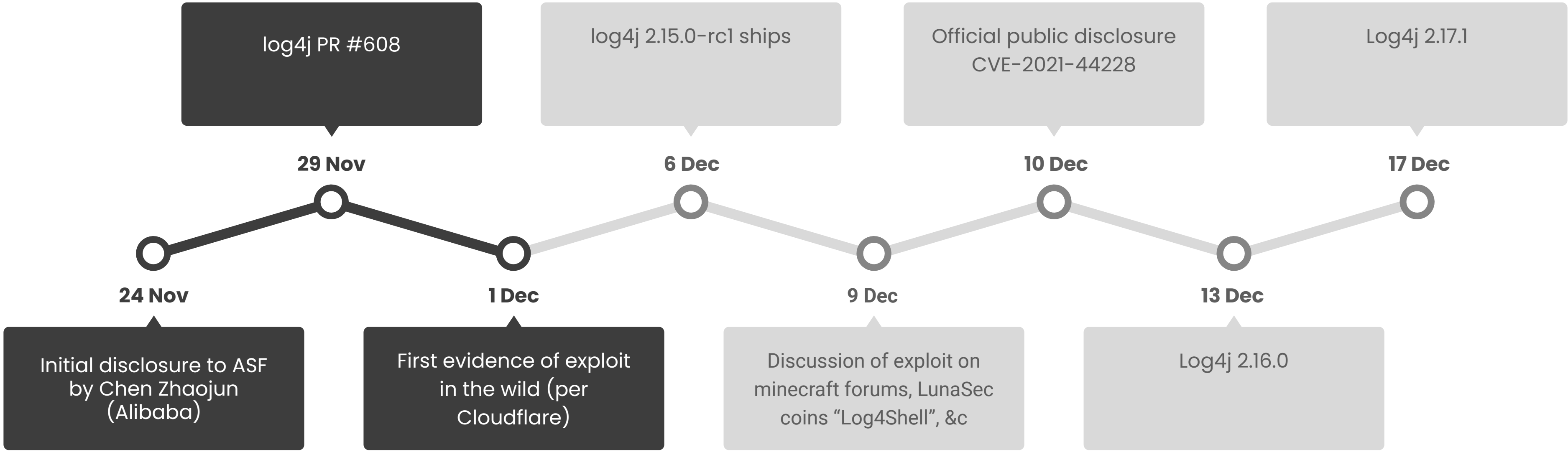
Dan Kaminsky

@dakami

Amateurs think about vulnerabilities, professionals think about vectors.

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

log4shell Timeline



24 Nov

Initial disclosure to ASF by Chen Zhaojun (Alibaba)

29 Nov

log4j PR #608

1 Dec

First evidence of exploit in the wild (per Cloudflare)

6 Dec

log4j 2.15.0-rc1 ships

9 Dec

Discussion of exploit on minecraft forums, LunaSec coins “Log4Shell”, &c

10 Dec

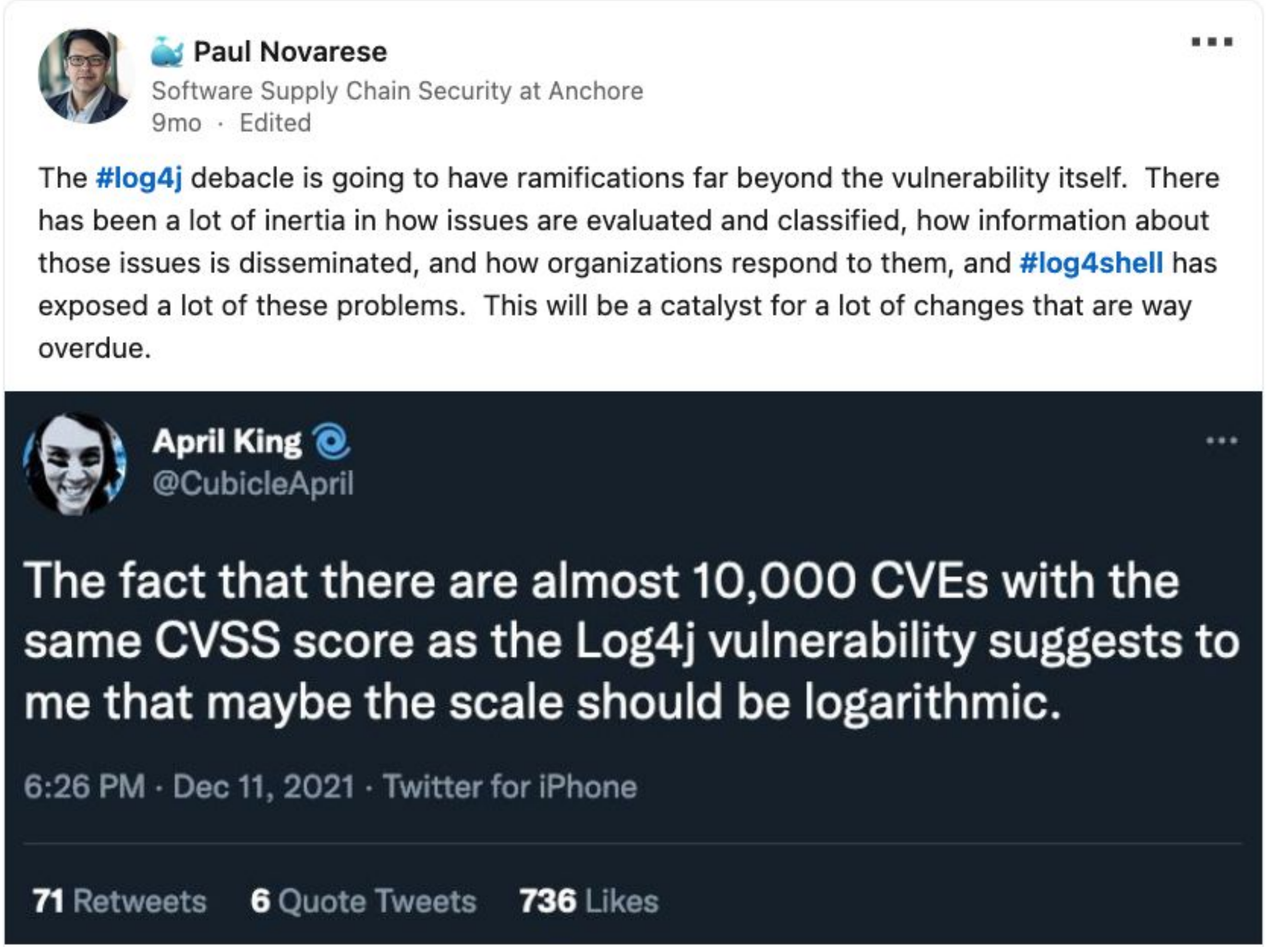
Official public disclosure CVE-2021-44228

13 Dec

Log4j 2.16.0

17 Dec

Log4j 2.17.1



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.

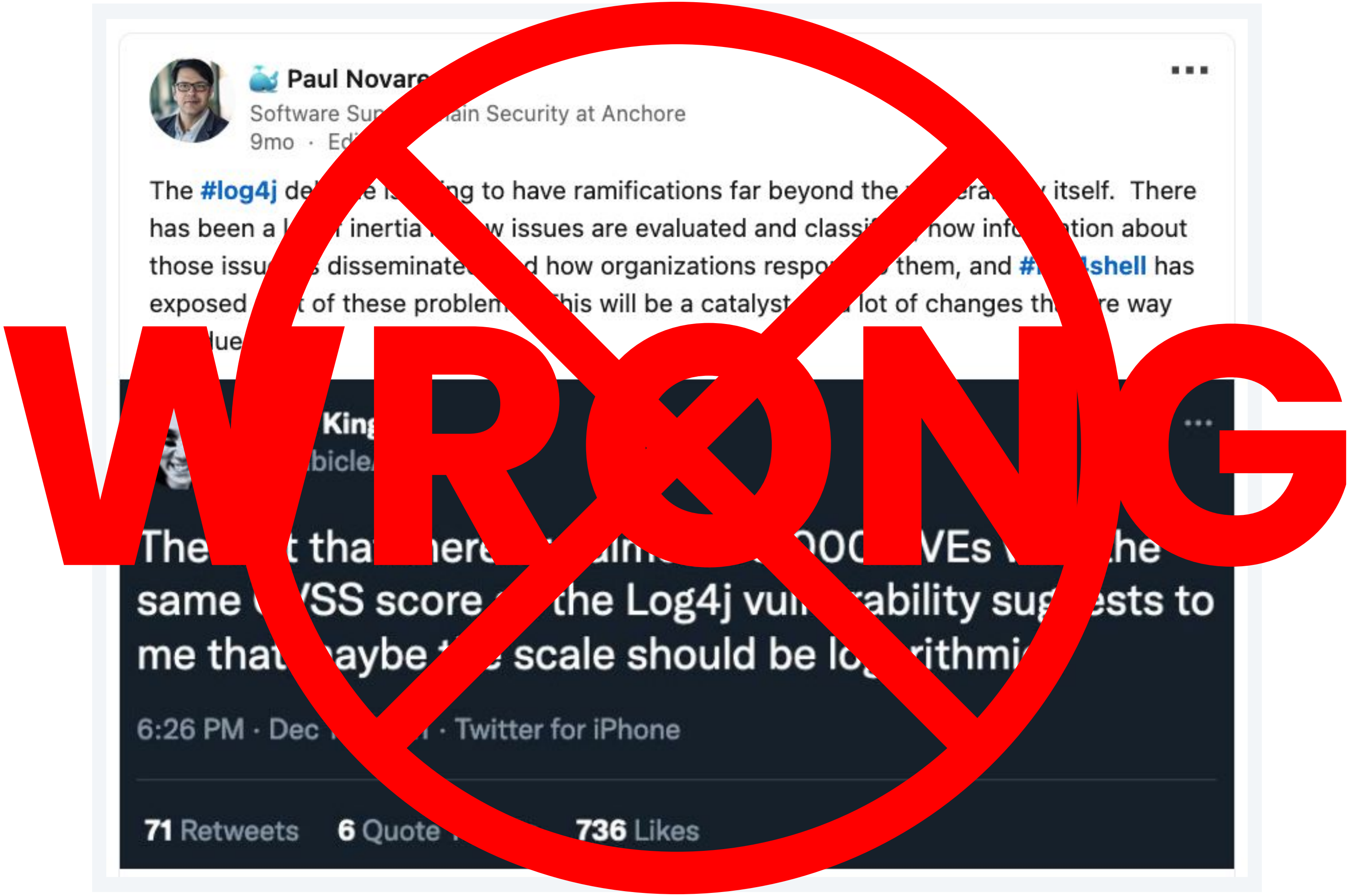
April King

@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 · Edi

The #log4j de e i ng to have ramifications far beyond the era itself. There has been a l r inertia i w issues are evaluated and classi how inf tion about those issu s disseminate d how organizations respo them, and #4shell has exposed t of these problem his will be a catalyst lot of changes th re way lue

King

bicle

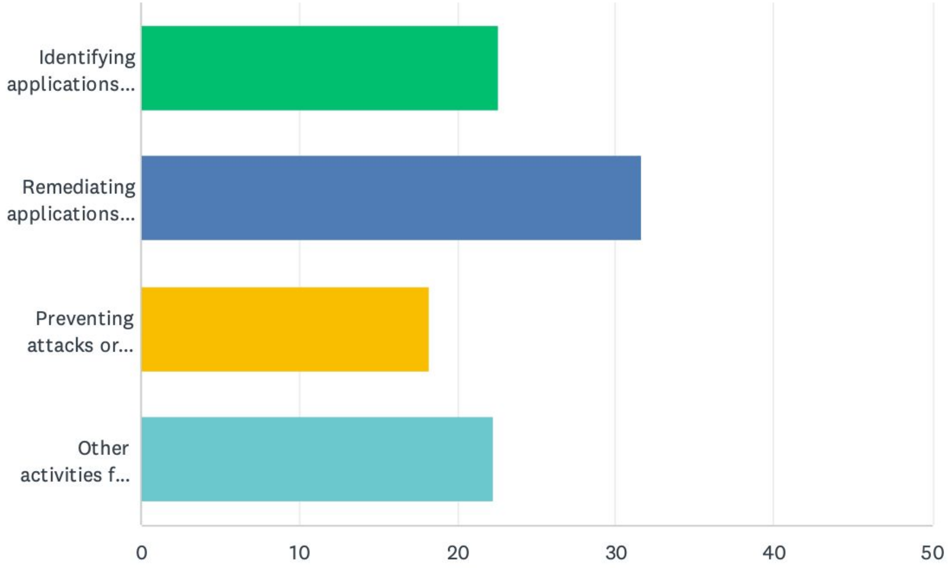
The t tha here 000 VEs he same VSS score the Log4j vul ability sug ests to me tha aybe scale should be lo rithmi

6:26 PM · Dec · Twitter for iPhone

71 Retweets 6 Quote 736 Likes

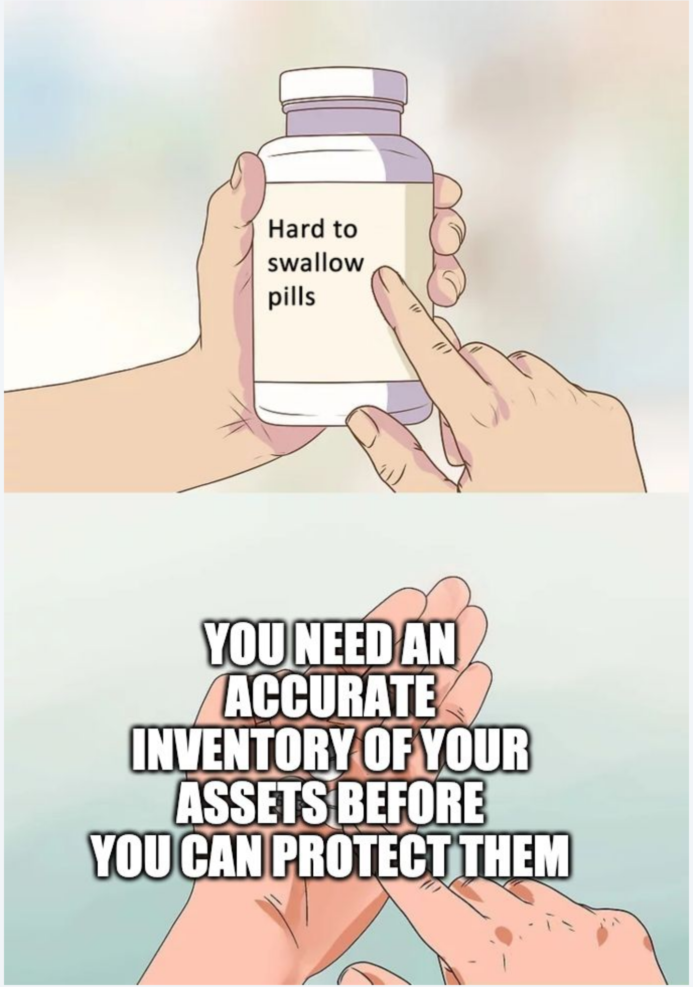
Q12 Estimate how many hours you personally have spent to date on each of the following activities.

Answered: 195 Skipped: 15

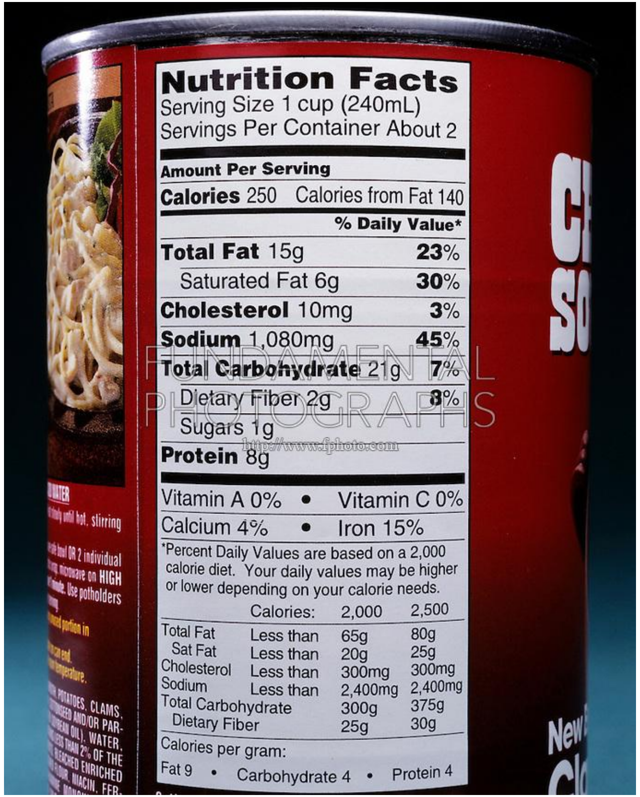


anchore

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?



Nutrition Facts

Serving Size 1 cup (240mL)
Servings Per Container About 2

Amount Per Serving

Calories 250 Calories from Fat 140

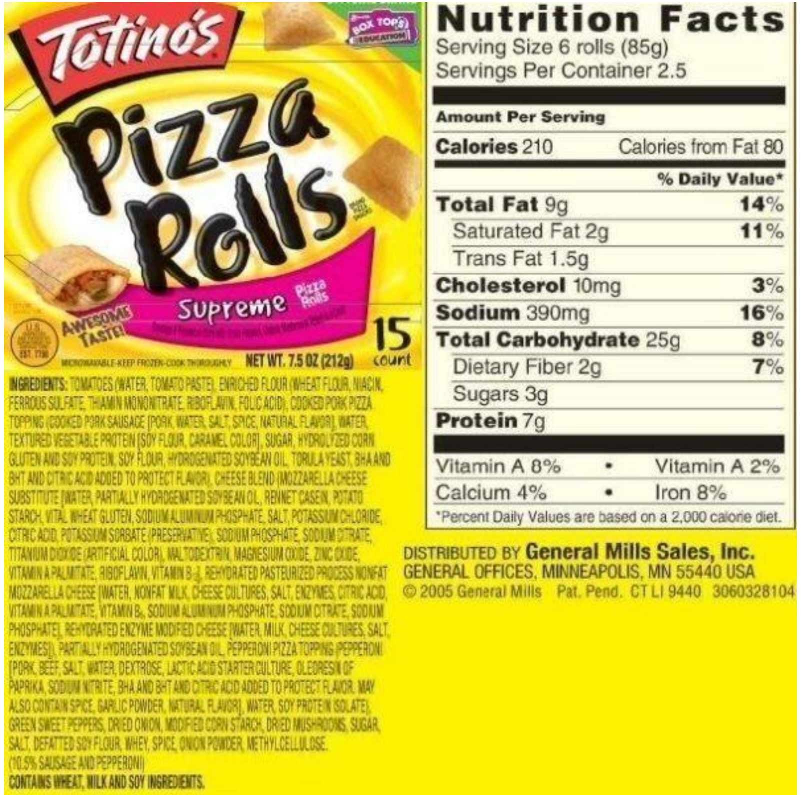
	% Daily Value*
Total Fat 15g	**23%**
Saturated Fat 6g	**30%**
Cholesterol 10mg	**3%**
Sodium 1,080mg	**45%**
Total Carbohydrate 21g	**7%**
Dietary Fiber 2g	**8%**
Sugars 1g	
Protein 8g	

Vitamin A 0% • Vitamin C 0%
Calcium 4% • Iron 15%

*Percent Daily Values are based on a 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs.

	Calories:	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g

Calories per gram:
Fat 9 • Carbohydrate 4 • Protein 4



MICROWAVABLE-KEEP FROZEN-COOK THOROUGHLY NET WT. 7.5 OZ (212g)

INGREDIENTS: TOMATOES (WATER, TOMATO PASTE), ENRICHED FLOUR (WHEAT FLOUR, NIACIN, FERROUS SULFATE, THIAMIN MONONITRATE, RIBOFLAVIN, FOLIC ACID), COOKED PORK PIZZA TOPPING (COOKED PORK SAUSAGE [PORK, WATER, SALT, SPICE, NATURAL FLAVOR], WATER, TEXTURED VEGETABLE PROTEIN [SOY FLOUR, CARAMEL COLOR], SUGAR, HYDROLYZED CORN GLUTEN AND SOY PROTEIN, SOY FLOUR, HYDROGENATED SOYBEAN OIL, TORULA YEAST, BHA AND BHT AND CITRIC ACID ADDED TO PROTECT FLAVOR), CHEESE BLEND (MOZZARELLA CHEESE SUBSTITUTE [WATER, PARTIALLY HYDROGENATED SOYBEAN OIL, RENNET CASEIN, POTATO STARCH, VITAL WHEAT GLUTEN, SODIUM ALUMINUM PHOSPHATE, SALT, POTASSIUM CHLORIDE, CITRIC ACID, POTASSIUM SORBATE (PRESERVATIVE), SODIUM PHOSPHATE, SODIUM CITRATE, TITANIUM DIOXIDE (ARTIFICIAL COLOR), MALTODEXTRIN, MAGNESIUM OXIDE, ZINC OXIDE, VITAMIN A PALMITATE, RIBOFLAVIN, VITAMIN B-12], REHYDRATED PASTEURIZED PROCESS NONFAT MOZZARELLA CHEESE [WATER, NONFAT MILK, CHEESE CULTURES, SALT, ENZYMES, CITRIC ACID, VITAMIN A PALMITATE, VITAMIN B12, SODIUM ALUMINUM PHOSPHATE, SODIUM CITRATE, SODIUM PHOSPHATE], REHYDRATED ENZYME MODIFIED CHEESE [WATER, MILK, CHEESE CULTURES, SALT, ENZYMES]), PARTIALLY HYDROGENATED SOYBEAN OIL, PEPPERONI PIZZA TOPPING (PEPPERONI [PORK, BEEF, SALT, WATER, DEXTROSE, LACTIC ACID STARTER CULTURE, OLEORESIN OF PAPRIKA, SODIUM NITRITE, BHA AND BHT AND CITRIC ACID ADDED TO PROTECT FLAVOR. MAY ALSO CONTAIN SPICE, GARLIC POWDER, NATURAL FLAVOR], WATER, SOY PROTEIN ISOLATE), GREEN SWEET PEPPERS, DRIED ONION, MODIFIED CORN STARCH, DRIED MUSHROOMS, SUGAR, SALT, DEFATTED SOY FLOUR, WHEY, SPICE, ONION POWDER, METHYLCELLULOSE. (10.5% SAUSAGE AND PEPPERONI)

CONTAINS WHEAT, MILK AND SOY INGREDIENTS.

Nutrition Facts

Serving Size 6 rolls (85g)
Servings Per Container 2.5

Amount Per Serving

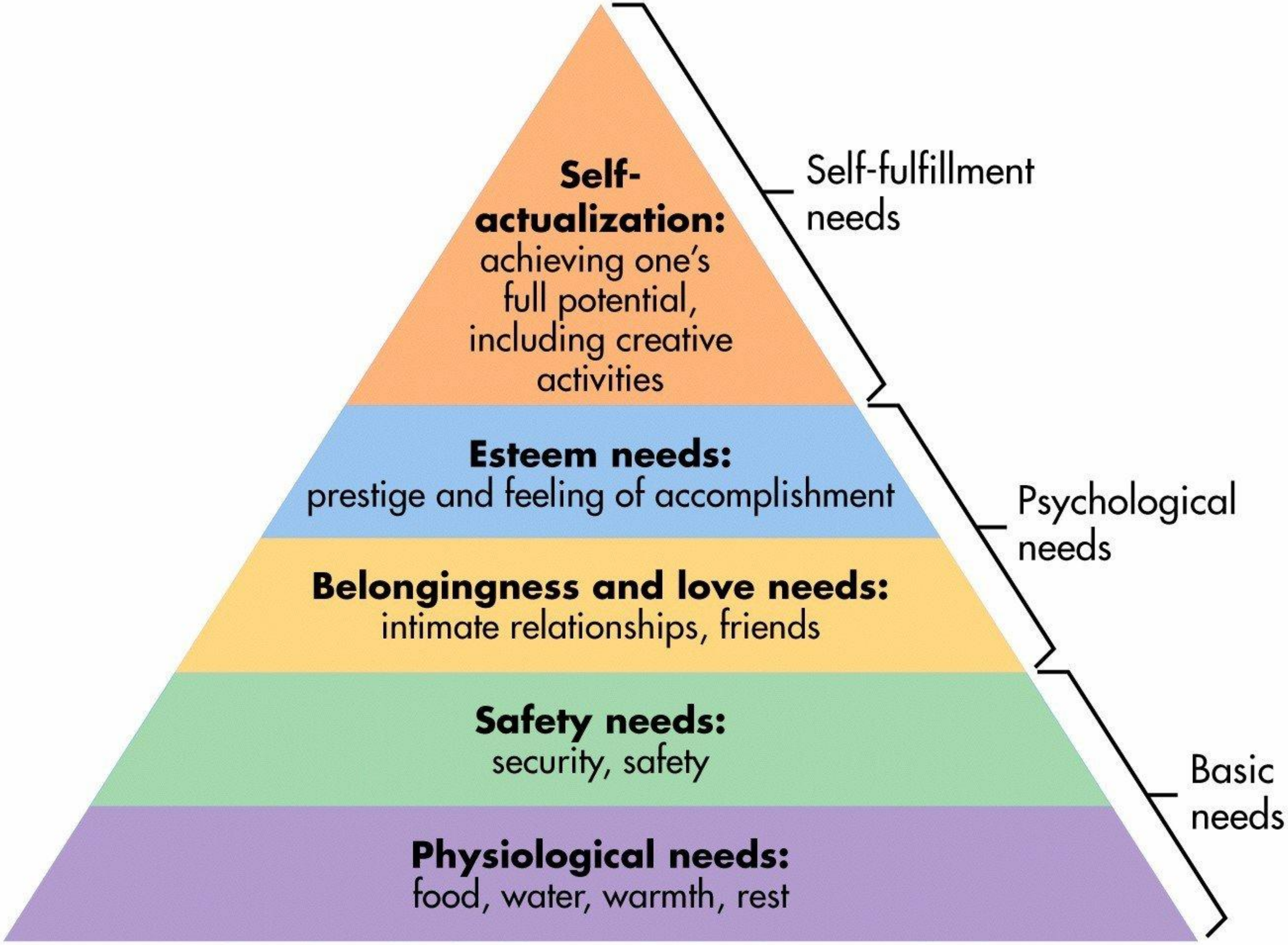
Calories 210 Calories from Fat 80

	% Daily Value*
Total Fat 9g	**14%**
Saturated Fat 2g	**11%**
Trans Fat 1.5g	
Cholesterol 10mg	**3%**
Sodium 390mg	**16%**
Total Carbohydrate 25g	**8%**
Dietary Fiber 2g	**7%**
Sugars 3g	
Protein 7g	

Vitamin A 8% • Vitamin A 2%
Calcium 4% • Iron 8%

*Percent Daily Values are based on a 2,000 calorie diet.

DISTRIBUTED BY **General Mills Sales, Inc.**
GENERAL OFFICES, MINNEAPOLIS, MN 55440 USA
© 2005 General Mills Pat. Pend. CT LI 9440 3060328104



Self-actualization: achieving one's full potential, including creative activities

Esteem needs: prestige and feeling of accomplishment

Belongingness and love needs: intimate relationships, friends

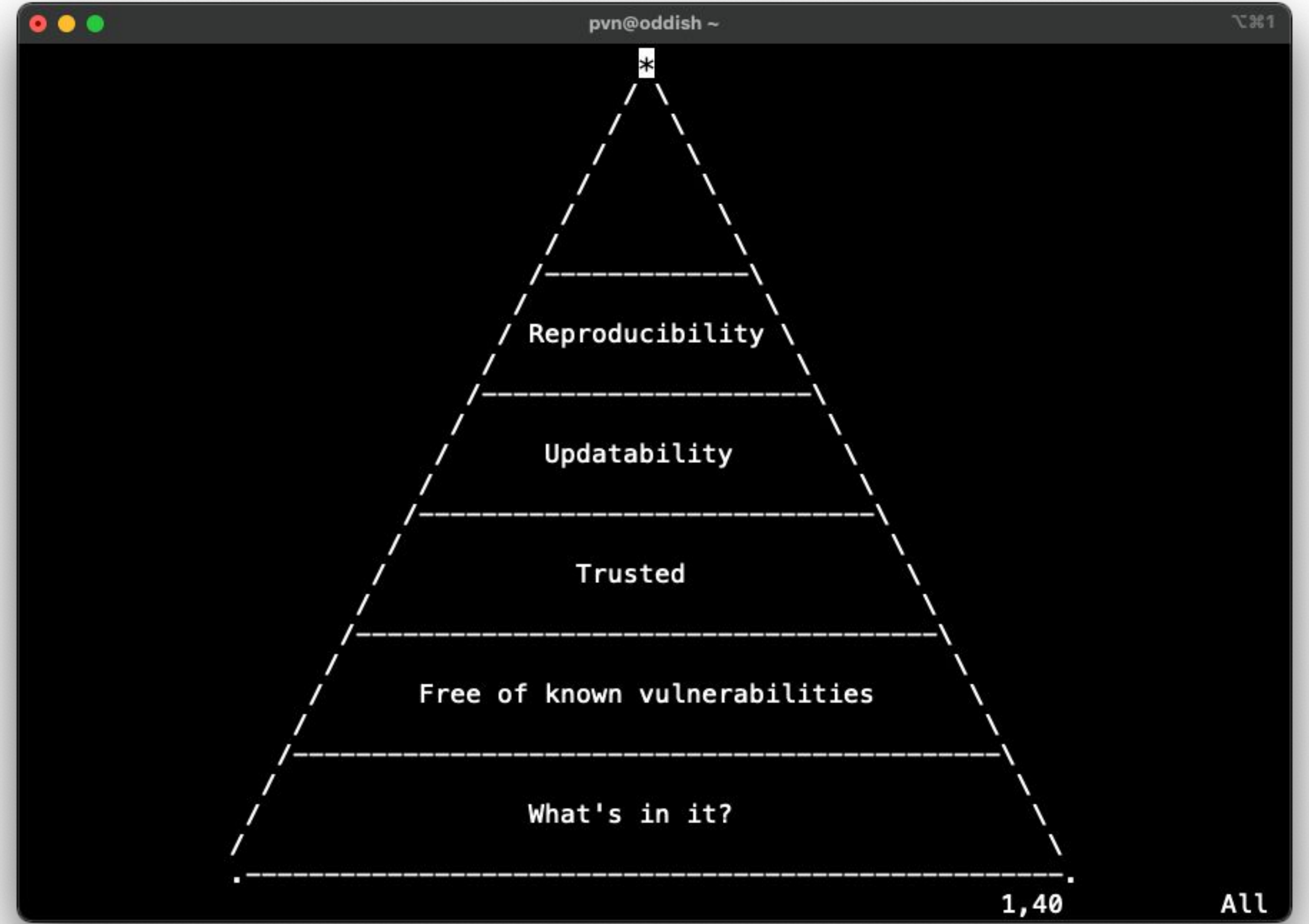
Safety needs: security, safety

Physiological needs: food, water, warmth, rest

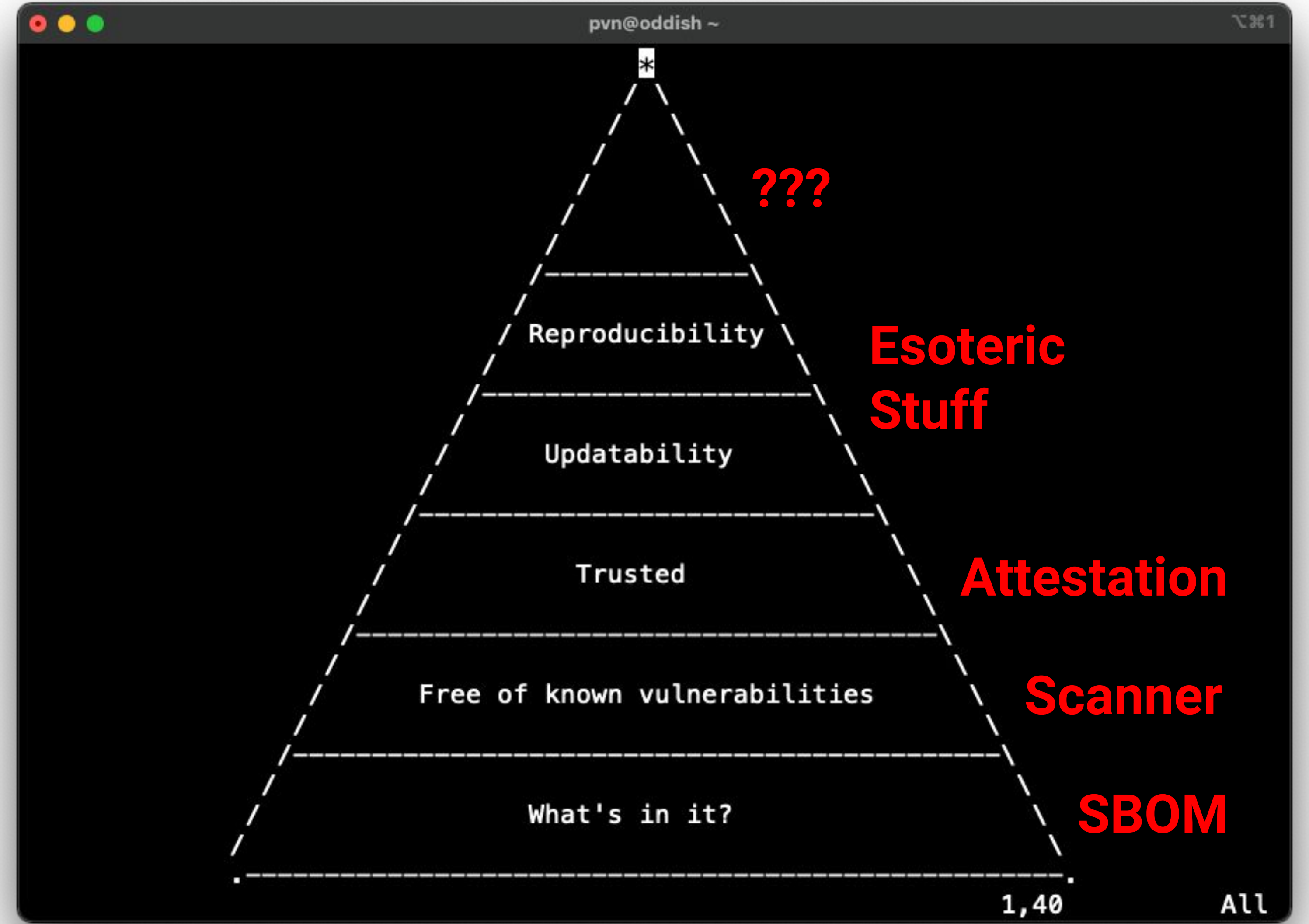
Self-fulfillment needs

Psychological needs

Basic needs



```
                           *
                          / \
                         /   \
                        /     \
                       /       \
                      /         \
                     /           \
                    /-------------\
                   /               \
                  / Reproducibility \
                 /                   \
                /---------------------\
               /                       \
              /      Updatability       \
             /                           \
            /-----------------------------\
           /                               \
          /            Trusted              \
         /                                   \
        /-------------------------------------\
       /                                       \
      /      Free of known vulnerabilities      \
     /                                           \
    /---------------------------------------------\
   /                                               \
  /                 What's in it?                   \
 /                                                   \
.-----------------------------------------------------.
                                                  1,40          All
```



```
                          *
                         / \
                        /   \
                       /     \
                      /       \
                     /         \
                    /           \
                   /-------------\
                  /               \
                 / Reproducibility \
                /                   \
               /---------------------\
              /                       \
             /      Updatability       \
            /                           \
           /-----------------------------\
          /                               \
         /            Trusted              \
        /                                   \
       /-------------------------------------\
      /                                       \
     /      Free of known vulnerabilities      \
    /                                           \
   /---------------------------------------------\
  /                                               \
 /                 What's in it?                   \
/                                                   \
.----------------------------------------------------.
                                                 1,40          All
```

???

Esoteric Stuff

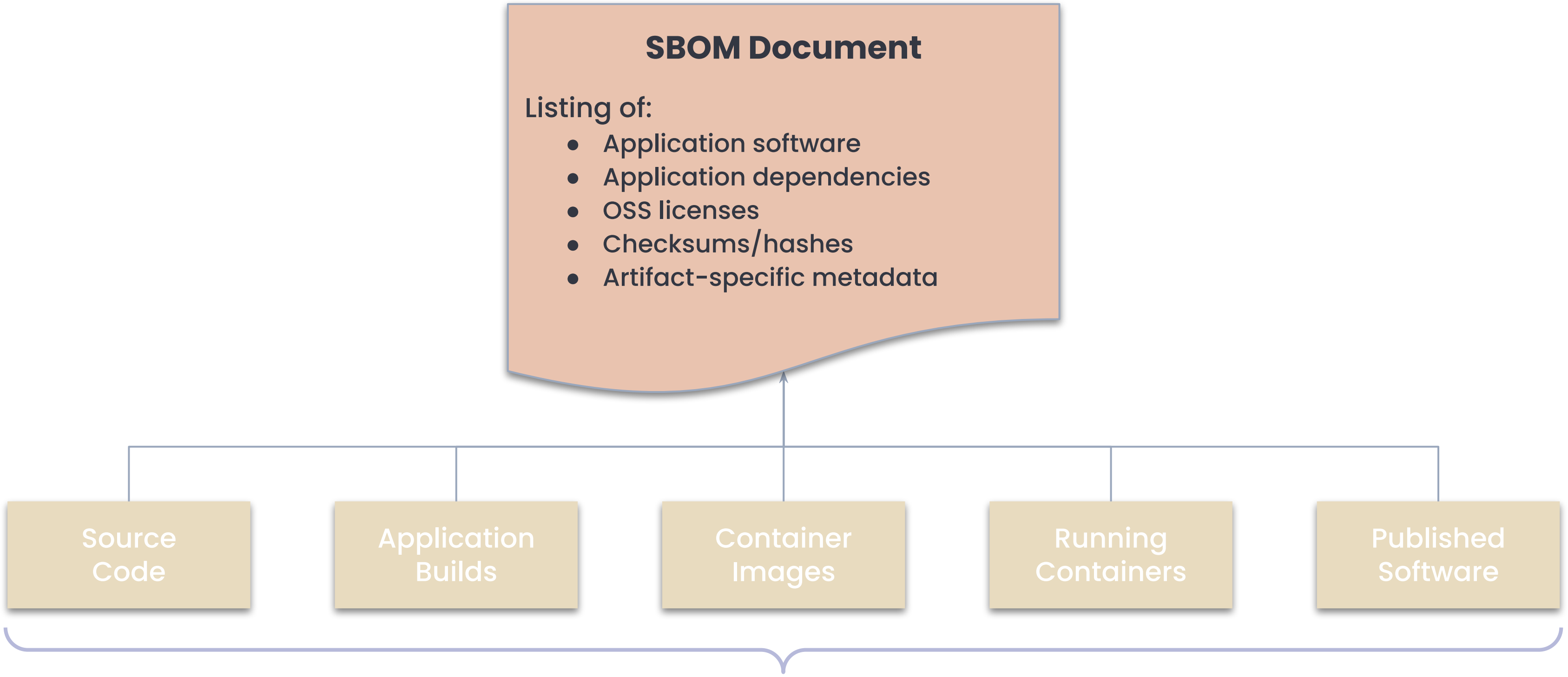
Attestation

Scanner

SBOM

Addressing the Problem

What is an SBOM?



SBOM Document

Listing of:

- Application software
- Application dependencies
- OSS licenses
- Checksums/hashes
- Artifact-specific metadata

Source Code

Application Builds

Container Images

Running Containers

Published Software

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

anchore

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

For example a running system, a machine image, a container image, etc.

Each item uniquely

Such as each component name, version, UUID, and relationships to other components.

What did the cataloguing

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.

Introducing Syft

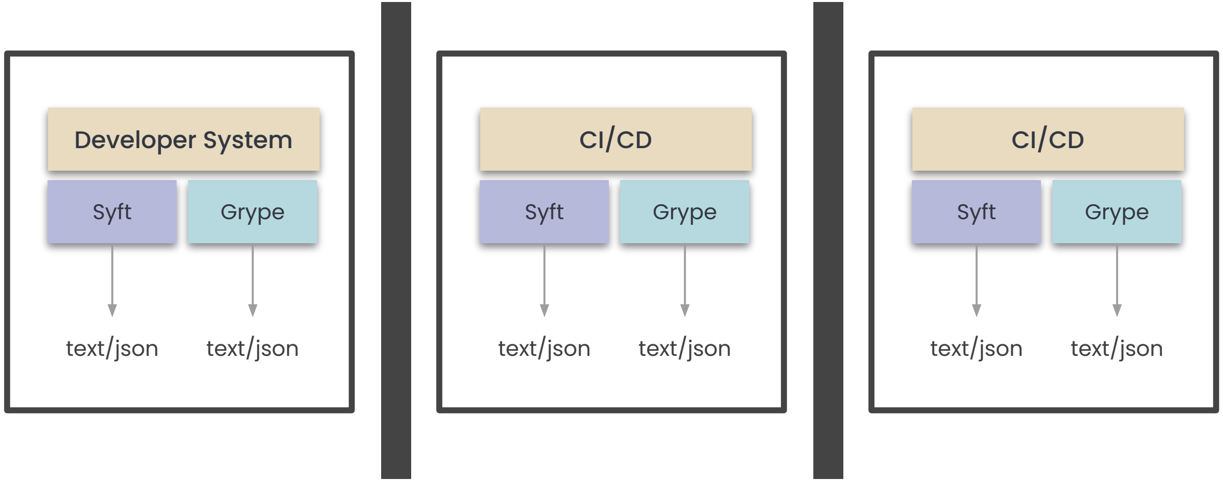
- Syft is an **open source tool that generates SBOMs** from container images and filesystems

- 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

Now What?

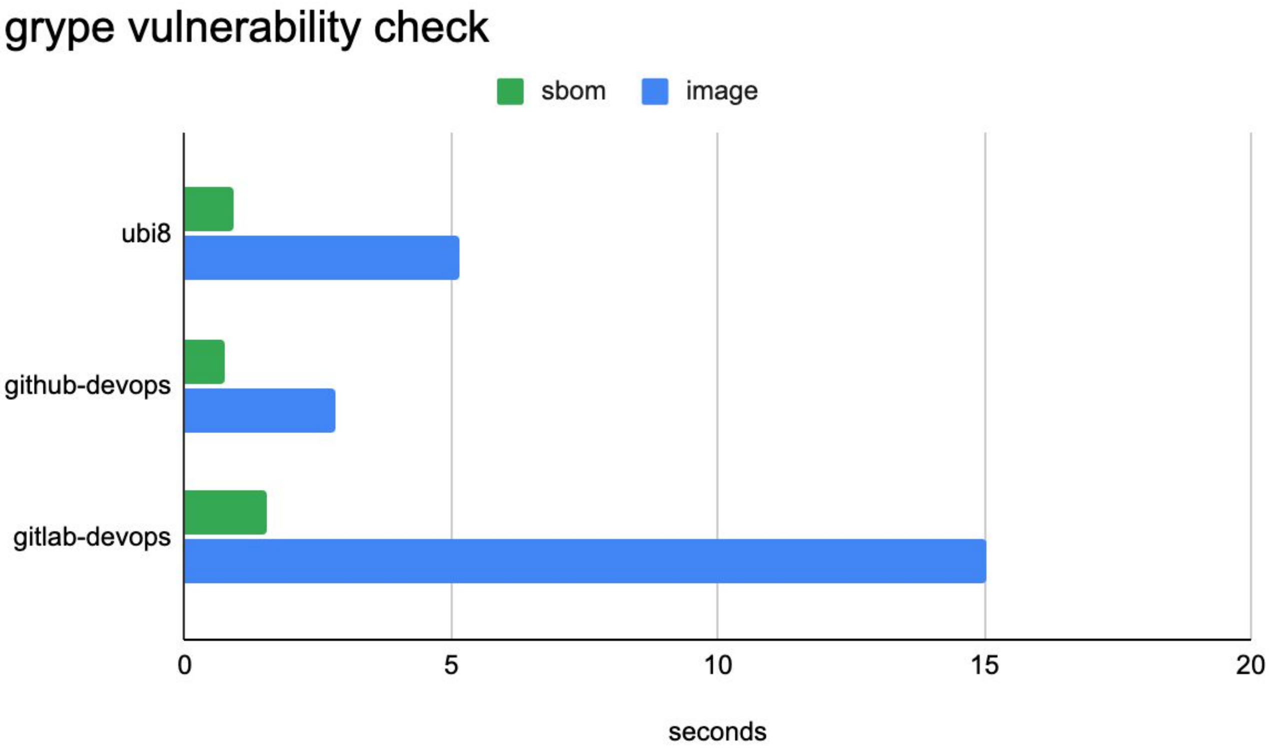
How will this improve my life?

How Do SBOMs Actually Help?

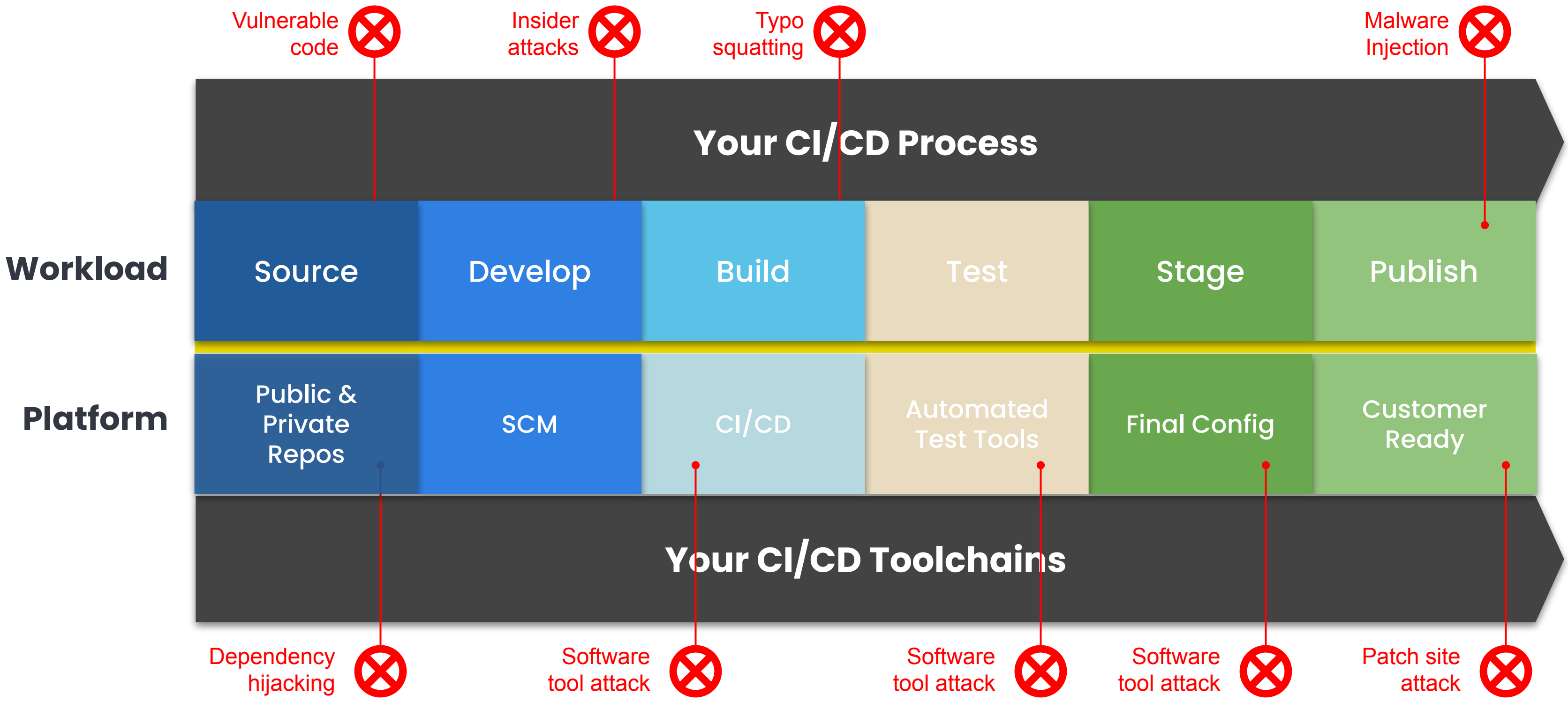
anchore

Grype Scan Timing

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

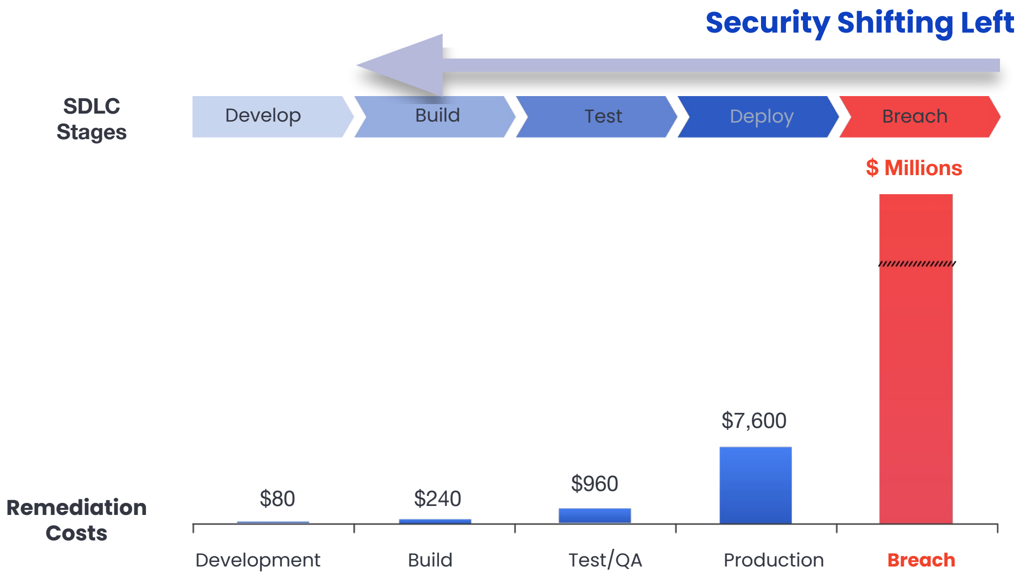


SBOMs Enable Continuous Evaluation

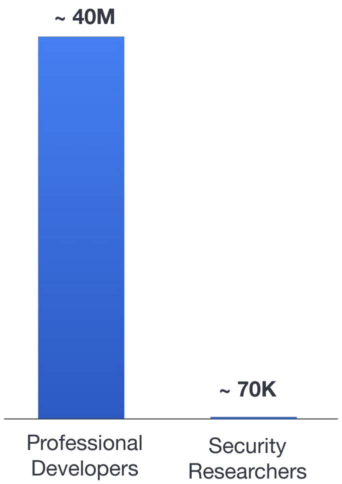


anchore

Shift Security Left

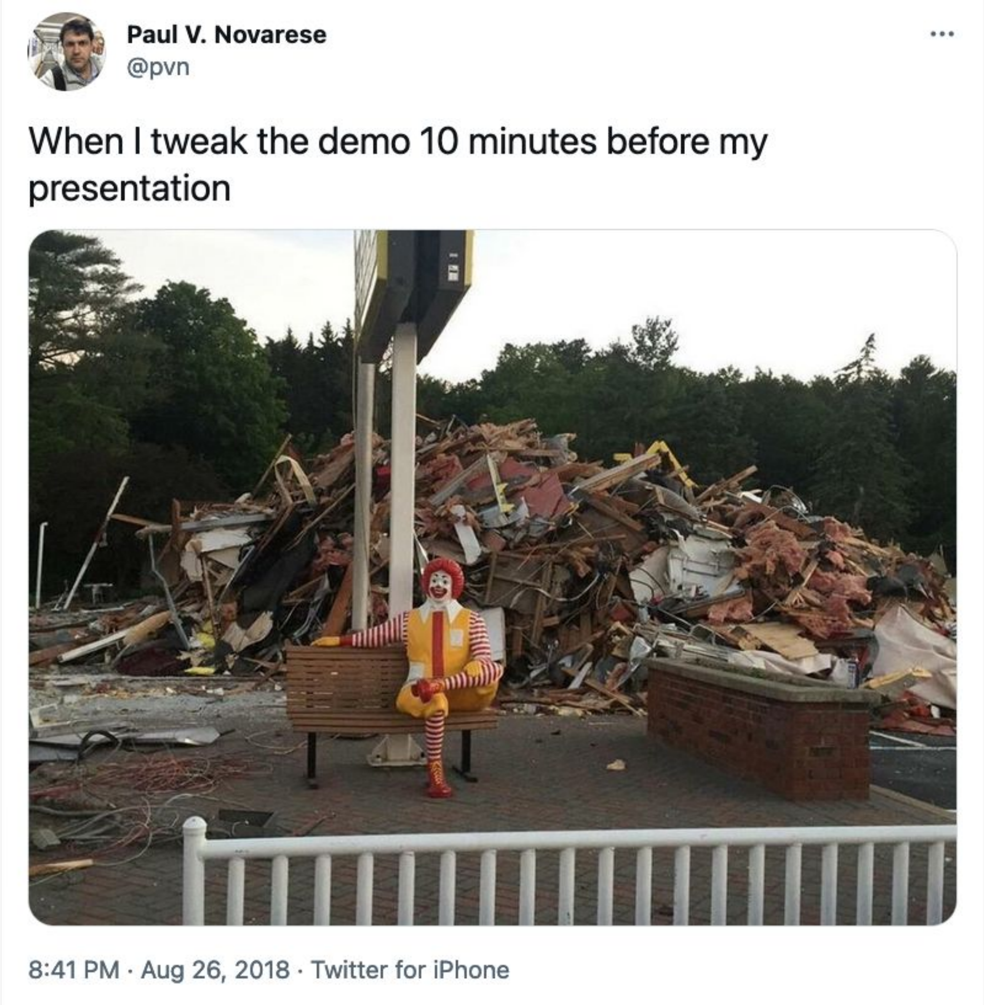


Vastly more cost effective to remediate during development



570x more developers than security researchers

anchore

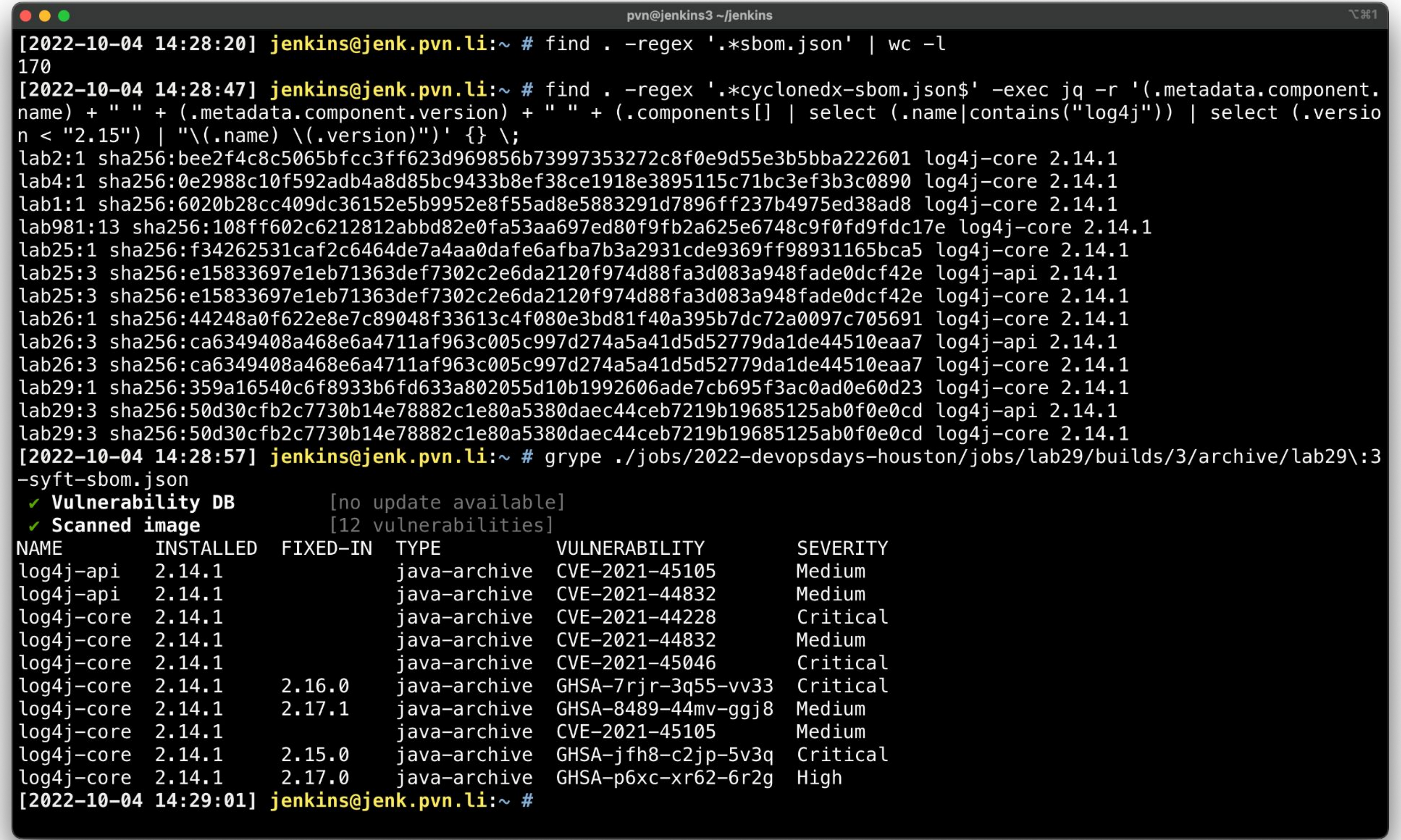


Paul V. Novarese

@pvn

When I tweak the demo 10 minutes before my presentation

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



```
[2022-10-04 14:28:20] jenkins@jenk.pvn.li:~ # find . -regex '.*sbom.json' | wc -l
170
[2022-10-04 14:28:47] jenkins@jenk.pvn.li:~ # find . -regex '.*cyclonedx-sbom.json$' -exec jq -r '(.metadata.component.
name) + " " + (.metadata.component.version) + " " + (.components[] | select (.name|contains("log4j")) | select (.versio
n < "2.15") | "\(.name) \(.version)")' {} \;
lab2:1 sha256:bee2f4c8c5065bfcc3ff623d969856b73997353272c8f0e9d55e3b5bba222601 log4j-core 2.14.1
lab4:1 sha256:0e2988c10f592adb4a8d85bc9433b8ef38ce1918e3895115c71bc3ef3b3c0890 log4j-core 2.14.1
lab1:1 sha256:6020b28cc409dc36152e5b9952e8f55ad8e5883291d7896ff237b4975ed38ad8 log4j-core 2.14.1
lab981:13 sha256:108ff602c6212812abbd82e0fa53aa697ed80f9fb2a625e6748c9f0fd9fdc17e log4j-core 2.14.1
lab25:1 sha256:f34262531caf2c6464de7a4aa0dafe6afba7b3a2931cde9369ff98931165bca5 log4j-core 2.14.1
lab25:3 sha256:e15833697e1eb71363def7302c2e6da2120f974d88fa3d083a948fade0dcf42e log4j-api 2.14.1
lab25:3 sha256:e15833697e1eb71363def7302c2e6da2120f974d88fa3d083a948fade0dcf42e log4j-core 2.14.1
lab26:1 sha256:44248a0f622e8e7c89048f33613c4f080e3bd81f40a395b7dc72a0097c705691 log4j-core 2.14.1
lab26:3 sha256:ca6349408a468e6a4711af963c005c997d274a5a41d5d52779da1de44510eaa7 log4j-api 2.14.1
lab26:3 sha256:ca6349408a468e6a4711af963c005c997d274a5a41d5d52779da1de44510eaa7 log4j-core 2.14.1
lab29:1 sha256:359a16540c6f8933b6fd633a802055d10b1992606ade7cb695f3ac0ad0e60d23 log4j-core 2.14.1
lab29:3 sha256:50d30cfb2c7730b14e78882c1e80a5380daec44ceb7219b19685125ab0f0e0cd log4j-api 2.14.1
lab29:3 sha256:50d30cfb2c7730b14e78882c1e80a5380daec44ceb7219b19685125ab0f0e0cd log4j-core 2.14.1
[2022-10-04 14:28:57] jenkins@jenk.pvn.li:~ # grype ./jobs/2022-devopsdays-houston/jobs/lab29/builds/3/archive/lab29\:3
-syft-sbom.json
 ✔ Vulnerability DB        [no update available]
 ✔ Scanned image           [12 vulnerabilities]
NAME        INSTALLED  FIXED-IN  TYPE           VULNERABILITY        SEVERITY
log4j-api   2.14.1               java-archive   CVE-2021-45105       Medium
log4j-api   2.14.1               java-archive   CVE-2021-44832       Medium
log4j-core  2.14.1               java-archive   CVE-2021-44228       Critical
log4j-core  2.14.1               java-archive   CVE-2021-44832       Medium
log4j-core  2.14.1               java-archive   CVE-2021-45046       Critical
log4j-core  2.14.1     2.16.0    java-archive   GHSA-7rjr-3q55-vv33  Critical
log4j-core  2.14.1     2.17.1    java-archive   GHSA-8489-44mv-ggj8  Medium
log4j-core  2.14.1               java-archive   CVE-2021-45105       Medium
log4j-core  2.14.1     2.15.0    java-archive   GHSA-jfh8-c2jp-5v3q  Critical
log4j-core  2.14.1     2.17.0    java-archive   GHSA-p6xc-xr62-6r2g  High
[2022-10-04 14:29:01] jenkins@jenk.pvn.li:~ #
```

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

One Last Bad Analogy

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

Q&A

Download Syft

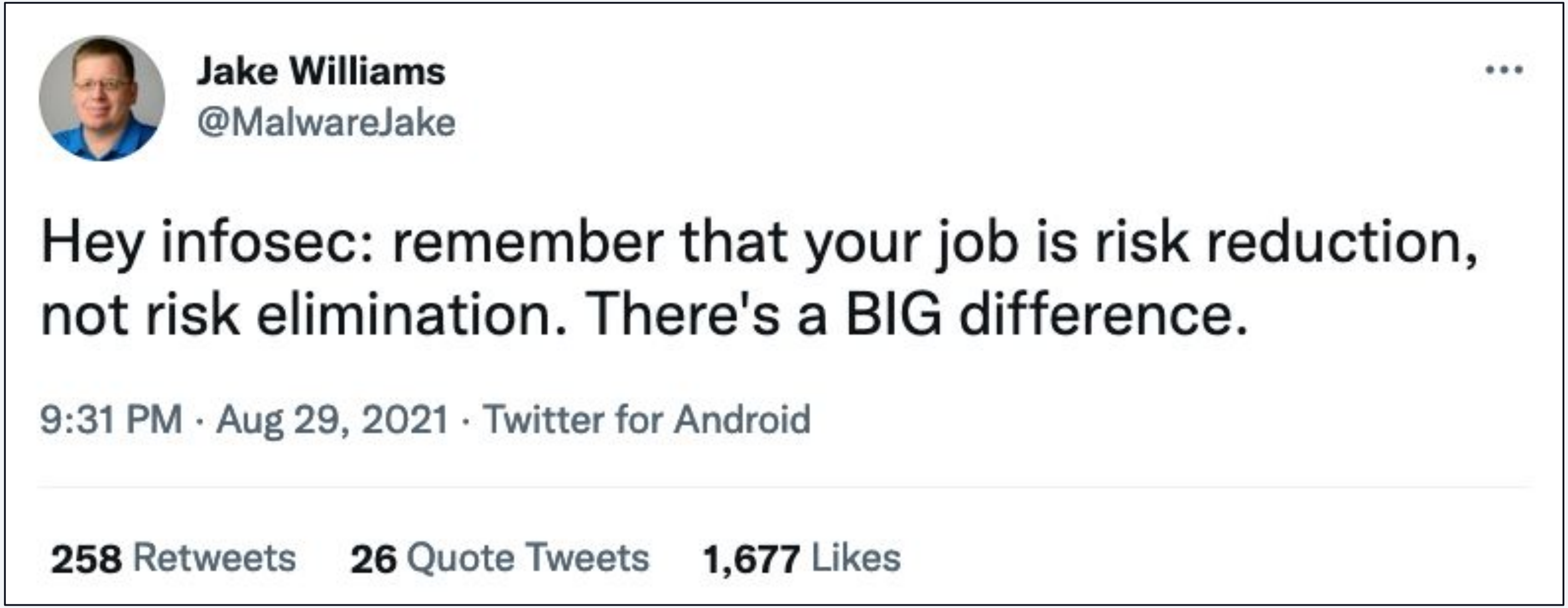
https://github.com/anchore/syft

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

Draft of upcoming site content for SBOM.me: https://github.com/joshbressers/sbom-examples/blob/readme-update/site/index.md

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 6: https://www.mend.io/resources/blog/popular-cryptocurrency-exchange-dydx-has-had-its-npm-account-hacked/
Slide 6: https://www.mend.io/resources/blog/cybercriminals-targeted-users-of-packages-with-a-total-of-1-5-billion-weekly-downloads-on-npm/
Slide 7: https://joshdata.me/iceberger.html
Slide 16: https://twitter.com/dakami/status/896477575475642368
Slides 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
Slides 18-19: https://twitter.com/CubicleApril/status/1469825942684160004
Slides 18-19: https://www.linkedin.com/posts/novarese_log4j-log4shell-activity-6876206319238463488-8bEA
Slides 24-26: Maslow's Hierarchy of Supply Chain Needs: https://www.youtube.com/watch?v=rcP8QHFMwCw
Slide 27: 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