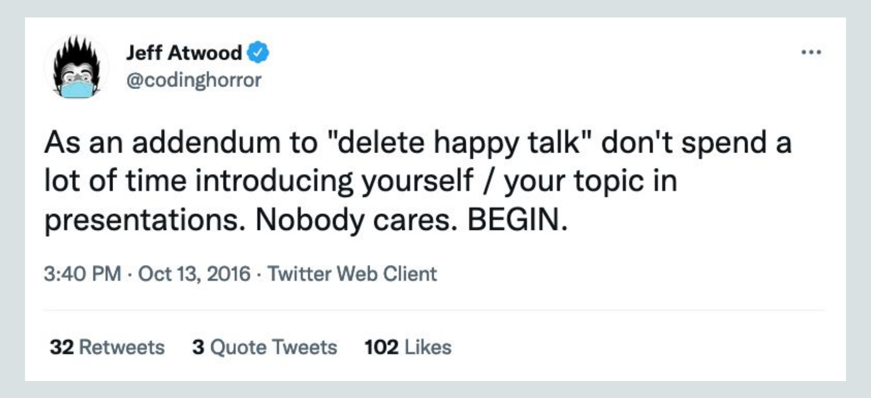
anchore

Secure Your Supply Chain: Adding a Software Bill of Materials to Your Containers to Improve Vulnerability Scanning

Presenter

Paul Novarese
Senior Solutions Architect
Anchore
pvn@anchore.com



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

Agenda

00 Types of attacks and why software supply chain attacks are different

01 Why container visibility is important

02 What an SBOM is and what it does

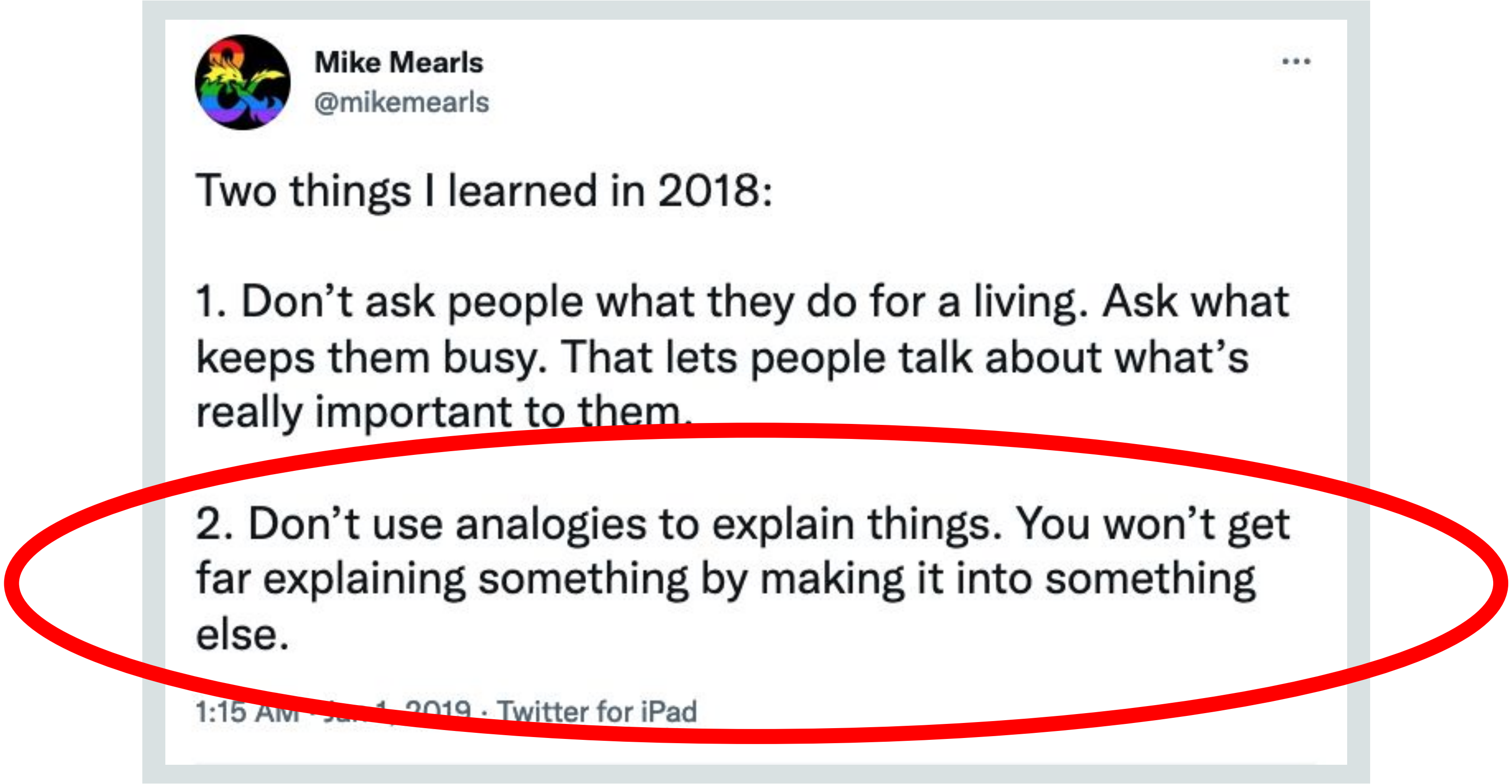
03 How to further secure your containers

Attack Types

Everything old is new again.

anchore

Story Time



Mike Mearls
@mikemearls

Two things I learned in 2018:

1. Don’t ask people what they do for a living. Ask what keeps them busy. That lets people talk about what’s really important to them.

2. Don’t use analogies to explain things. You won’t get far explaining something by making it into something else.

1:15 AM · Jan 1, 2019 · Twitter for iPad

Story Time

City of Toronto Archives, Fonds 1266, Item 5859

COLOUR CANADIAN COLOUR

Douglas Haig

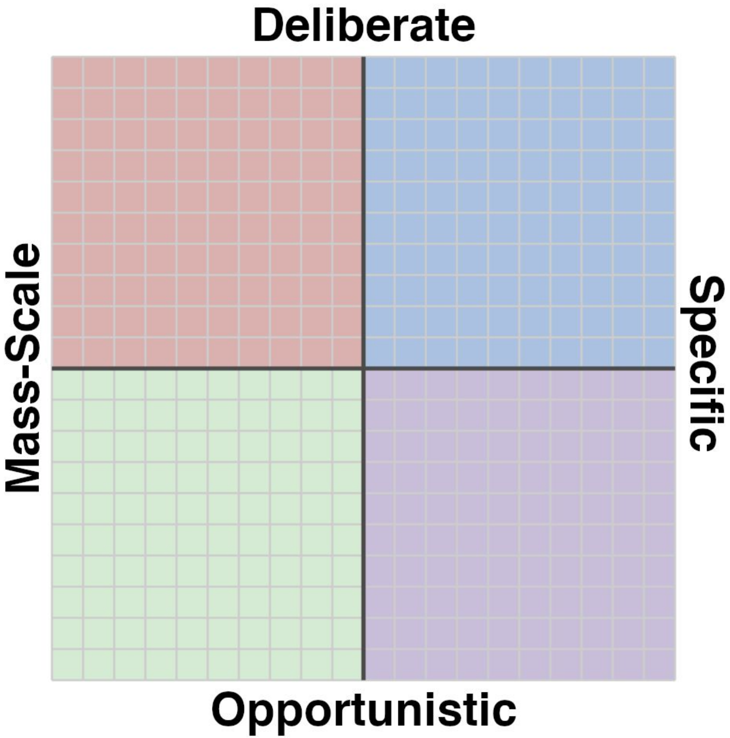
“Bullets have little stopping power against the horse” (1914)

WESTERN FRONT, 1915

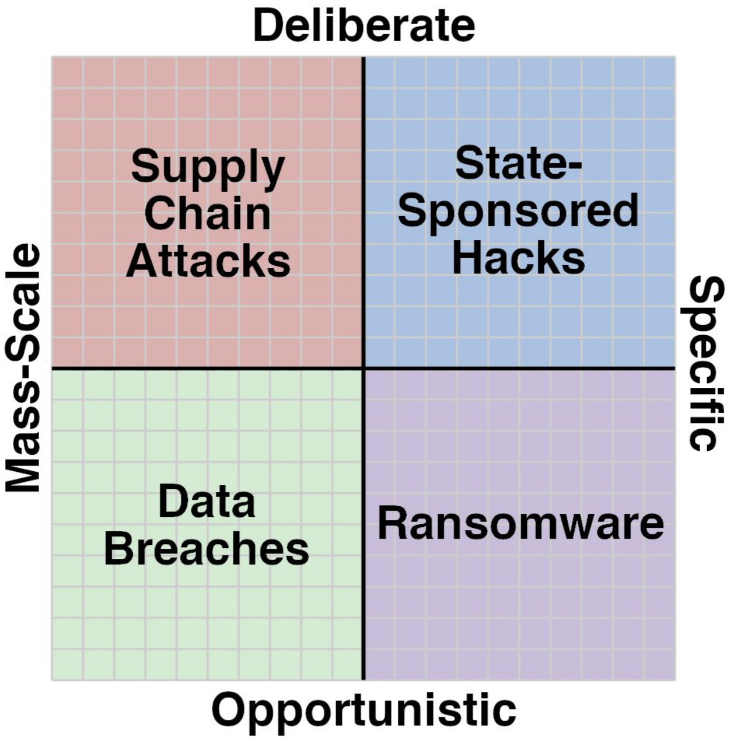
NOOOOOOO!!!! YOU CAN'T DEPLOY MILES AND MILES OF BARBED WIRE AND USE EXTREMELY ACCURATE, HIGH-POWERED AUTOMATIC RIFLES!!! I HAVE INVESTED A TON OF TIME AND EFFORT INTO TRAINING THESE CAVALRINOS!!!

haha machnine gun go brrrrr

Types of Attacks



Types of Attacks



Deliberate

Supply Chain Attacks

State-Sponsored Hacks

Mass-Scale

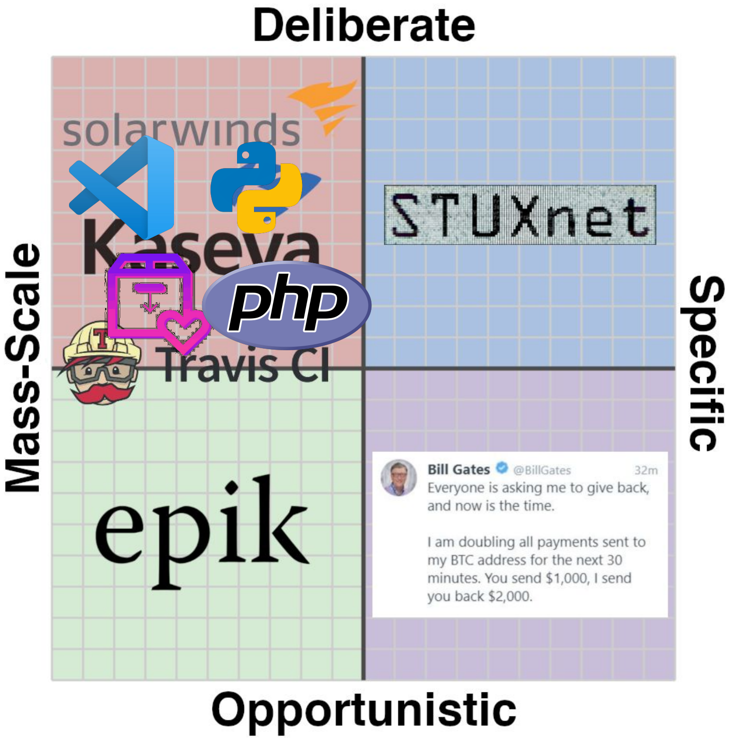
Specific

Data Breaches

Ransomware

Opportunistic

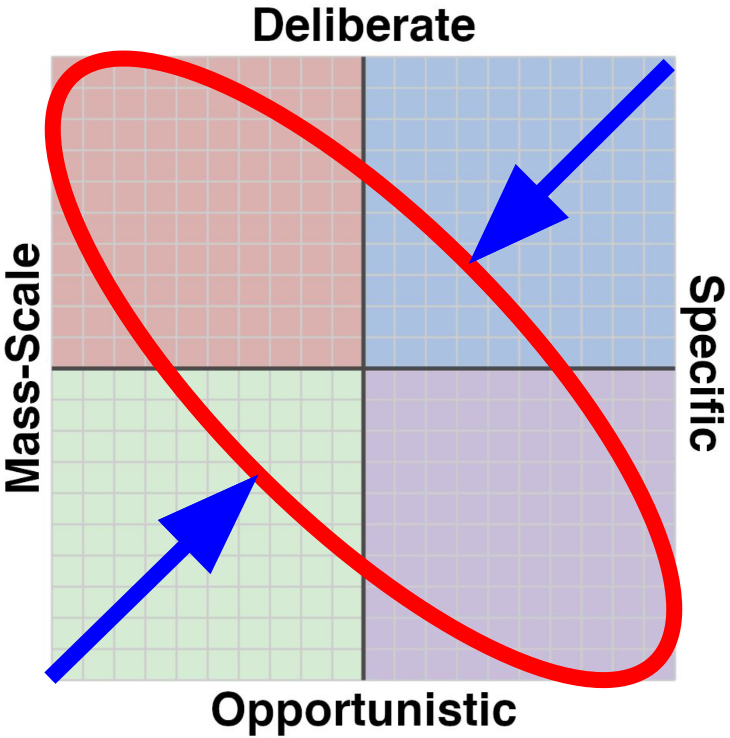
Types of Attacks: Examples



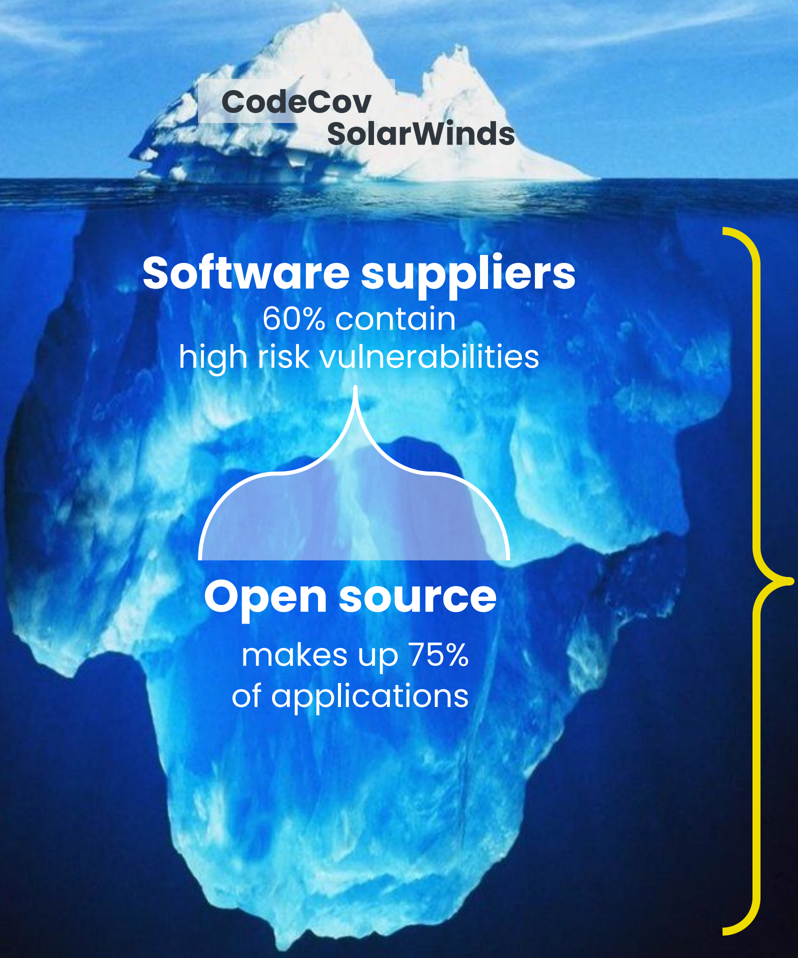
Bill Gates @BillGates 32m
Everyone is asking me to give back, and now is the time.

I am doubling all payments sent to my BTC address for the next 30 minutes. You send $1,000, I send you back $2,000.

“It Won’t Happen to Me”



Risk in the Software Supply Chain



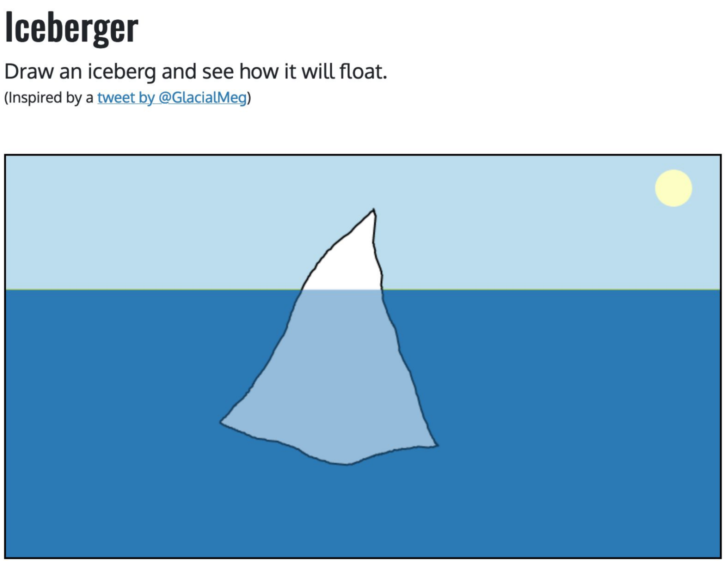
CodeCov
SolarWinds

Software suppliers
60% contain
high risk vulnerabilities

Open source
makes up 75%
of applications

Attackers are targeting here

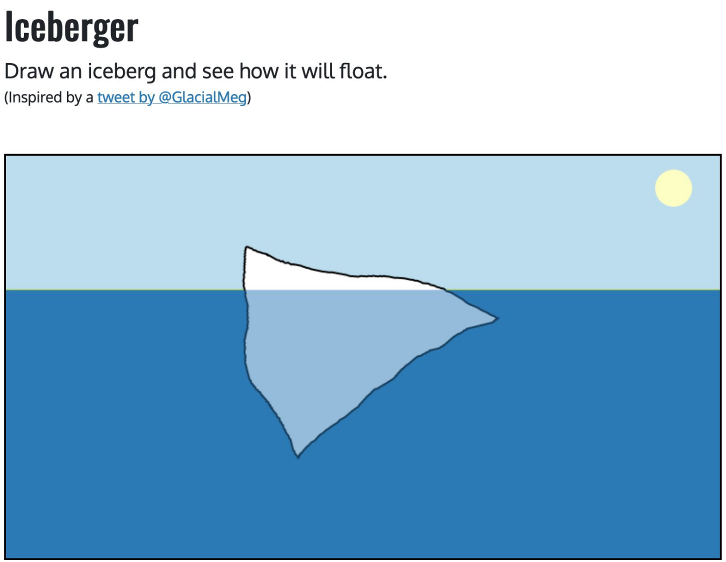
WRONG



Iceberger

Draw an iceberg and see how it will float.

(Inspired by a tweet by @GlacialMeg)

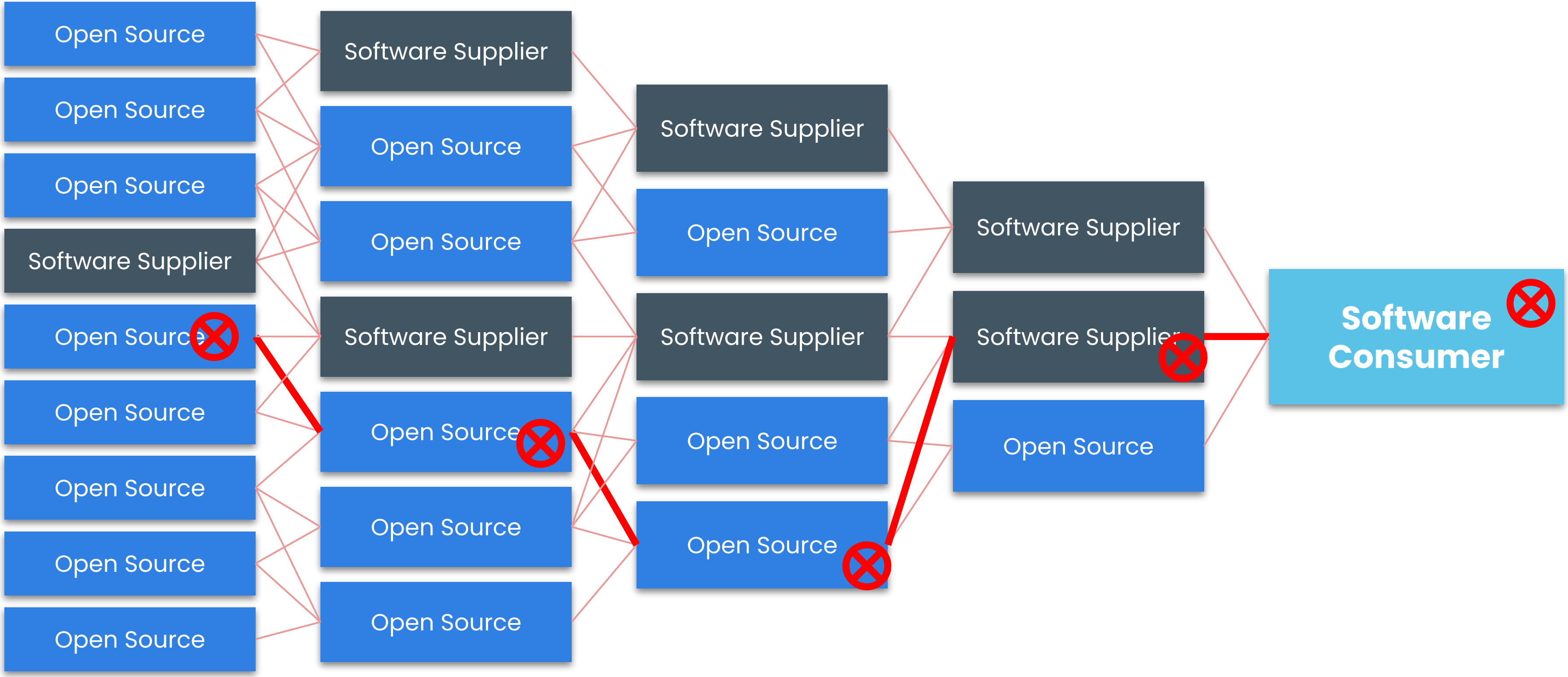


Iceberger

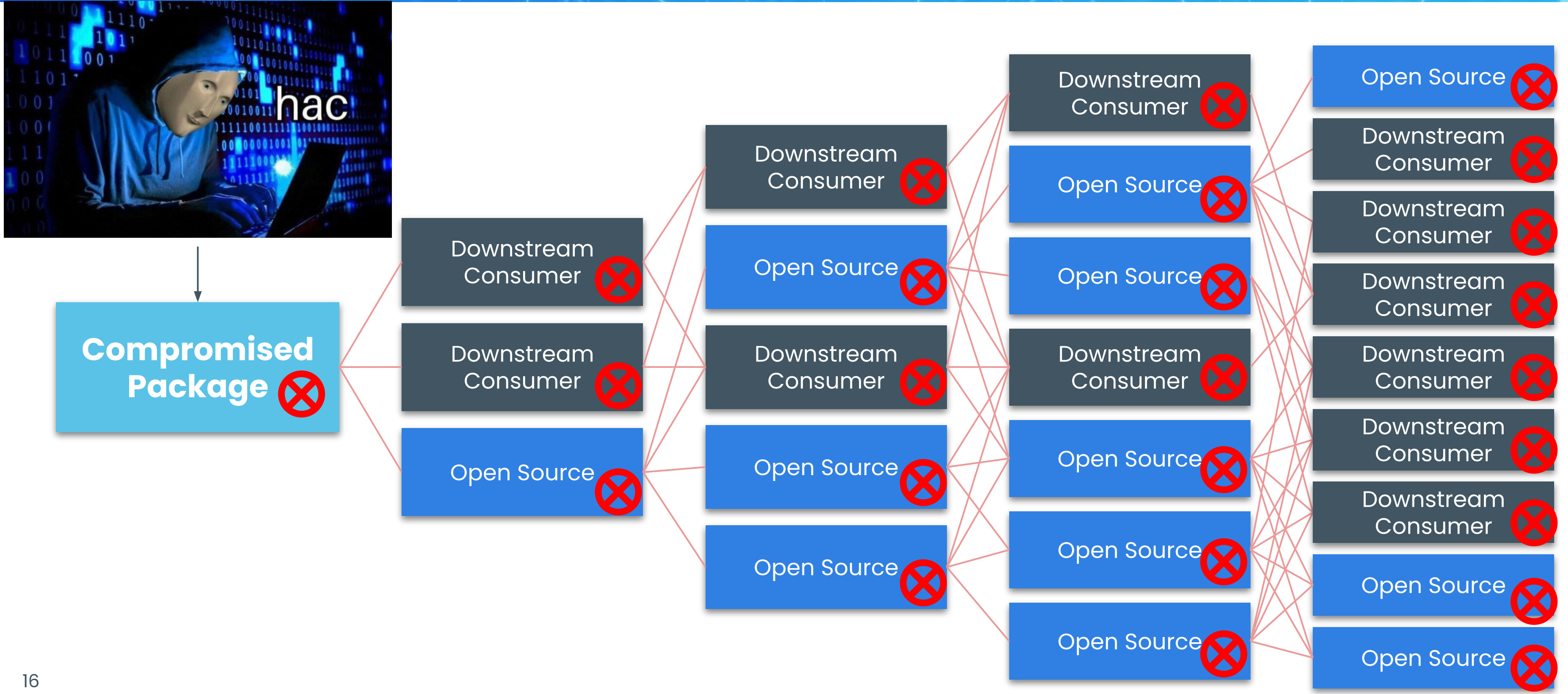
Draw an iceberg and see how it will float.

(Inspired by a tweet by @GlacialMeg)

Software Supply Chain: The Problem



The Reverse Funnel



Compromised Package

Downstream Consumer

Downstream Consumer

Open Source

Downstream Consumer

Open Source

Downstream Consumer

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

Downstream Consumer

Downstream Consumer

Downstream Consumer

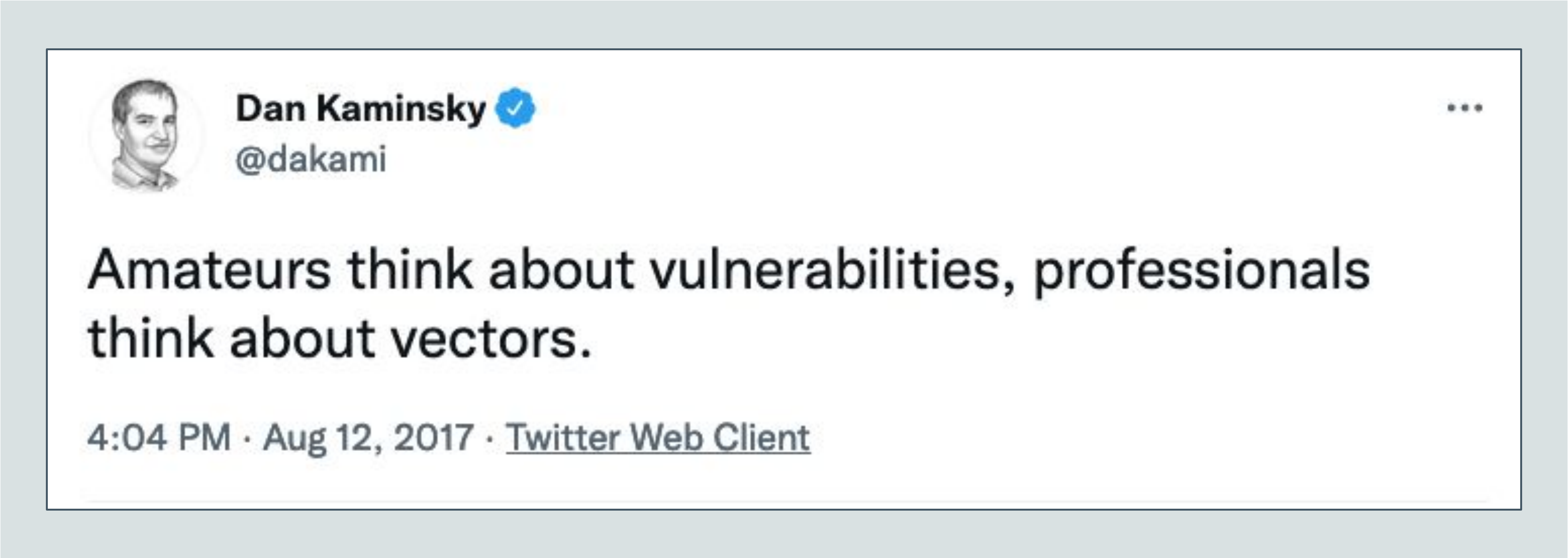
Open Source

Open Source

What's in this Image?

Knowing is half the battle.

anchore



Dan Kaminsky

@dakami

Amateurs think about vulnerabilities, professionals think about vectors.

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

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.

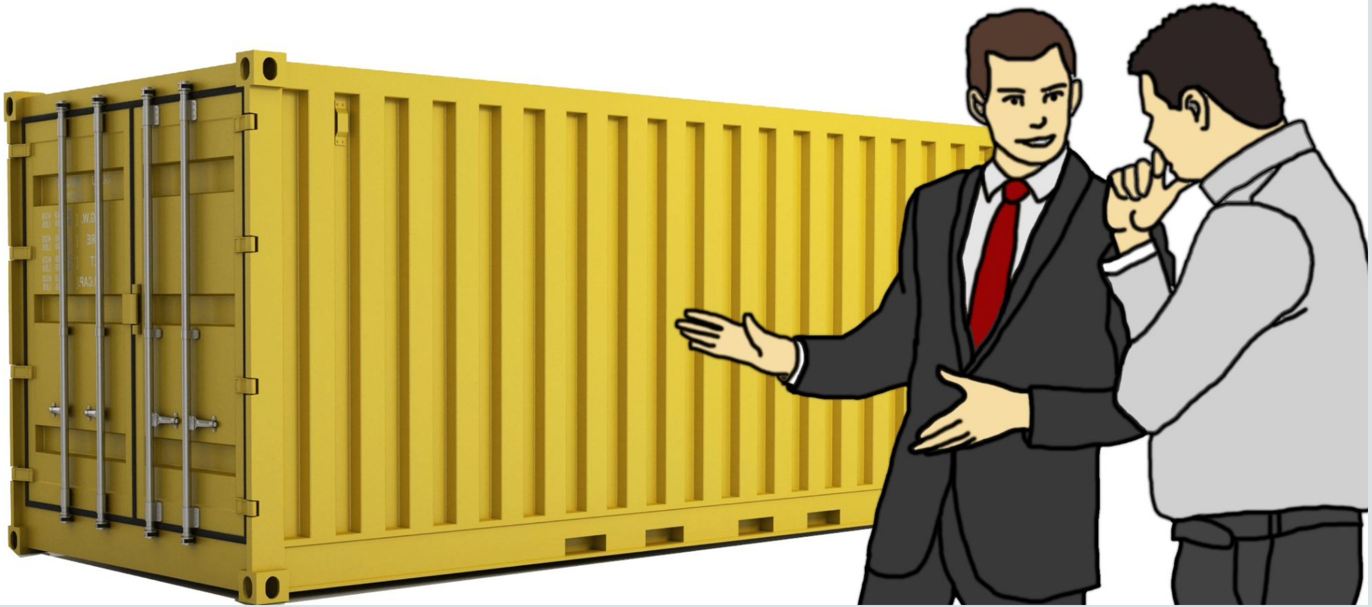
04

Credentials

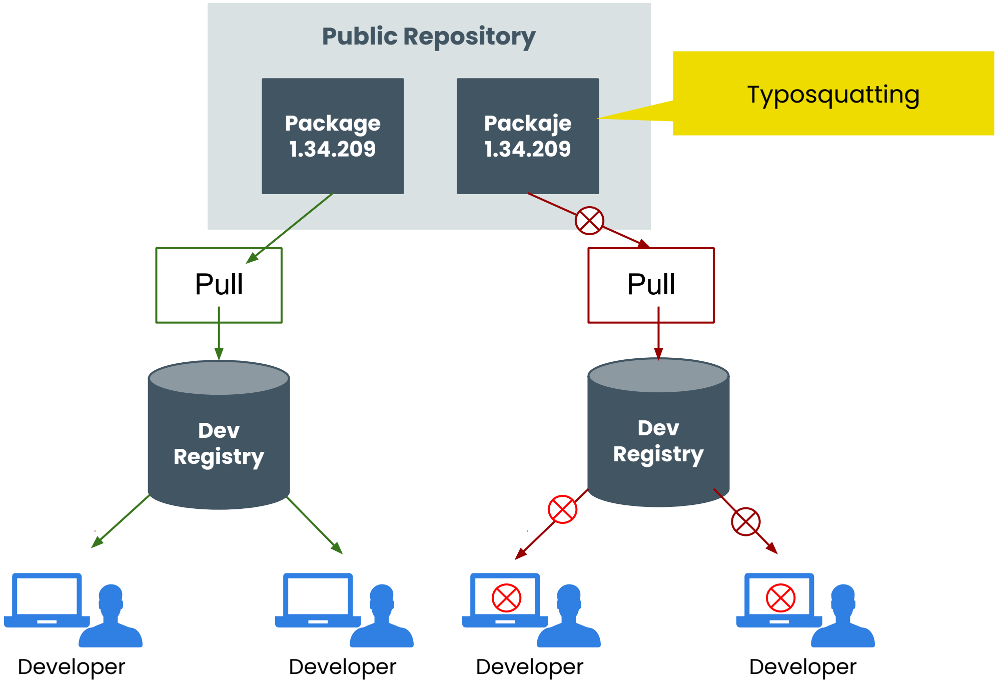
Unintentional inclusion of dev or prod secrets, keys, or other credentials accidentally included in the container.

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

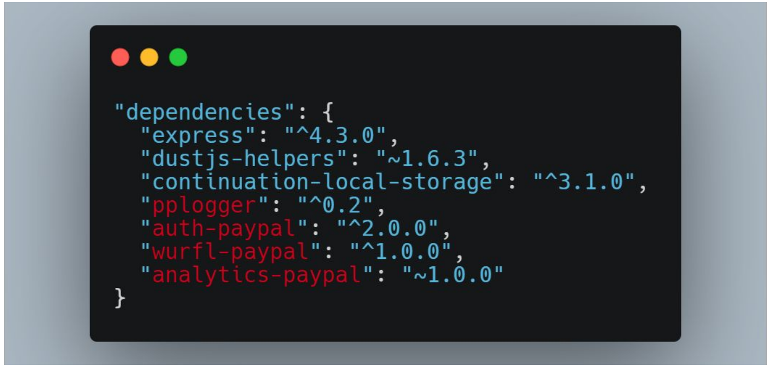
slaps roof of container this bad boy can fit so many supply chain attacks in it



Know What You’re Getting



Typosquatting



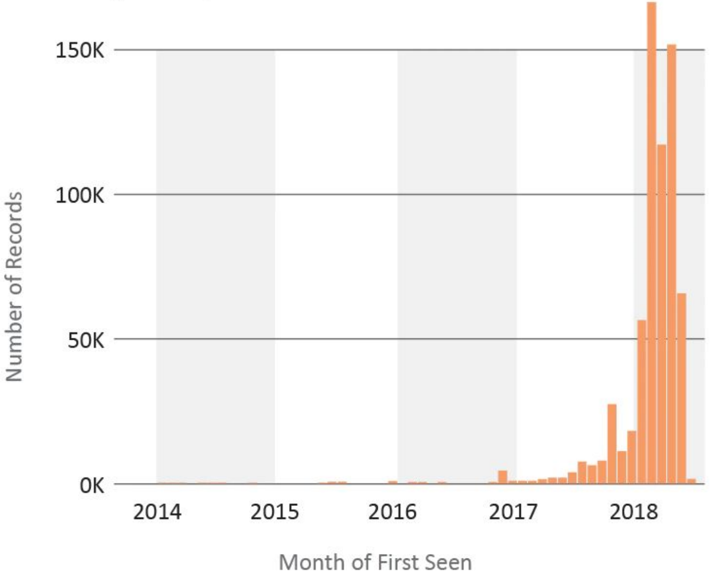
```
"dependencies": {
  "express": "^4.3.0",
  "dustjs-helpers": "~1.6.3",
  "continuation-local-storage": "^3.1.0",
  "pplogger": "^0.2",
  "auth-paypal": "^2.0.0",
  "wurfl-paypal": "^1.0.0",
  "analytics-paypal": "~1.0.0"
}
```

Dependency Confusion

What Is Cryptomining?

- Malware that infects computers, turning them into zombies used to mine for cryptocurrency without the users knowledge
- Steadily on the rise since 2017
- A prevalent form of attack in misconfigured Kubernetes clusters
- Two well-known attacks:
  - Kubeflow
  - ArgoCD

Figure 1. Cryptocurrency Mining Malware Detections from 2014-2018, courtesy of several CTA members



Illicit Cryptocurrency Mining Threat White Paper - Cyber Threat Alliance

What is Image Typosquatting?

- Humans make mistakes, there is no spell check when pulling images
  - ngniz:latest,
  - postgress:latest,
  - mysqll:latest
- Typosquatting can be combined with cryptomining by hiding miners in a misspelled name or tag
- And yes, this really does happen...

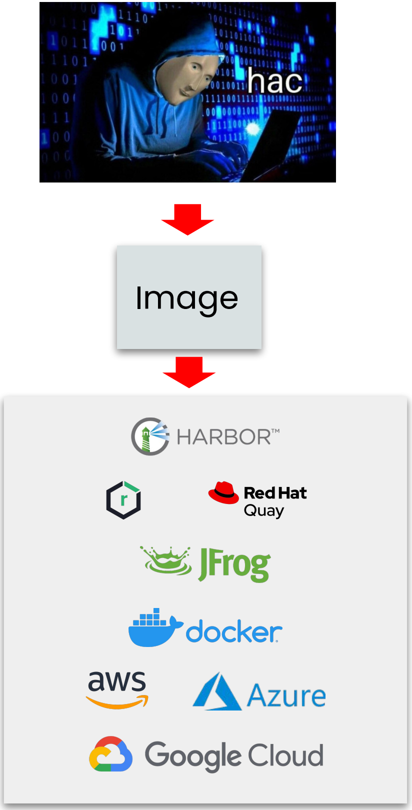
> *"Typosquatting and credential stuffing are two of the most common ways attackers try to target companies' container infrastructure and the Docker-image supply chain. Attacks are up nearly 600% in H2 2020 compared with the same period a year ago."*

DARKReading

What is Registry/Repository Poisoning?

- Registry and/or Repository Poisoning is when an attacker plants a malicious image in the victim’s registry or repository

- Registry/Repository Poisoning is particularly effective if the image appears benign. This can then easily proliferate throughout your environment



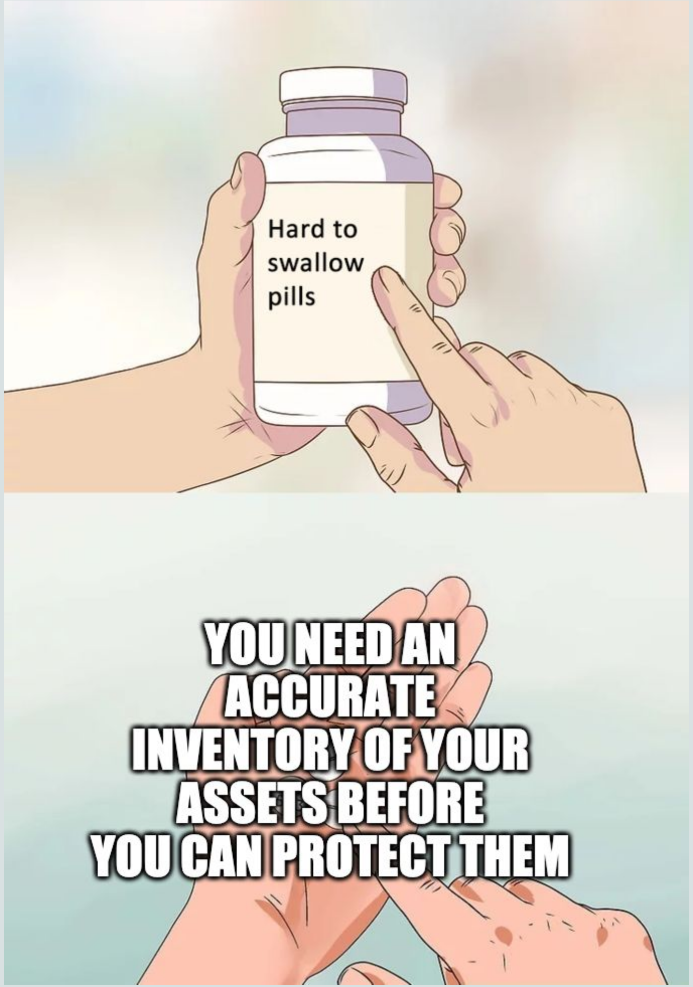
Addressing the Problem

NROL-39
NOTHING IS BEYOND OUR REACH

What’s a SBOM?

And what can it do for me?

anchore


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

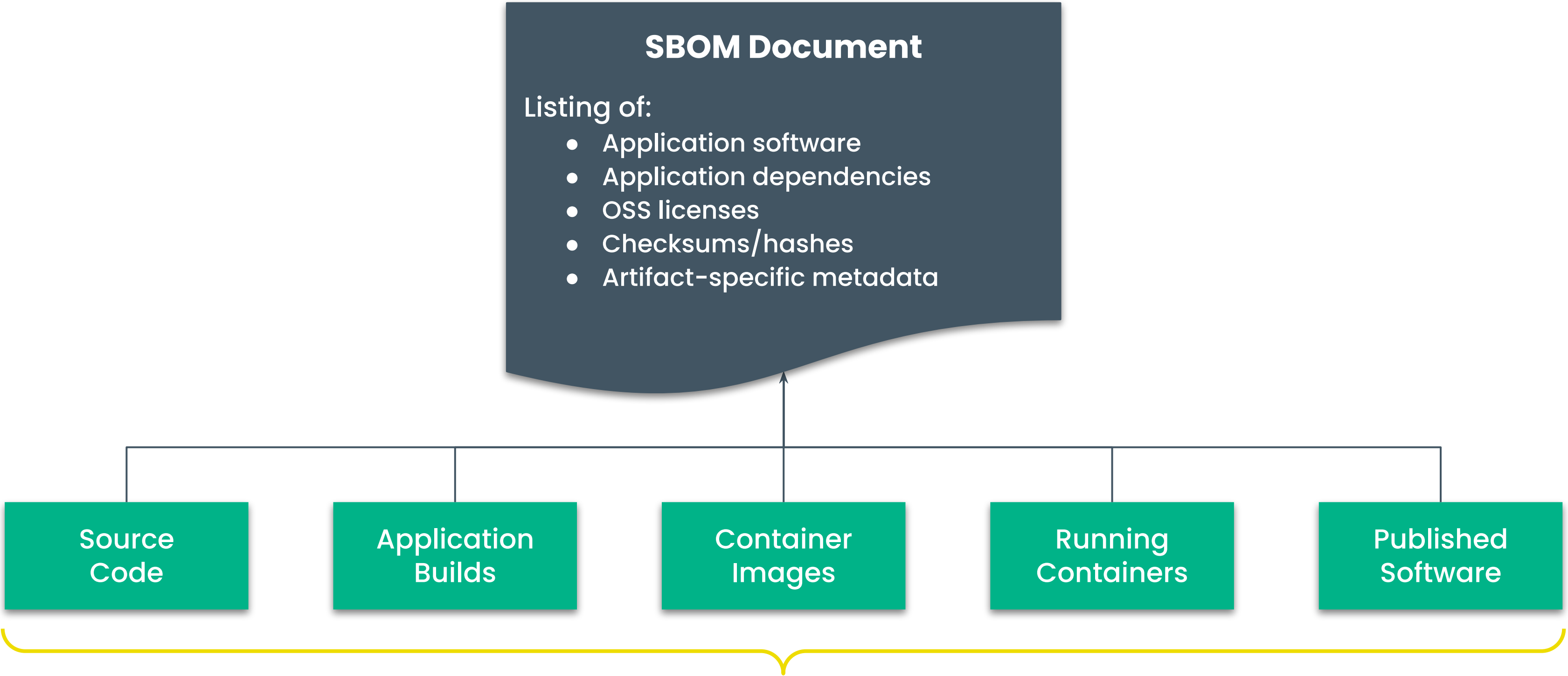
Amount Per Serving	
Calories 210	Calories from Fat 80
	% Daily Value*
Total Fat 9g	**14%**
Saturated Fat 2g	**11%**
Trans Fat 1.5g	
Cholesterol 10mg	**3%**
Sodium 390mg	**16%**
Total Carbohydrate 25g	**8%**
Dietary Fiber 2g	**7%**
Sugars 3g	
Protein 7g	

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

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

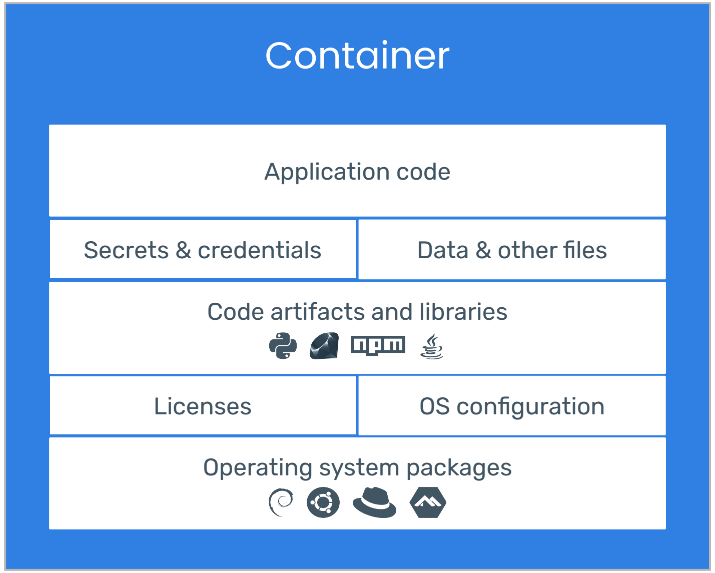
Running Containers

Published Software

Types of artifacts from which SBOMs can be generated

Containers Provide

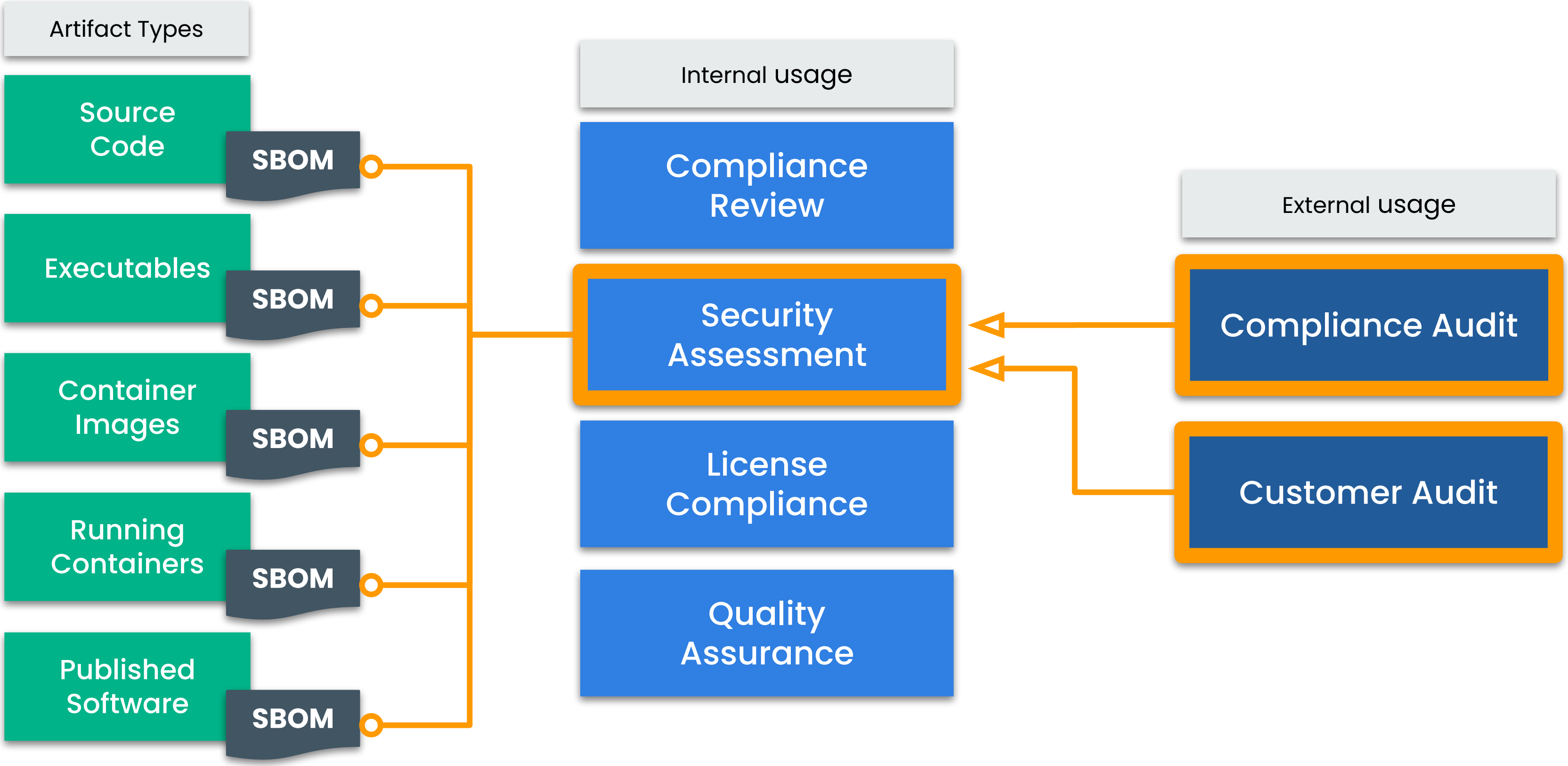
…an easy way to package and deliver



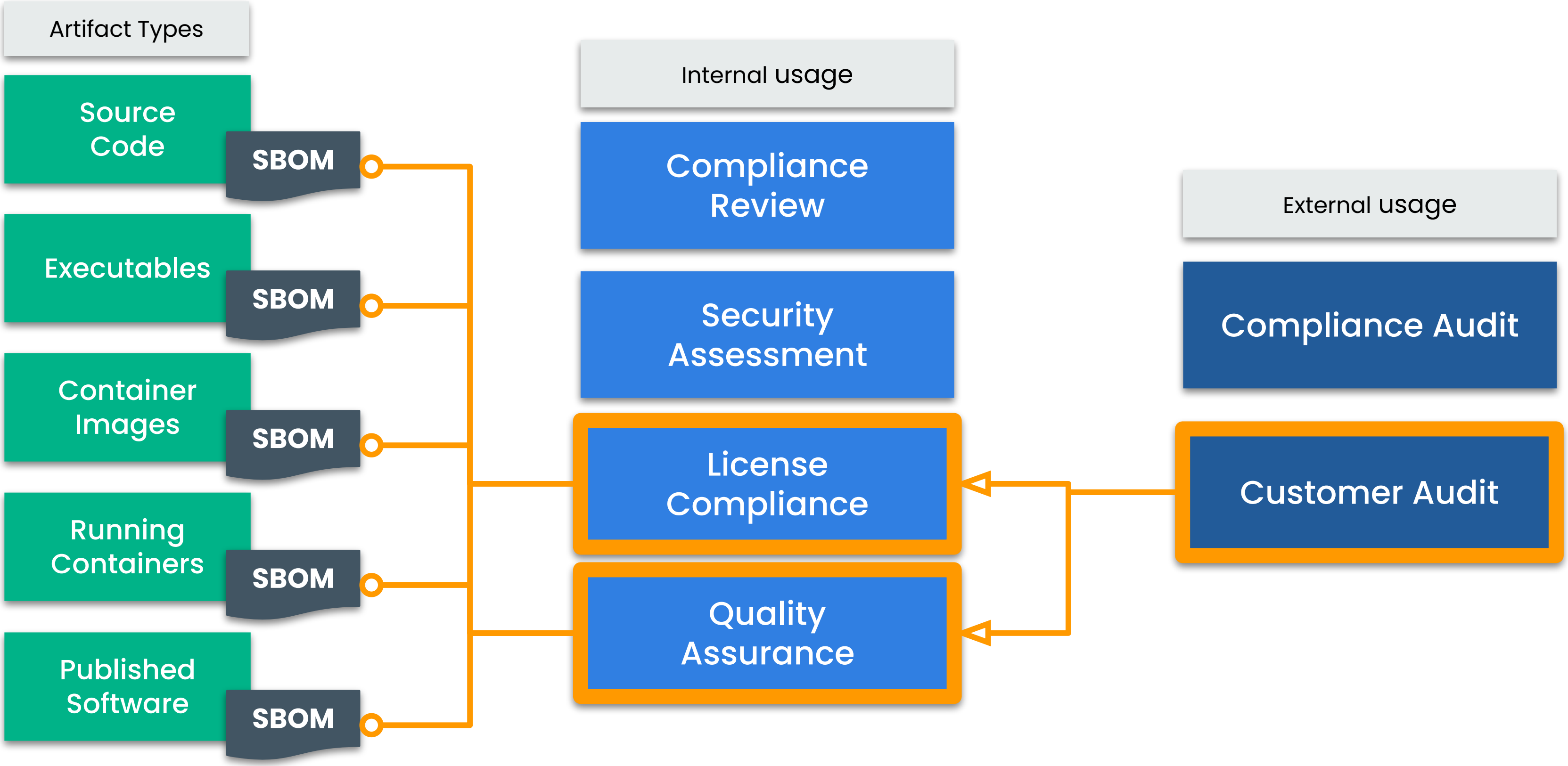
SBOM Includes

- App. dependencies
- OS Packages
- Licenses
- File data
- Configuration files
- Container metadata

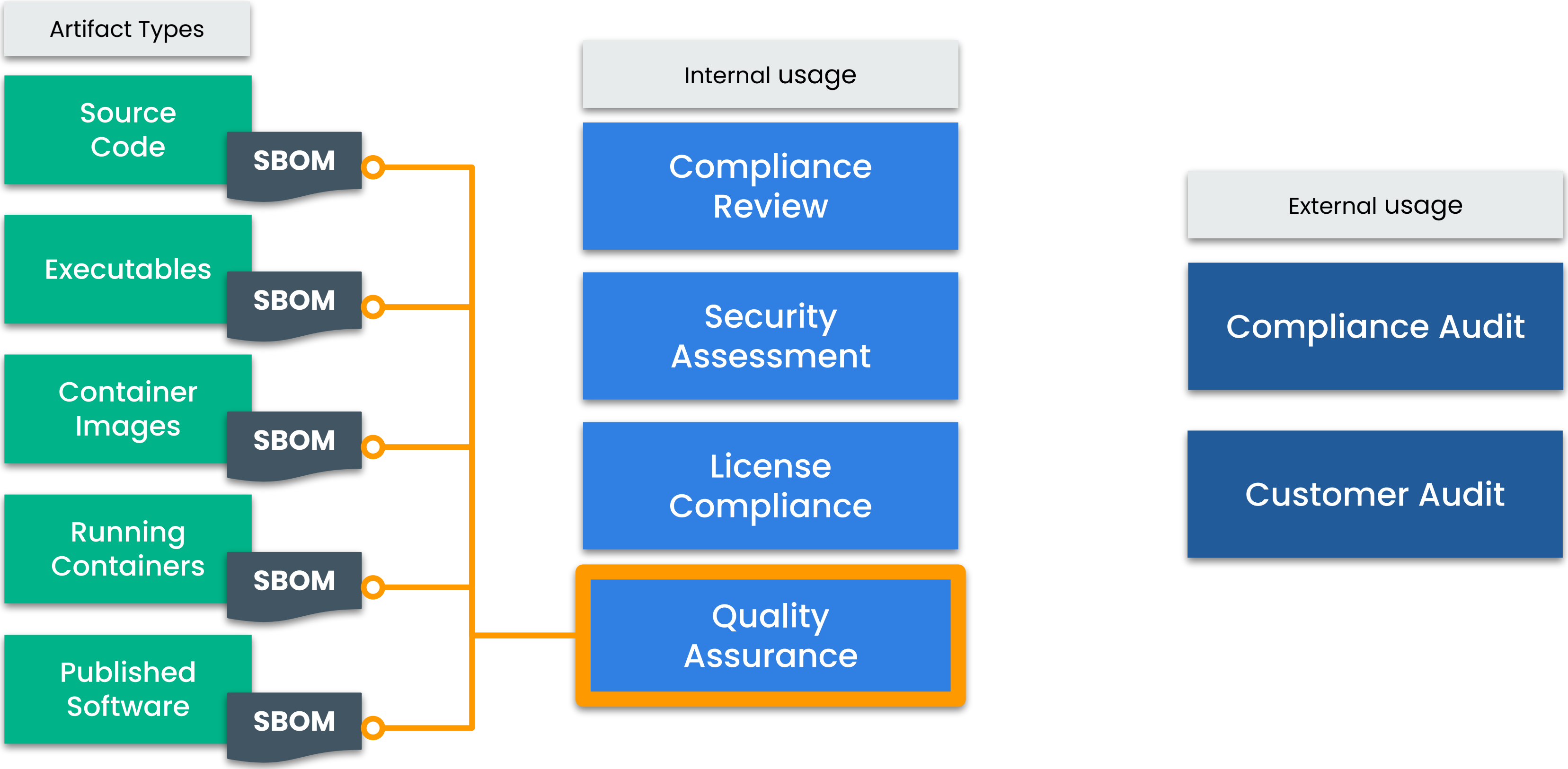
SBOM Use Case: Security Incidents



SBOM Use Case: Cross-Org Compliance



SBOM Use Case: Application Complexity



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

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

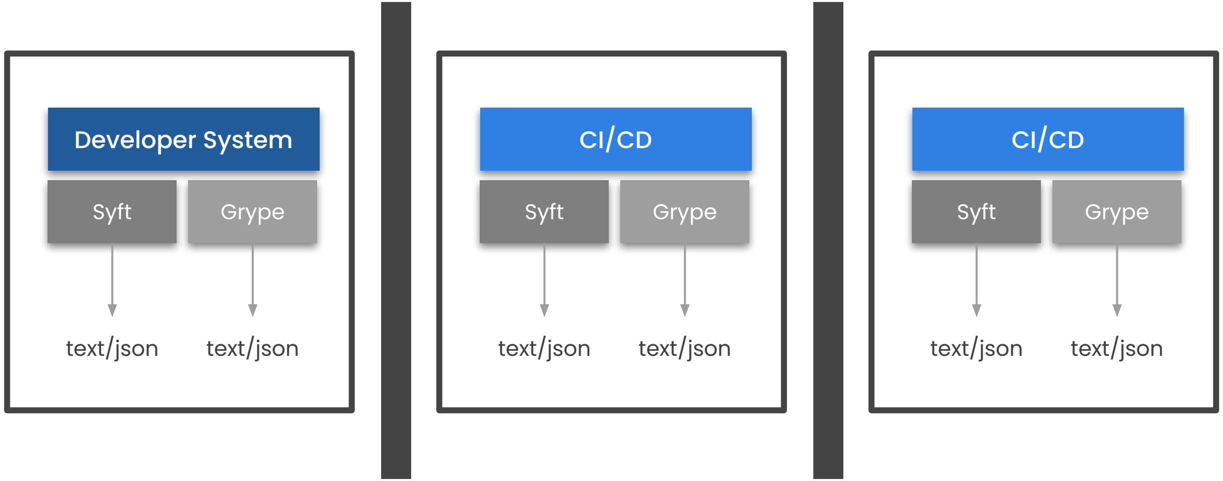
- Syft is an **open source tool that generates SBOMs** from container images and filesystems

- 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**
  - Summary table
  - JSON details
  - 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

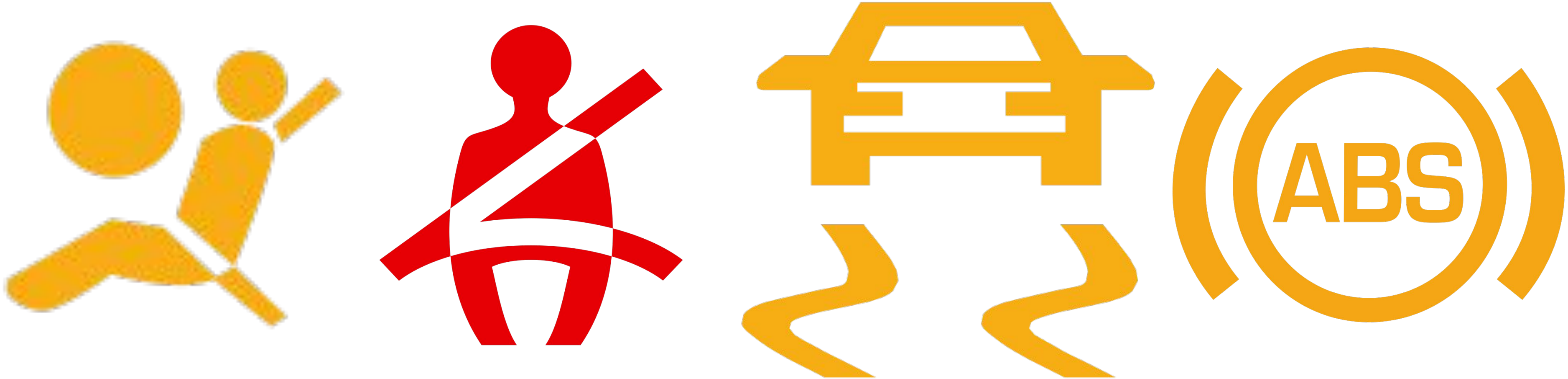
- **Lightweight** tools, written in **Go**
- **API-driven** to run in CI/CD
- **Linux** containers only
- **Local credentials** only
- **Stateless**, no data persistence
- **Siloed,** no centralized control

Now What?

How will this improve my life?

anchore

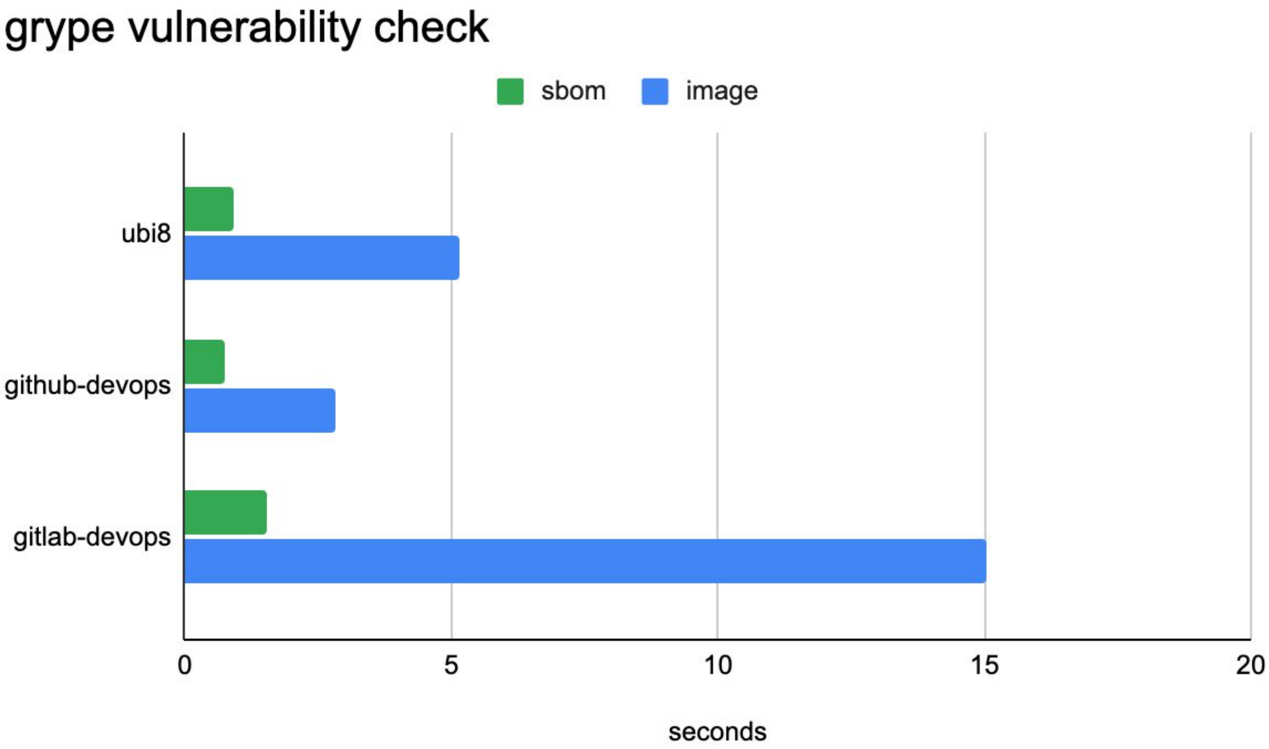
Story Time (again)



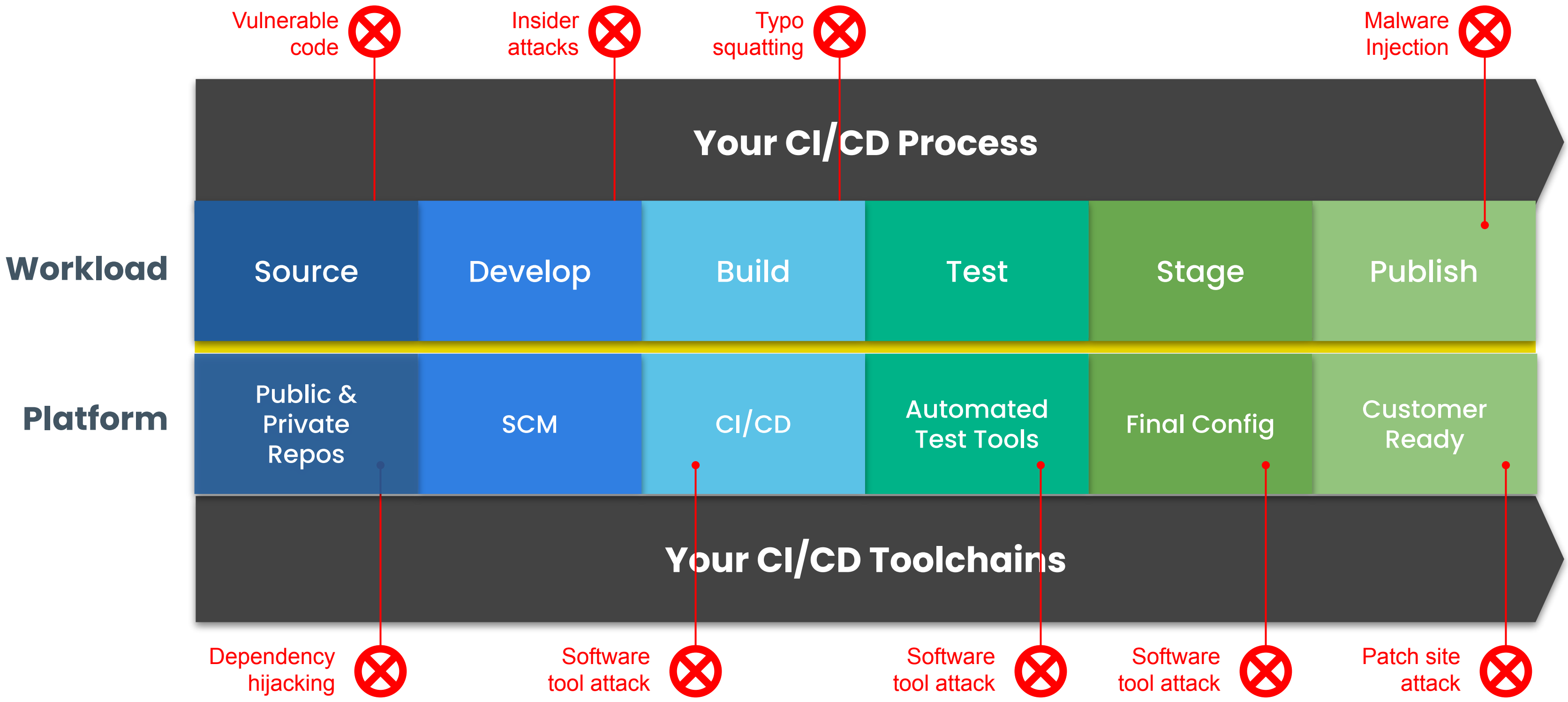
How Do SBOMs Actually Help?

Grype Scan Timing

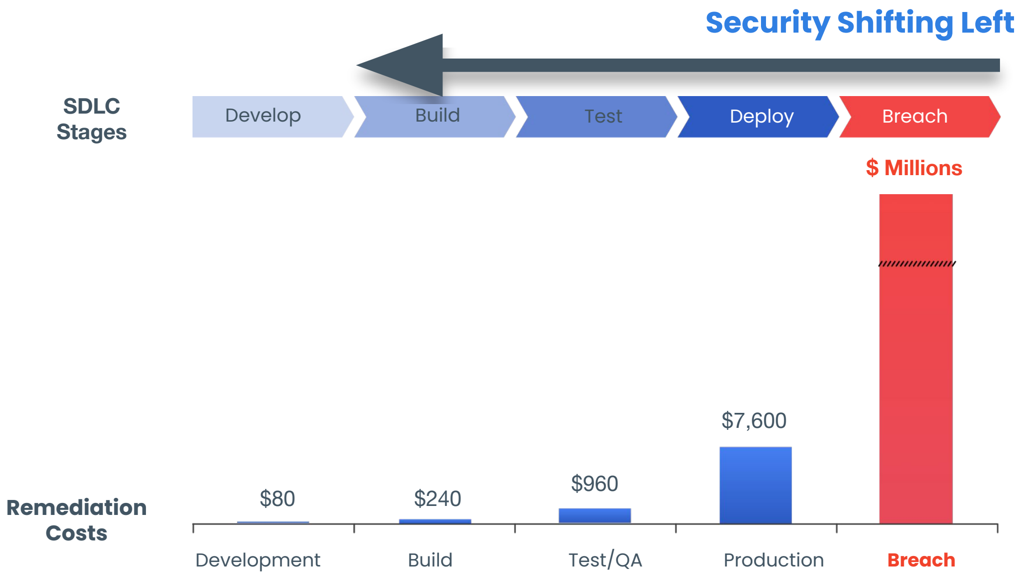
	ubi8	github -devops	gitlab -devops
sbom	0.917	0.751	1.55
image	5.159	2.839	15.031



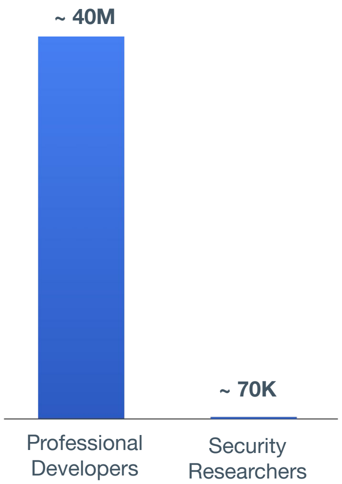
SBOMs Enable Continuous Evaluation



Shift Security Left

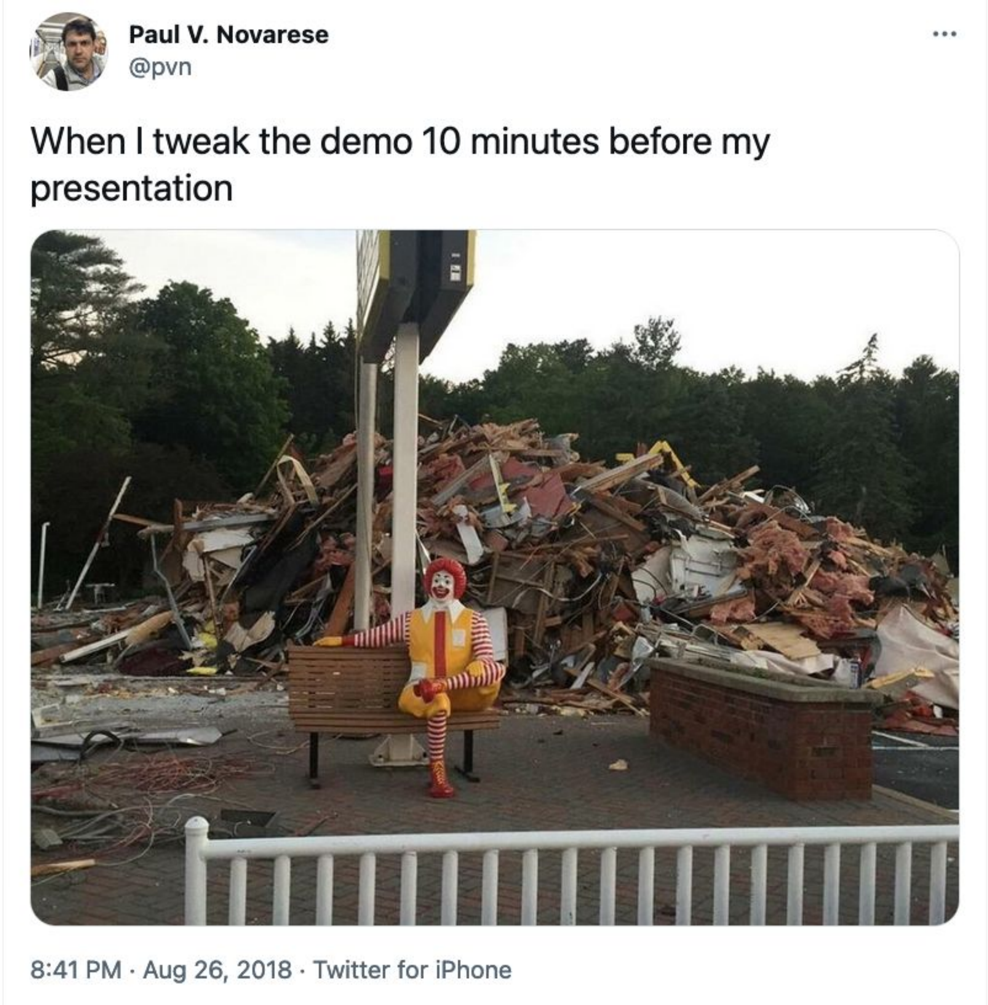


Vastly more cost effective to remediate during development



570x more developers than security researchers

STOP TALKING
DEMO TIME
memegenerato
DEMO TIME
memegenerator.net
LET'S DO
A DEMO
memegenerator.net
I CAN HAS DEMO?
DEMO?
WHAT COULD GO WRONG?
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

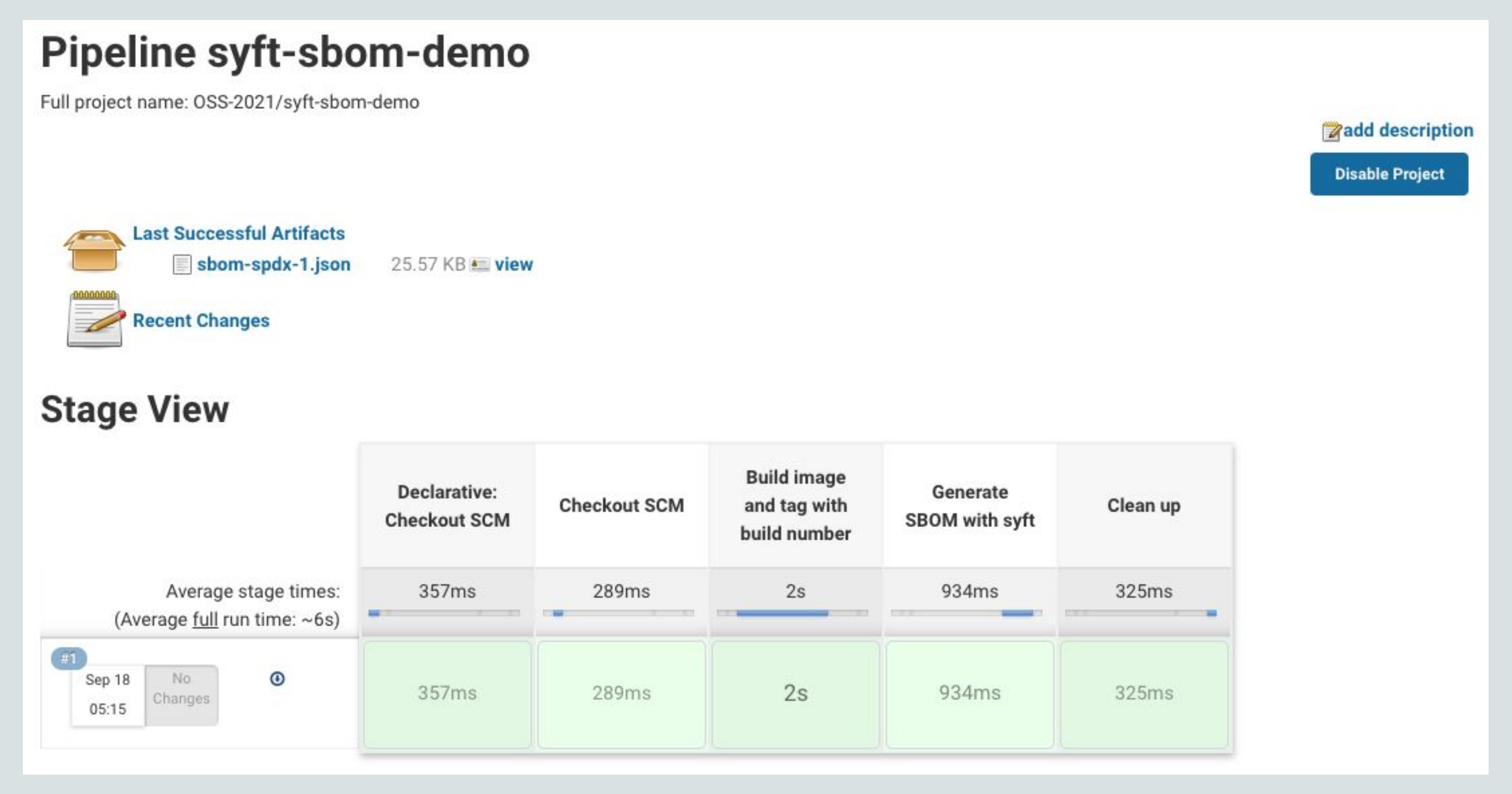
DIY Demos

- Create a SBOM in Jenkins: https://github.com/pvnovarese/oss-2021-syft-sbom-demo
  - Includes instructions on deploying a disposable Jenkins container
  - Difficulty: easy

- Complete workflow example in Github Actions with syft, grype, and cosign: https://github.com/pvnovarese/oss-2021-sbom-complete-workflow-demo
  - Includes Github Actions
  - Build an image, sign it, scan for vulns, and sign the scan results
  - Difficulty: intermediate
  - More info: Anchore Blog

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

Example SBOM Creation



Pipeline syft-sbom-demo

Full project name: OSS-2021/syft-sbom-demo

add description

Disable Project

Last Successful Artifacts

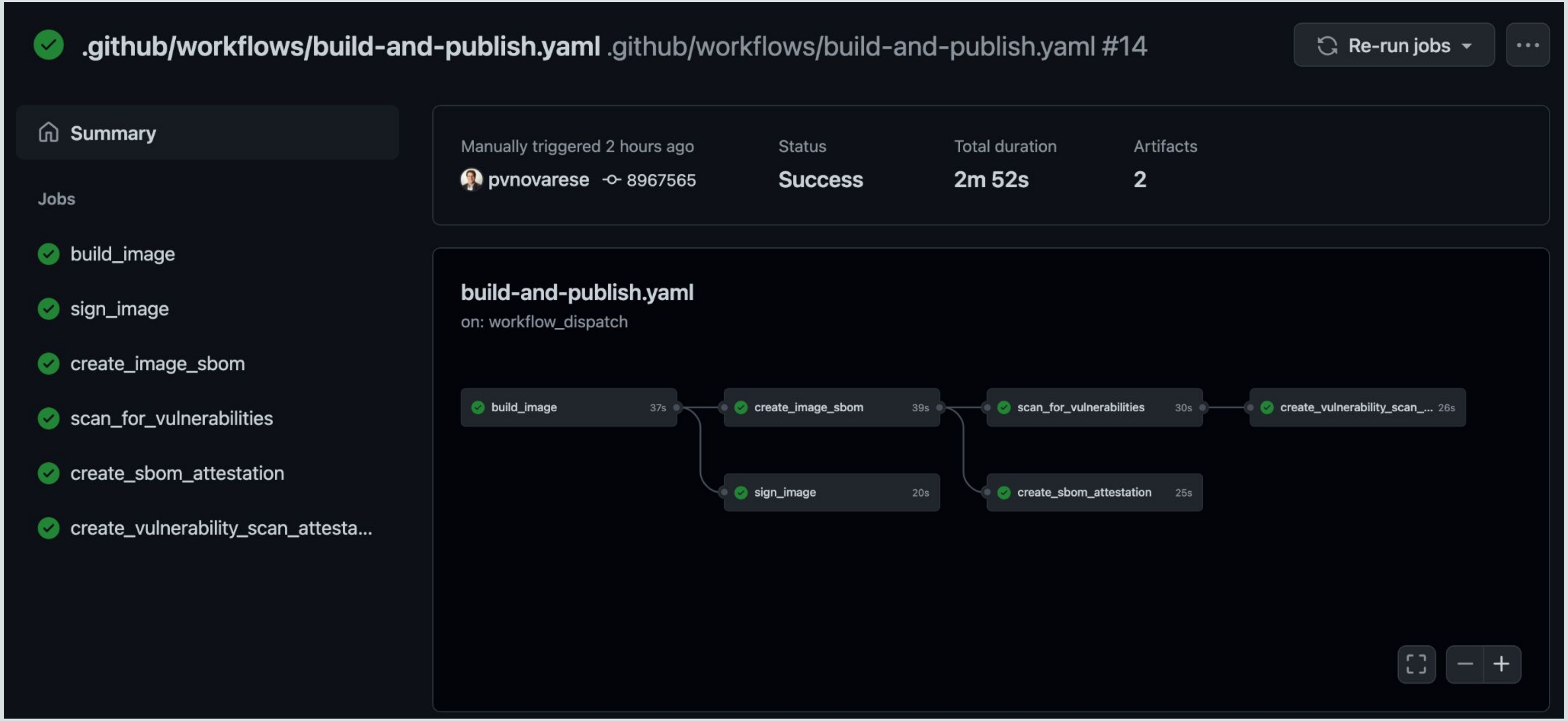
sbom-spdx-1.json 25.57 KB view

Recent Changes

Stage View

	Declarative: Checkout SCM	Checkout SCM	Build image and tag with build number	Generate SBOM with syft	Clean up
Average stage times: (Average full run time: ~6s)	357ms	289ms	2s	934ms	325ms
#1 Sep 18 05:15 No Changes	357ms	289ms	2s	934ms	325ms

Example Workflow



✓ .github/workflows/build-and-publish.yaml .github/workflows/build-and-publish.yaml #14

Jobs

- ✓ build_image
- ✓ sign_image
- ✓ create_image_sbom
- ✓ scan_for_vulnerabilities
- ✓ create_sbom_attestation
- ✓ create_vulnerability_scan_attesta...

Manually triggered 2 hours ago	Status	Total duration	Artifacts
pvnovarese -o- 8967565	Success	2m 52s	2

build-and-publish.yaml
on: workflow_dispatch

build_image 37s
create_image_sbom 39s
scan_for_vulnerabilities 30s
create_vulnerability_scan_... 26s
sign_image 20s
create_sbom_attestation 25s

Best Practices for Securing the Software Supply Chain

01 Centralized, secure CI/CD process for all software

02 Build images from trusted sources

03 Automate security testing and policy enforcement

04 Deploy only trusted images into production

Q&A

Download Syft

https://github.com/anchore/syft

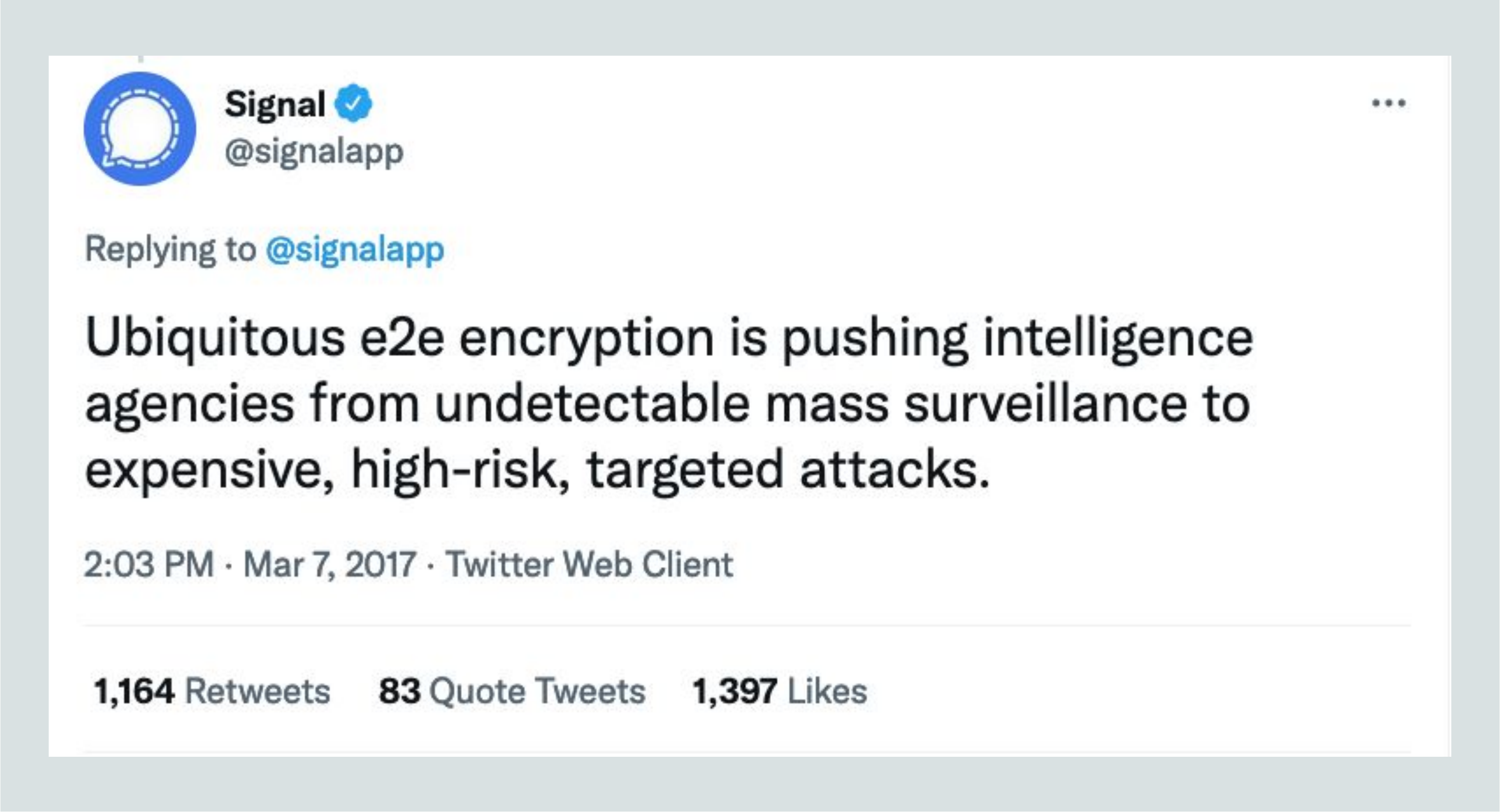
Download Grype

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/

anchore



Signal

@signalapp

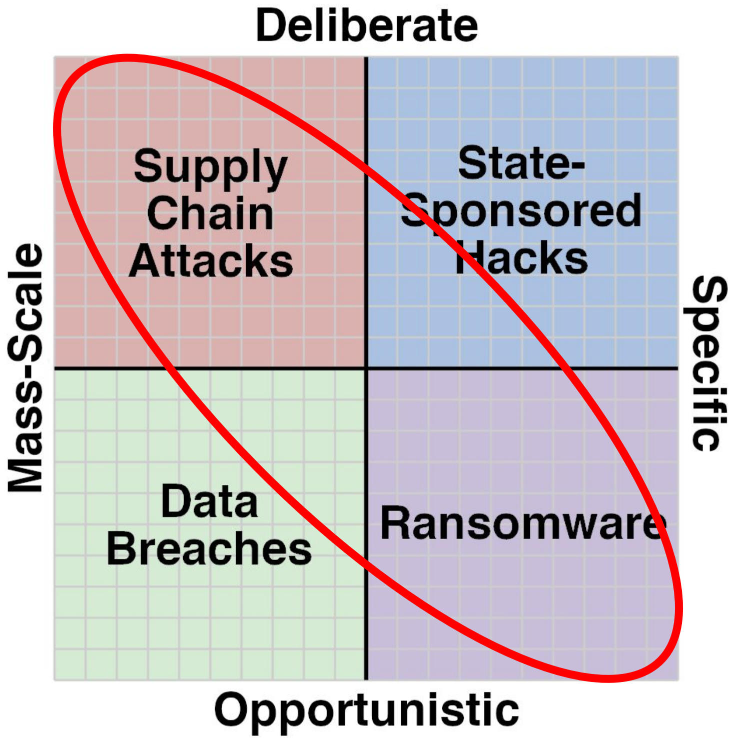
Replying to @signalapp

Ubiquitous e2e encryption is pushing intelligence agencies from undetectable mass surveillance to expensive, high-risk, targeted attacks.

2:03 PM · Mar 7, 2017 · Twitter Web Client

1,164 Retweets **83** Quote Tweets **1,397** Likes

Takeaways

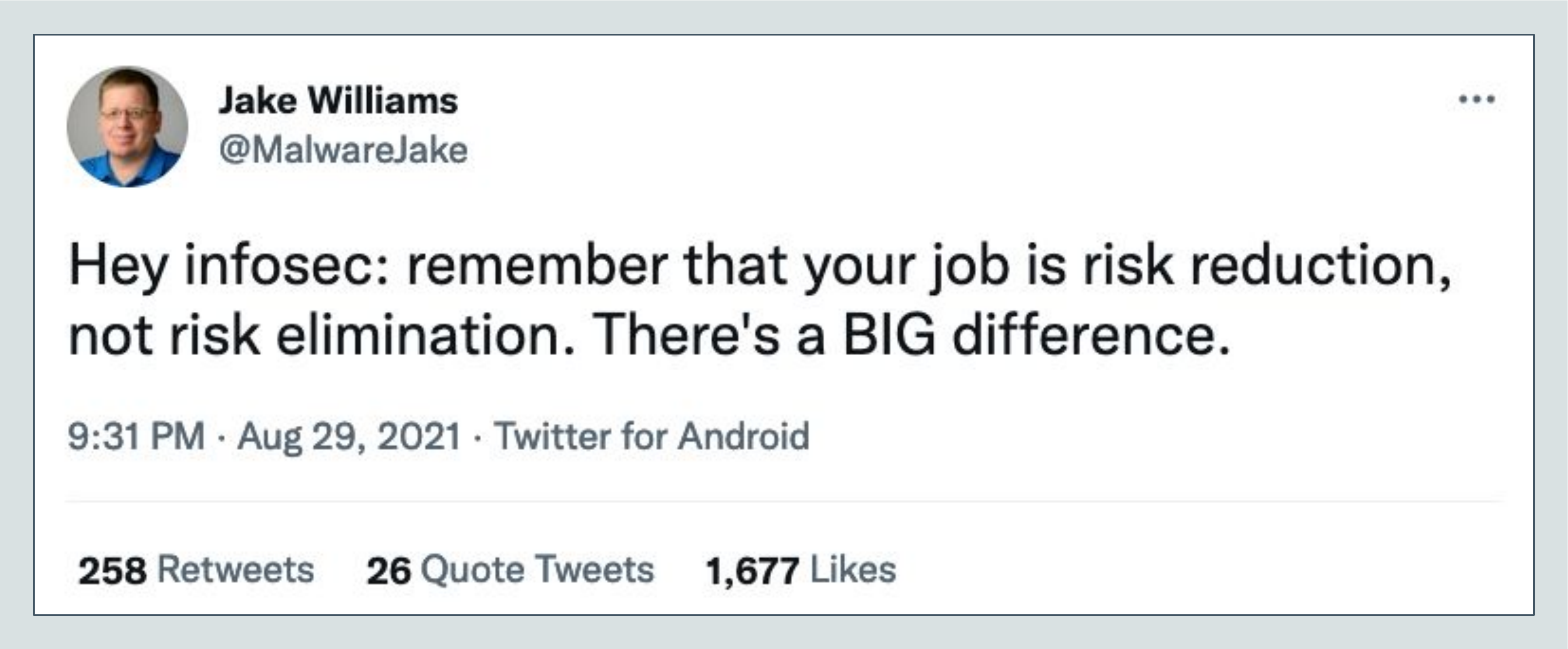

Deliberate
Supply Chain Attacks
State-Sponsored Hacks
Mass-Scale
Specific
Data Breaches
Ransomware
Opportunistic

One Last Thing

City of Toronto Archives, Fonds 1266, Item 5859

Douglas Haig

“Bullets have little stopping power against the horse” (1914)



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

Thanks!

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/

anchore

Reading List

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/

Github SBOM action: https://github.com/marketplace/actions/anchore-sbom-action

Footnotes

Twitter Links/Credits:
https://twitter.com/codinghorror/status/786667942142435329
https://twitter.com/dakami/status/896477575475642368
https://twitter.com/mikemearls/status/1079999471109337088

Other notes:
https://en.wikipedia.org/wiki/Douglas_Haig,_1st_Earl_Haig
https://en.wikipedia.org/wiki/USA-247
https://joshdata.me/iceberger.html

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

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

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