anchore

# Secure Your Cloud-Native Software Supply Chain

anchore

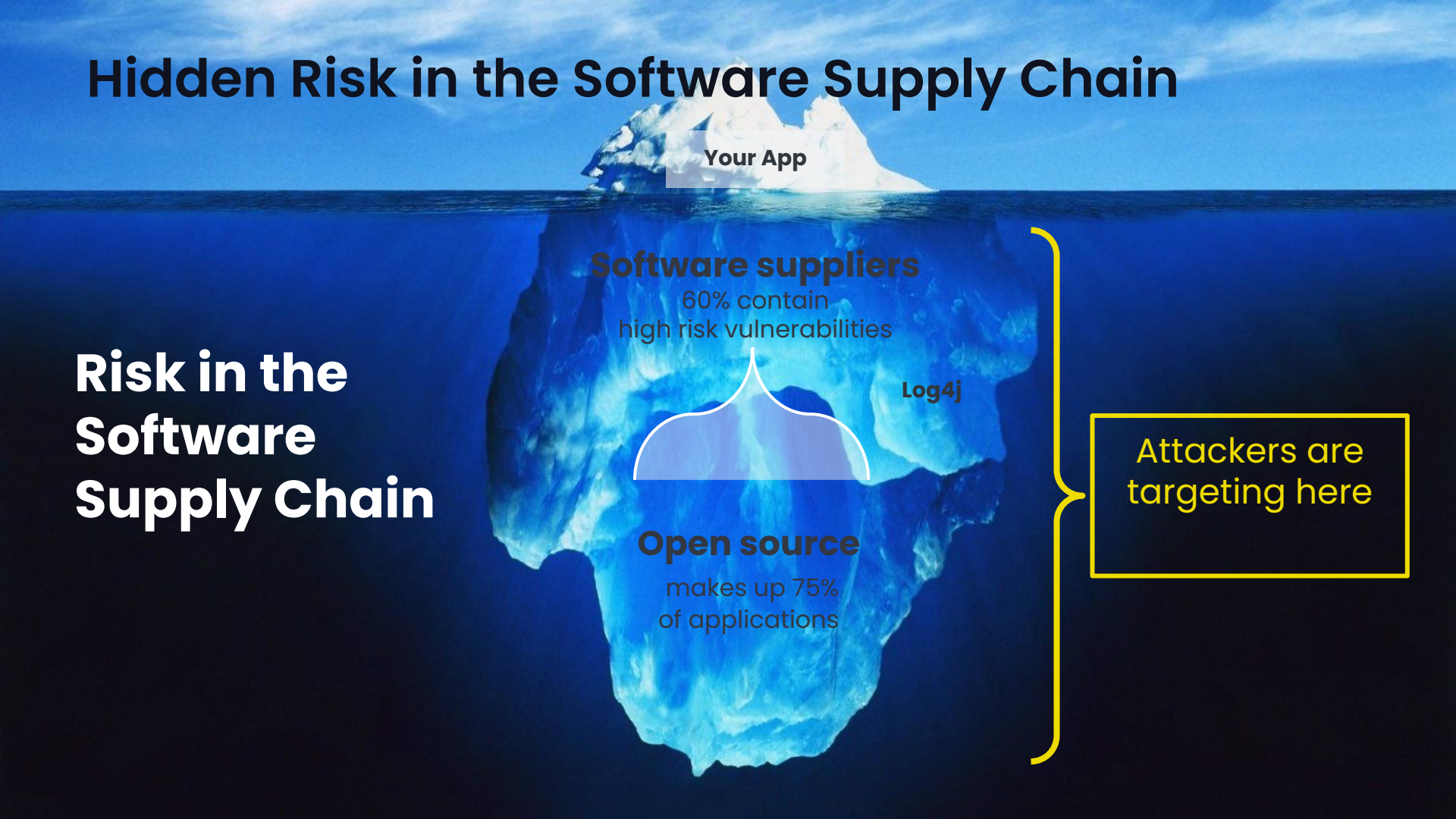
# Anchore SBOM Workshop

Paul Novarese
Principal Solutions Engineer
pvn@anchore.com
2023-09-26

anchore

# What is the Software Supply Chain?

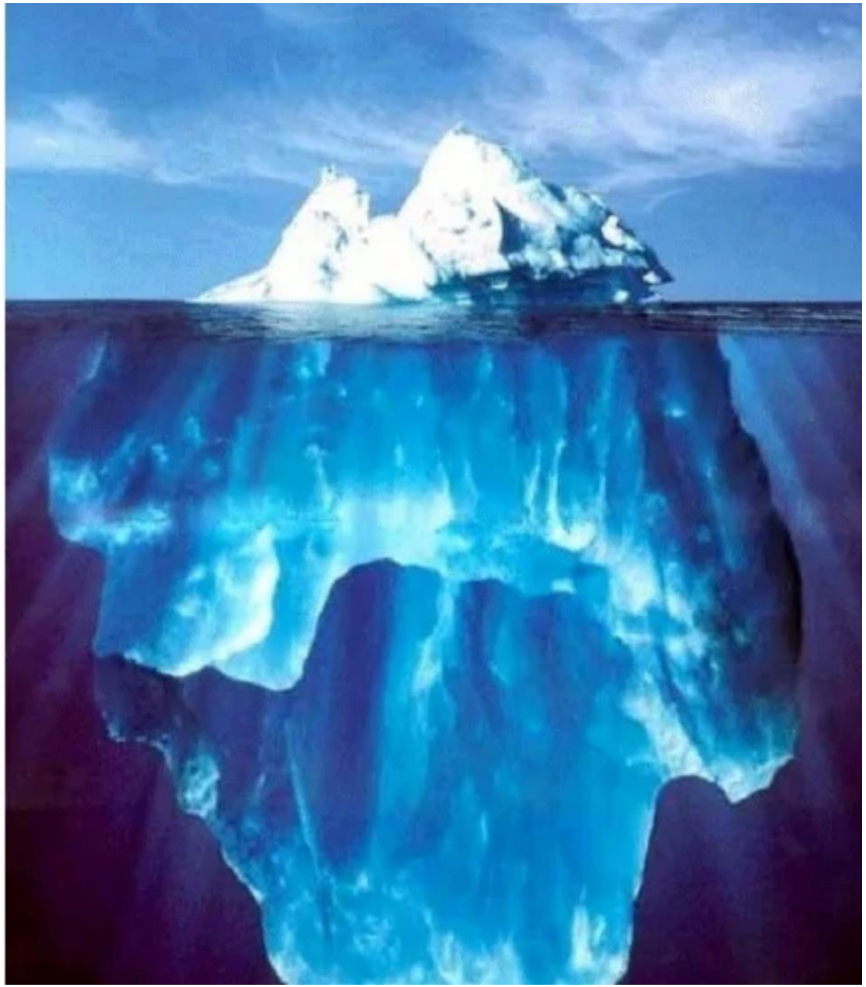
# Hidden Risk in the Software Supply Chain

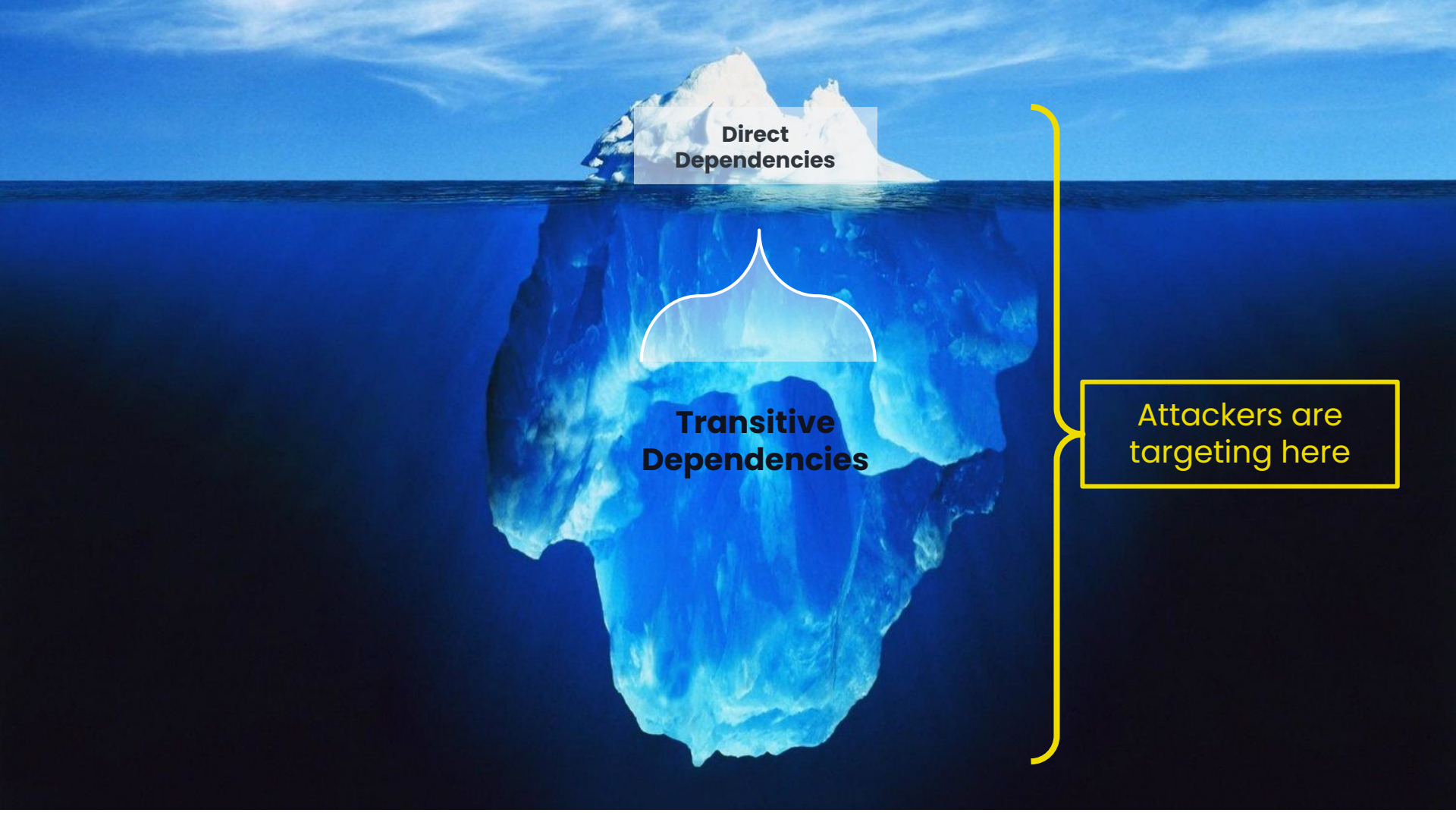



**Risk in the Software Supply Chain**

# Free is Just the Tip of the Iceberg: Open Source Library System Software

Lori Bowen Ayre
lori.ayre@galecia.com
METRO Webinar
October 6, 2009

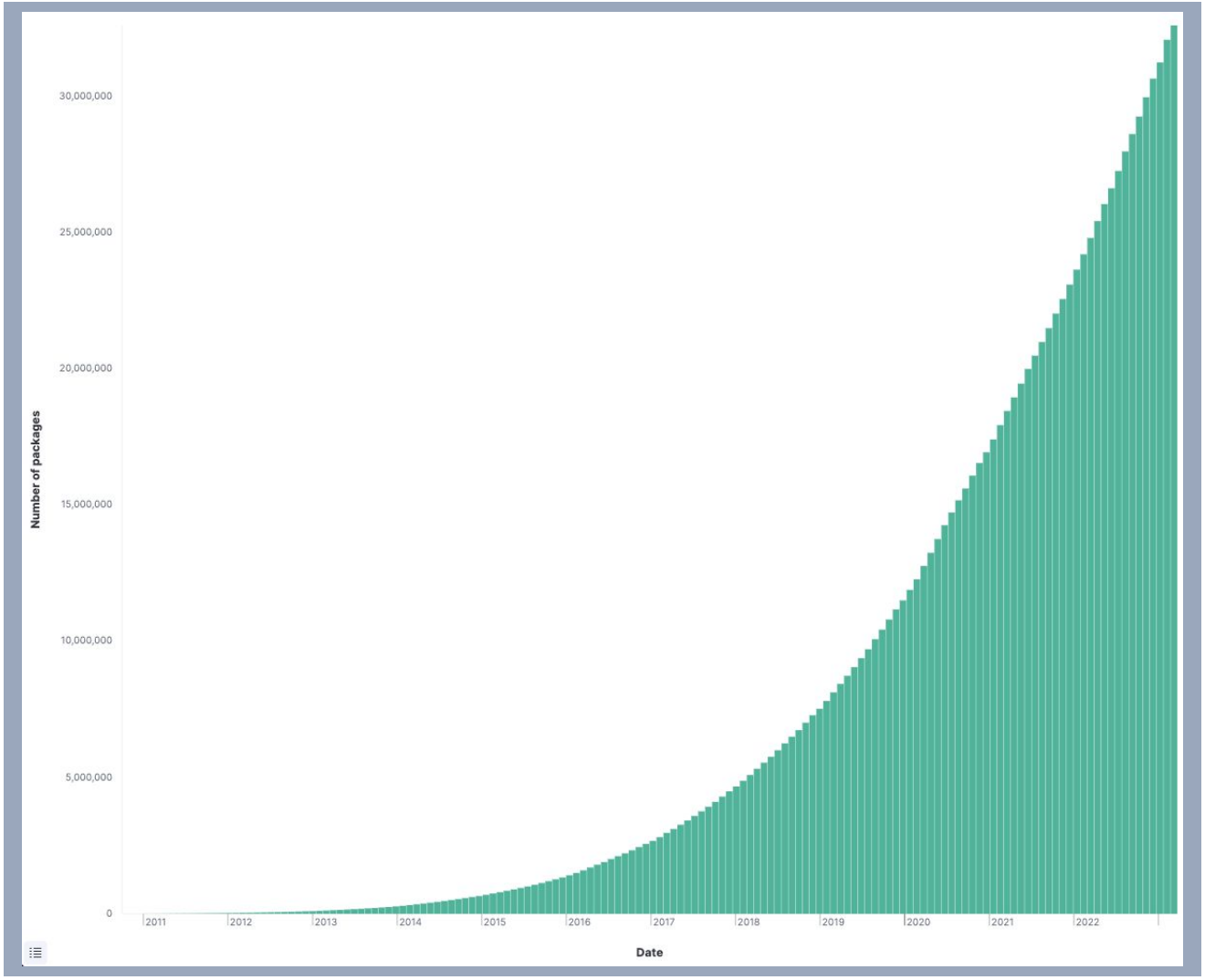



Direct
Dependencies
Transitive
Dependencies
Attackers are
targeting here

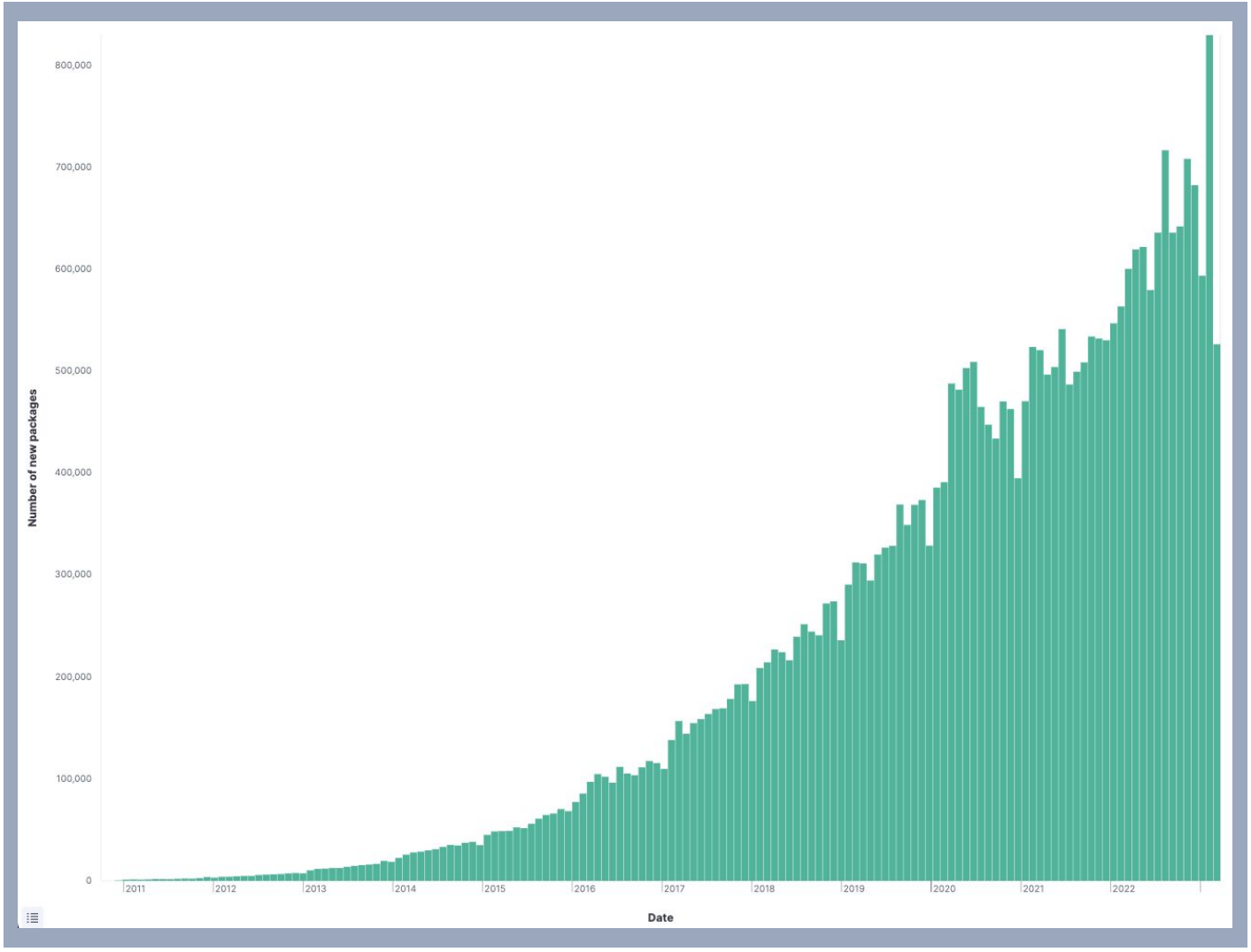
# This metaphor...

- You've seen this iceberg metaphor. I've used this metaphor 100 times, I've criticized this metaphor.
- This is an OLD metaphor
- Things have changed a lot but we're still thinking about old systems
- https://www.slideshare.net/loriayre/open-source-library-system-software-free-is-just-the-tip-of-the-iceberg
- They're attacking the bottom now - that's a supply chain attack
- But really, the top isn't "your code" - the top is your direct dependencies, bottom is transitive
- You can only directly control what's at the top
- They're attacking the whole iceberg, but you probably only know about the stuff at the top

Number of
NPM packages



Number of
NEW packages

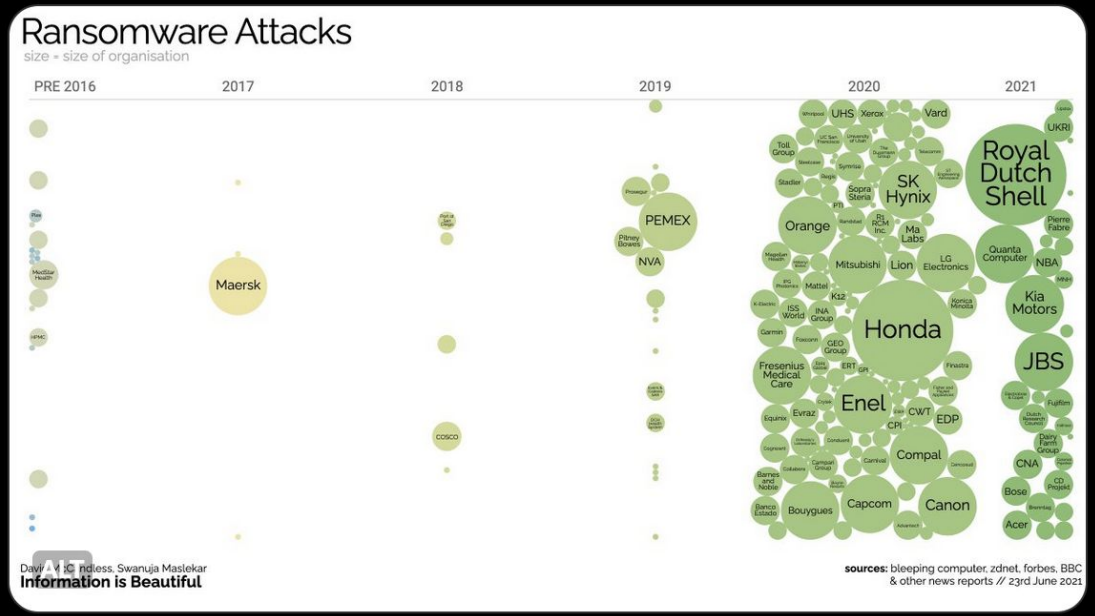


# Open source is huge

- NPM introduced 2010
- 32 million packages (as of March 2023)
- Approx. 1,000,000 new packages **per month**
- That’s just NPM!

**Information is Beautiful**
@infobeautiful

Are #Ransomware attacks increasing? I think #Ransomware attacks are increasing...
interactive: bit.ly/3h1IYPs

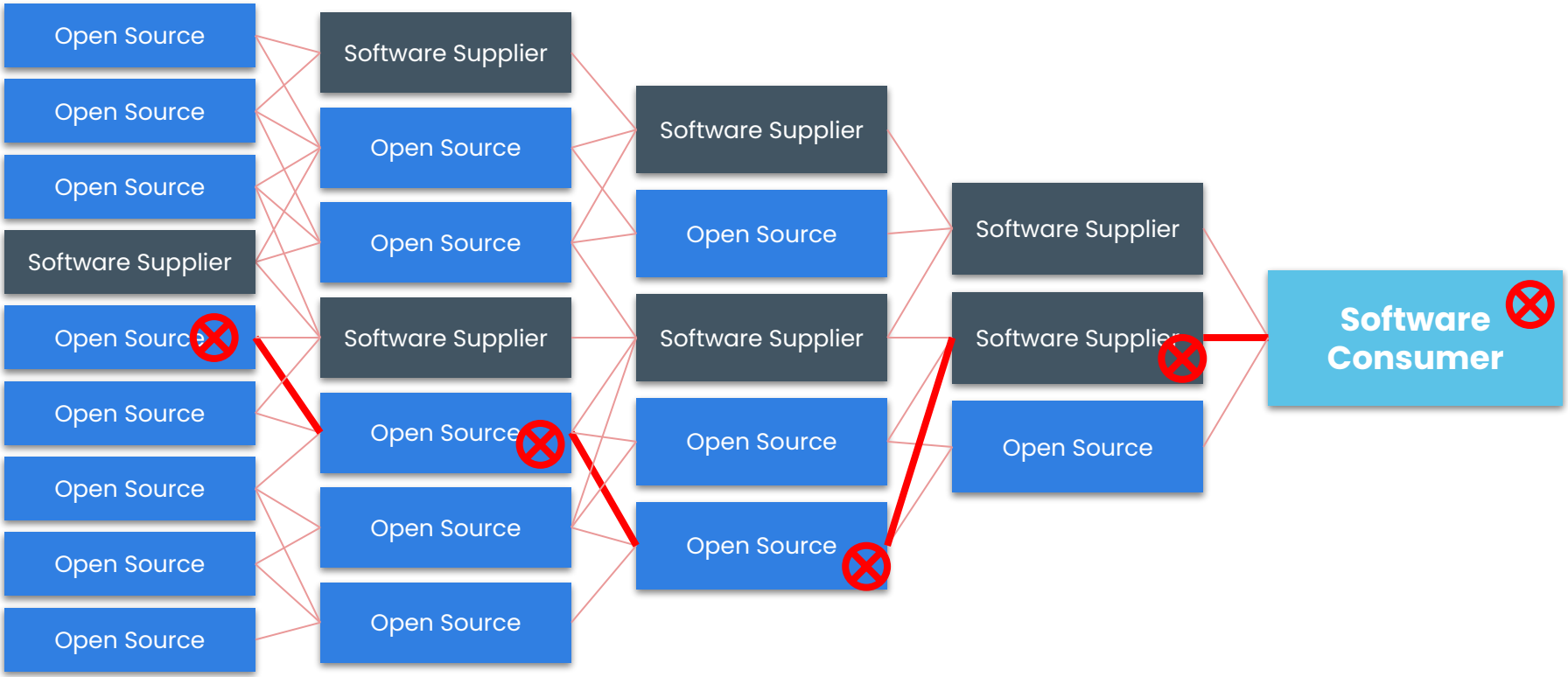



11:33 AM · Jun 23, 2021

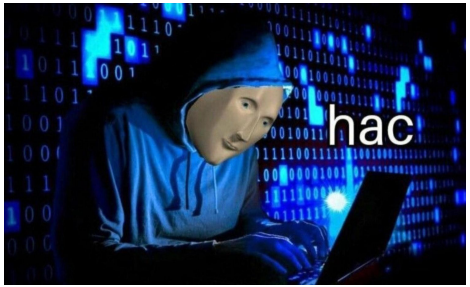
# The predictable consequence

- Ransomware has exploded along with transitive dependencies and open source in general
- I don’t believe in coincidences

# 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

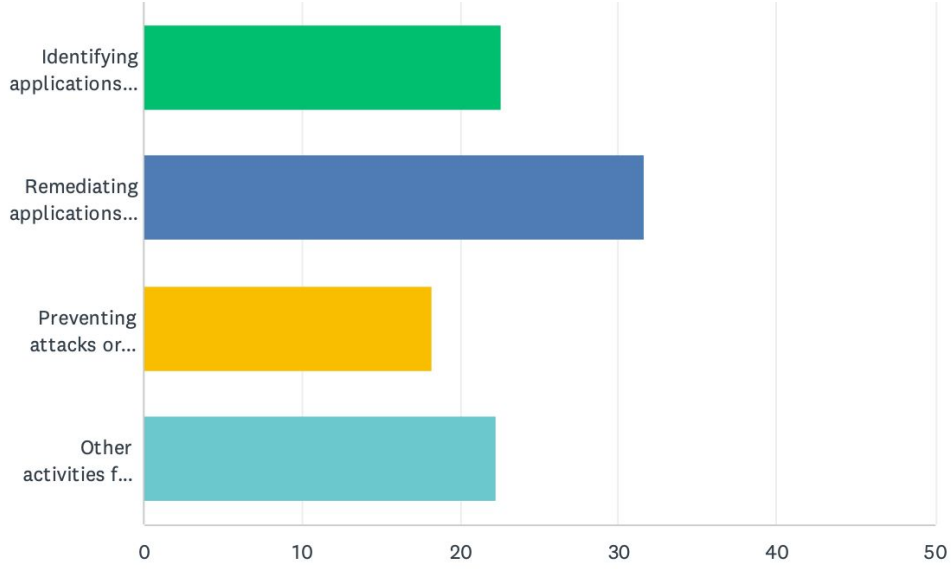
anchore

# What is a Software Bill of Materials?

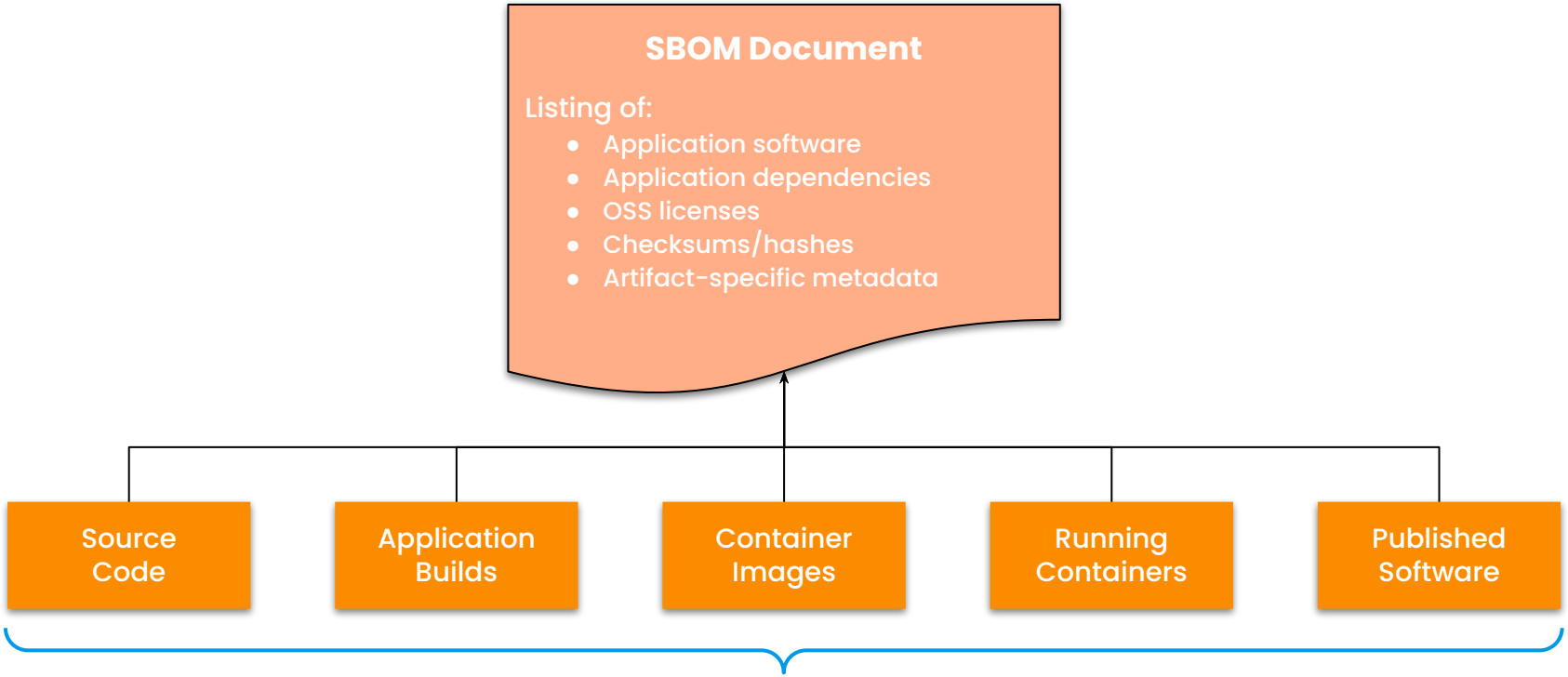
# What is an SBOM?


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

Answered: 195 Skipped: 15



# What is an SBOM?




Types of artifacts from which SBOMs can be generated

# If We Knew What We are Consuming

- People spent insane amounts of time just finding log4j, because nobody knew where (or even if) it was hiding
- Knowing = Faster Remediation
- SBOMs help, a LOT, but…
  - They aren't a silver bullet
  - Scanners aren't perfect (e.g. can't penetrate binary blobs, cf. OpenSSL3.)
  - Not all SBOMs are equal
  - SBOMs aren't ubiquitous (yet) (producers aren't reliably supplying them)
  - SBOMs are more accurate and useful when producers/maintainers generate them BUT something is better than nothing
  - SBOM management is hard
  - Any SBOM generated before an actual build is suspect (transitive deps)
  - SBOM Everywhere: https://github.com/ossf/sbom-everywhere
  - I don't know what the end game is but generating them is better than nothing, figure out the details later

# SBOM Takeaways

00 SBOMs enable continuous, automated security/compliance checks, reduce time spent identifying and remediating issues

01 SBOMs improve a lot of things but do not solve every problem you have

02 Log4j is extremely easy to find, OpenSSL 3 is often obscured

03 SBOMs are more effective when created by maintainers rather than consumers, but something is better than nothing

anchore

# SBOM Reading List

Making Better SBOMs: https://kccncna2022.sched.com/event/182GT/ – https://www.youtube.com/watch?v=earq775L4fc

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

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

GitHub Self-Service SBOMs: https://github.blog/2023-03-28-introducing-self-service-sboms/

anchore

# The Future of Software Supply Chain Security

An Example Project Health Metric:

Number of Maintainers

**Paul Novarese** (He/Him) • You
Software Supply Chain Security at Anchore
1yr • 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

# CVE-2020-19909

On August 25 2023, we got an email to the curl-library mailing list from Samuel Henrique that informed us that "someone" had recently created a CVE, a security vulnerability identification number and report really, for a curl problem.

```
I wanted to let you know that there's a recent
curl CVE published and it doesn't look like it
was acknowledged by the curl authors since it's
not mentioned in the curl website: CVE-2020-19909
```

We can't tell who filed it. We just know that it is now there.

# September 4, 2023 – September 11, 2023

Period: 1 week

## Overview

**20** Active pull requests

**13** Active issues

| 16 | 4 | 6 | 7 |
|---|---|---|---|
| Merged pull requests | Open pull requests | Closed issues | New issues |

Excluding merges, **9 authors** have pushed **16 commits** to main and **21 commits** to all branches. On main, **20 files** have changed and there have been **240 additions** and **124 deletions**.


**1** Release published by **1** person

**v0.90.0**
published 3 hours ago

**16** Pull requests merged by **7** people

**fix the help output of power-user**
#2113 merged 8 hours ago

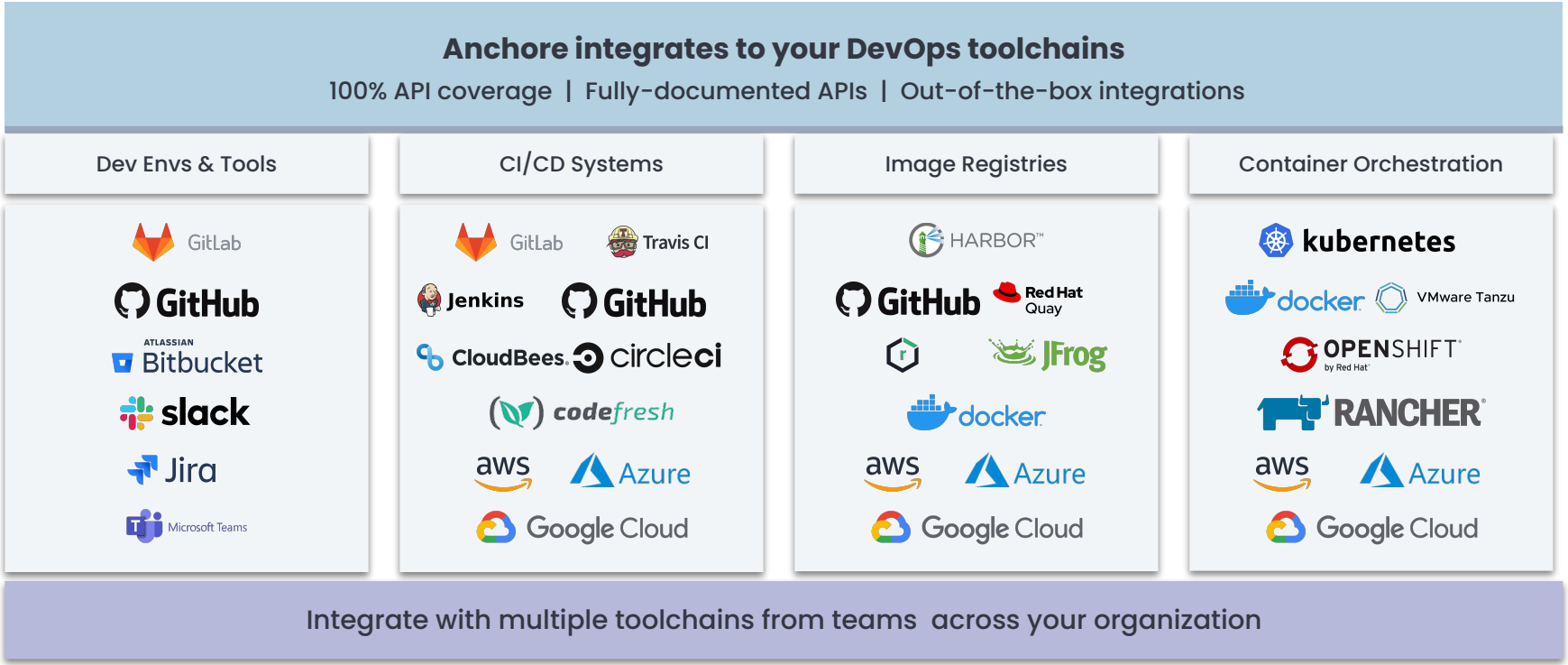
# OK, If Not CVSS, Then What?

- GHSAs (more transparent than CVEs)
- CISA KEV, EPSS, VEX &c
- GitHub Insights and other project health metrics
  - This is (currently) a very manual process
  - But it's getting a lot easier
  - Project health isn't **directly** about safety
  - What happens when it hits the fan?

anchore

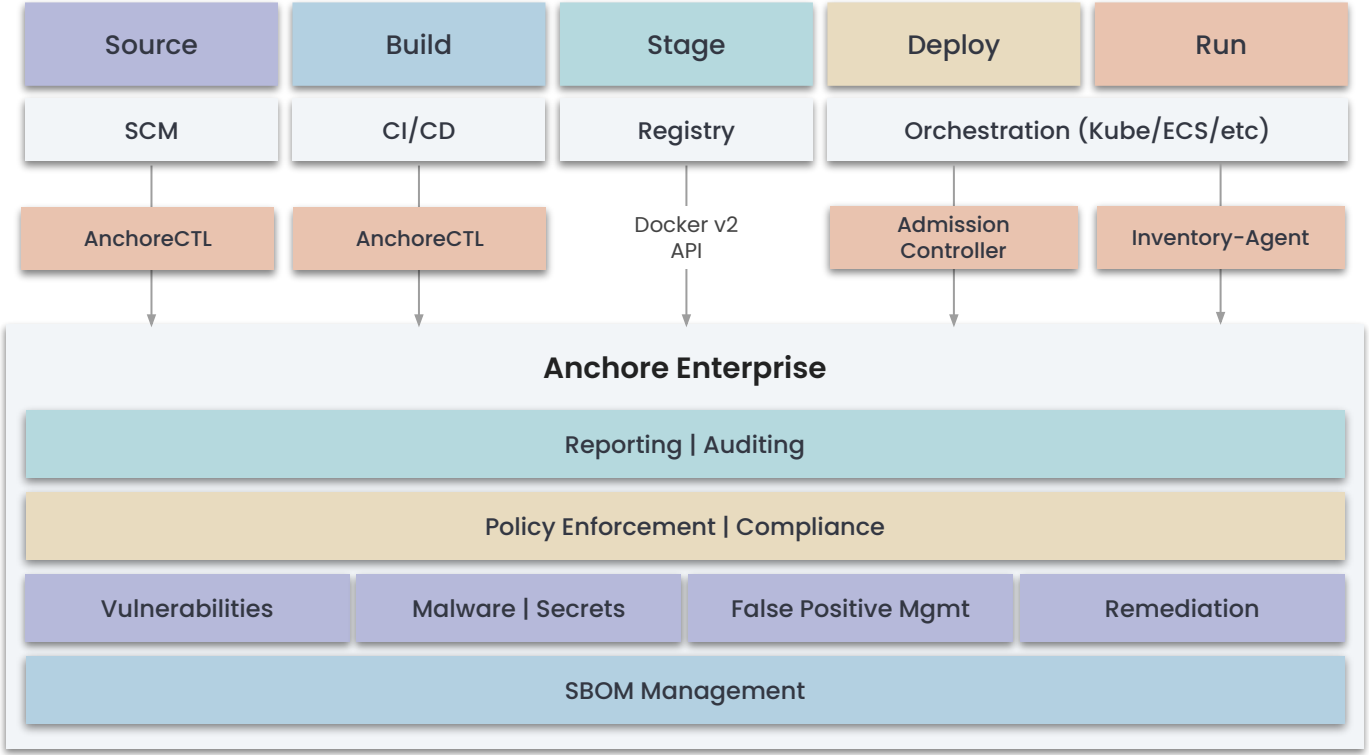
# Introducing Anchore

# Automation-Centric, 100% API Coverage




anchore

# Anchore Enterprise: How it Works

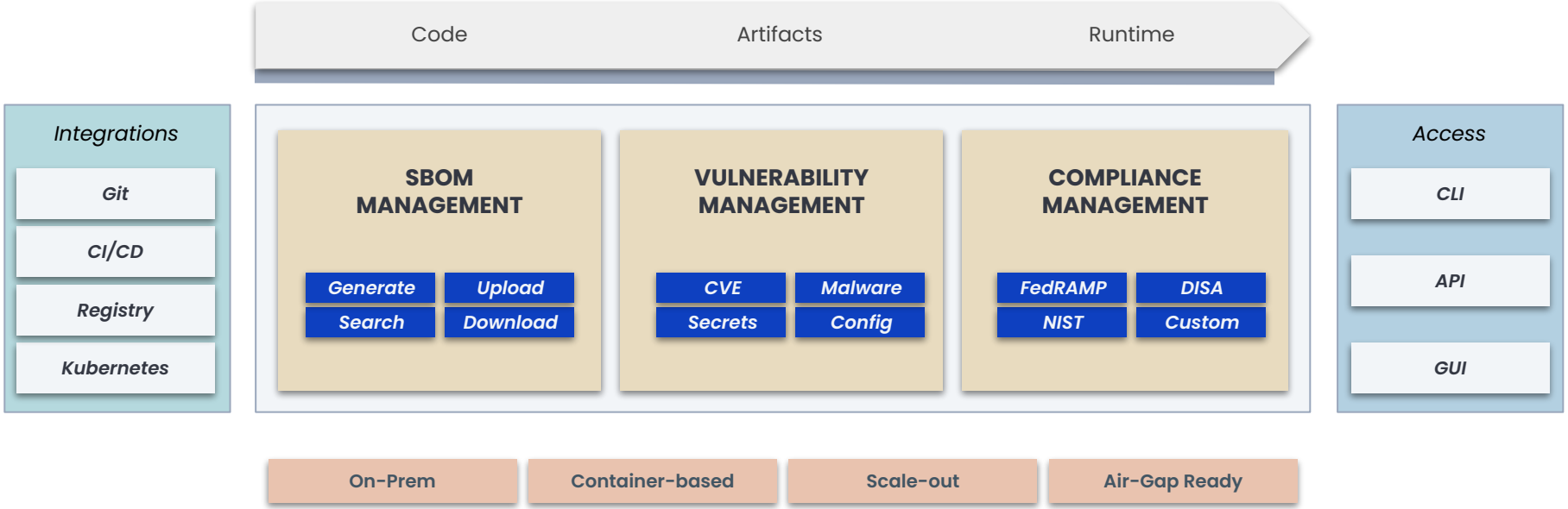



## Enterprise Capabilities

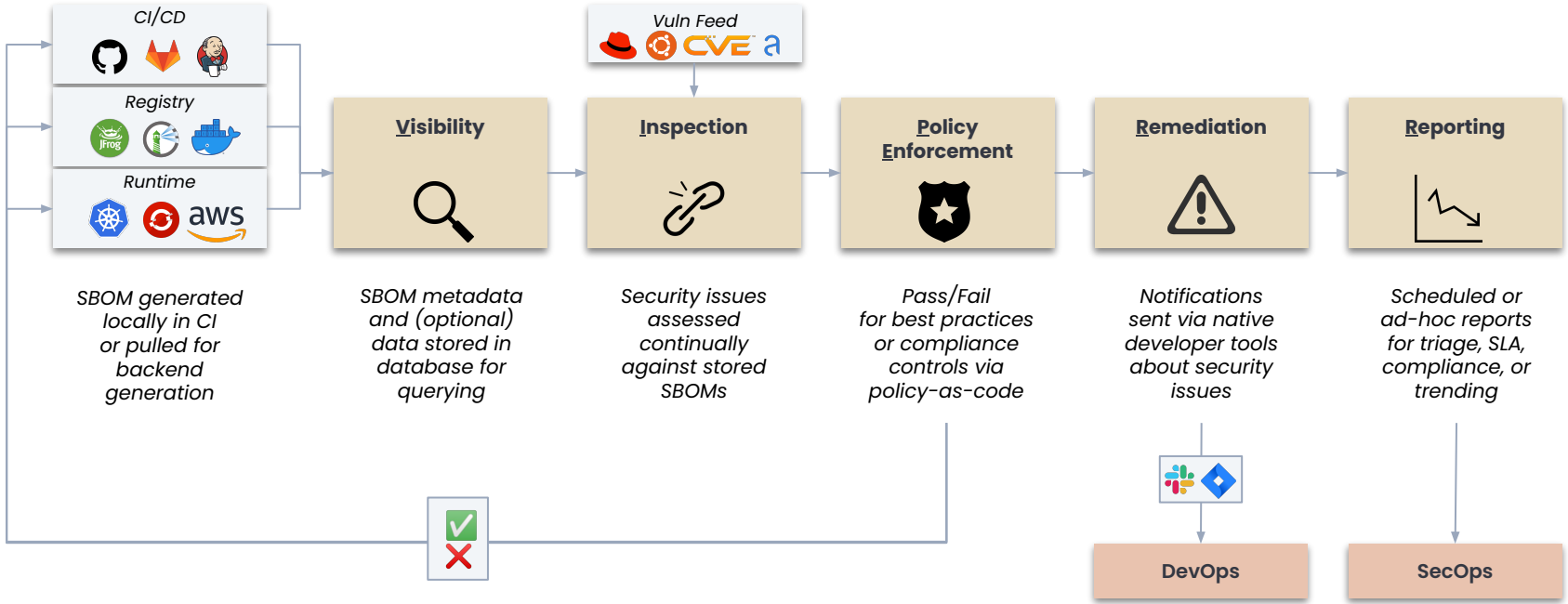
- Linux **and Windows** containers
- **Malware & secrets** scanning in addition to vulnerabilities
- **Fully-supported** integrations with CI/CD tools
- **Continuous scanning** from develop to runtime
- **Persist SBOMs and security results** across apps and teams
- **Enhanced** vulnerability feed
- **Centralized policy** enforcement with pre-built policy packs
- API/GUI for **reporting and auditing**
- **Notifications**
- **Remediation** recommendations & workflows
- **Enterprise control** with support for RBAC, SSO, LDAP
- **SLA Technical Support**

anchore

# Anchore Enterprise: Feature Overview

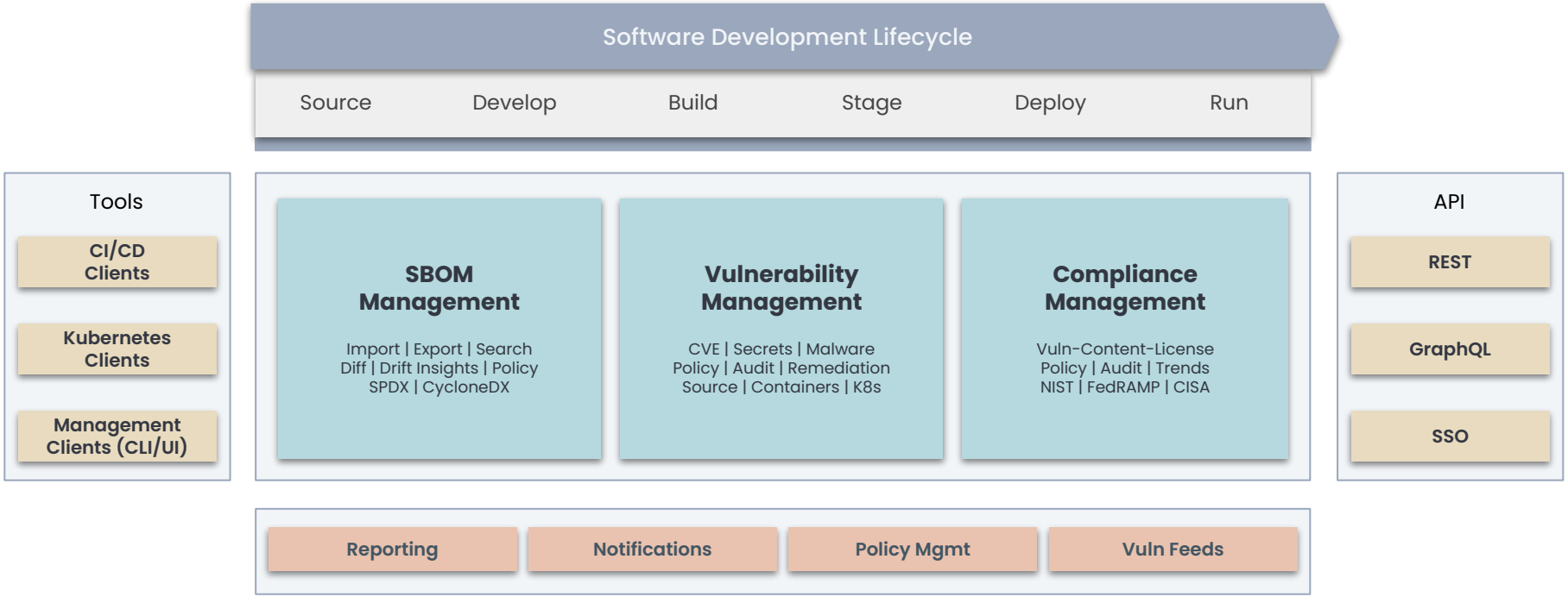


# Anchore Enterprise: Architecture

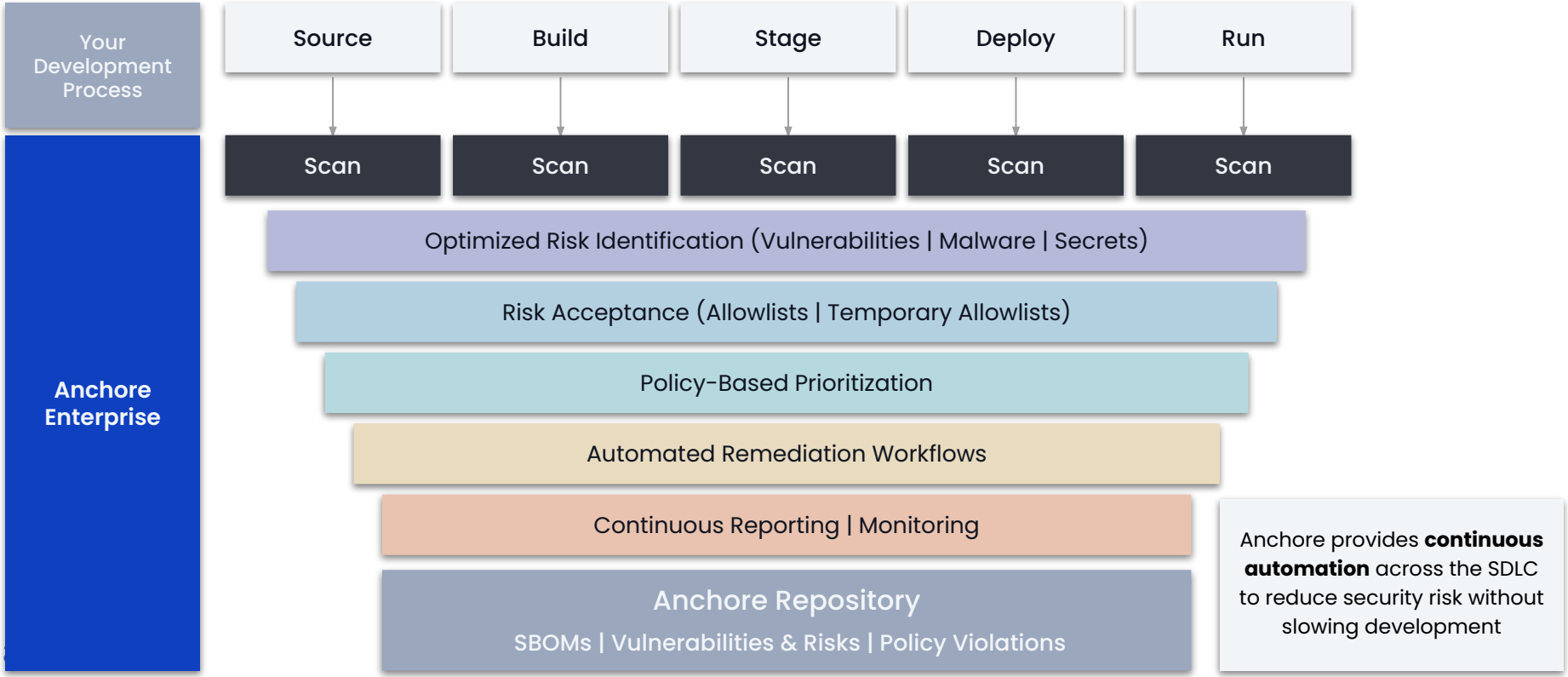



anchore

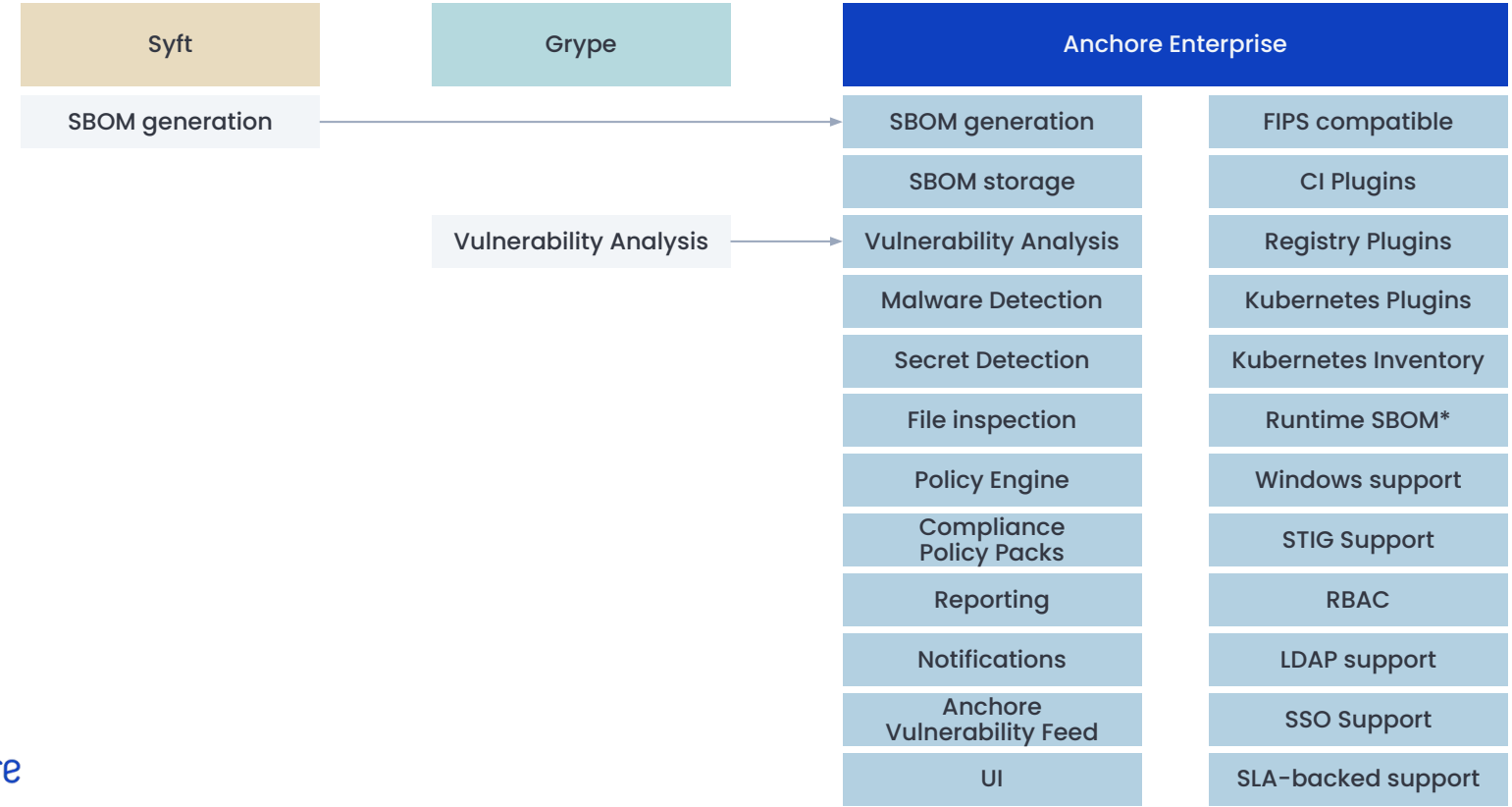
# Product Overview



# Vulnerability Management in the SDLC



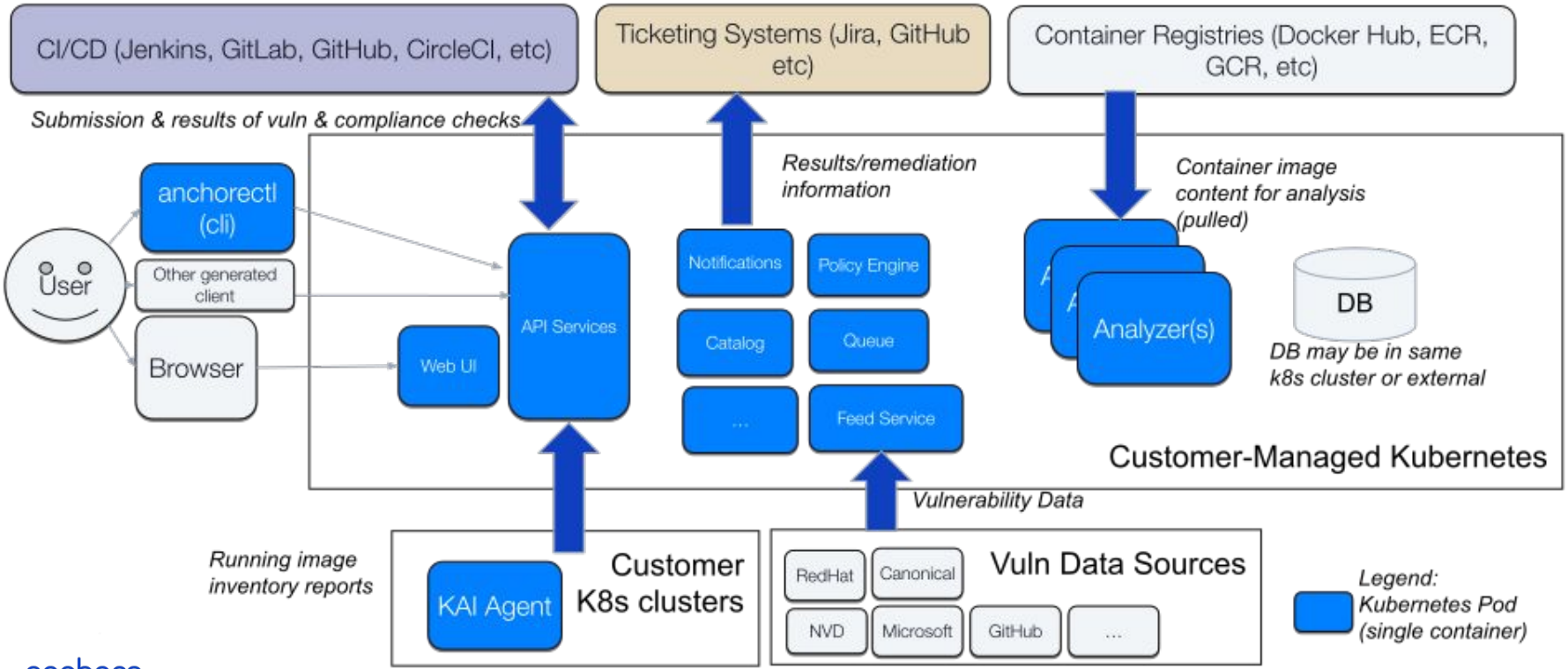
# OSS vs Enterprise by feature




anchore

** Q2 2023*

# Architectural Context




anchore

anchore

# Thanks!

anchore.com

info@anchore.com

github.com/anchore

@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:
https://anchore.com/slack/

These slides and lab examples archived here:
https://github.com/pvnovarese/2023-09-sbom-workshop