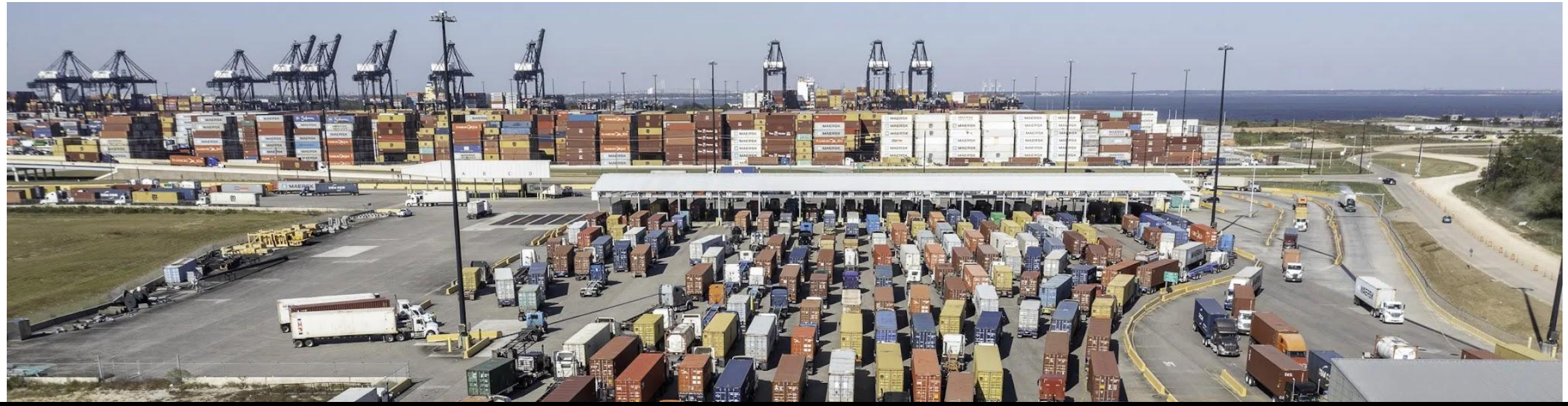
Pyrsia

Securing your OSS Supply Chain

@sudhindraRao

Pyrsia Team @JFrog

Dark state of Supply chain



NOT THIS

THIS

The Register®
Biting the hand that feeds IT

{* SECURITY *}

Missed patch caused Equifax data breach

Apache Struts was popped, but company had at least TWO MONTHS to fix it

Thu 14 Sep 2017 // 02:09 UTC

65 GOT TIPS?

Simon Sharwood BIO EMAIL TWITTER

SHARE

Equifax has revealed that the cause of its massive data breach was a flaw it should have patched weeks before it was attacked.

The company has updated its www.equifaxsecurity2017.com/ site with a new “A Progress Update for Consumers” that opens as follows:

> **Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.**

// MOST READ


Amazon spies on staff, fires them by text for not hitting secretive targets, workers 'feel forced to work through pain, injuries' – report

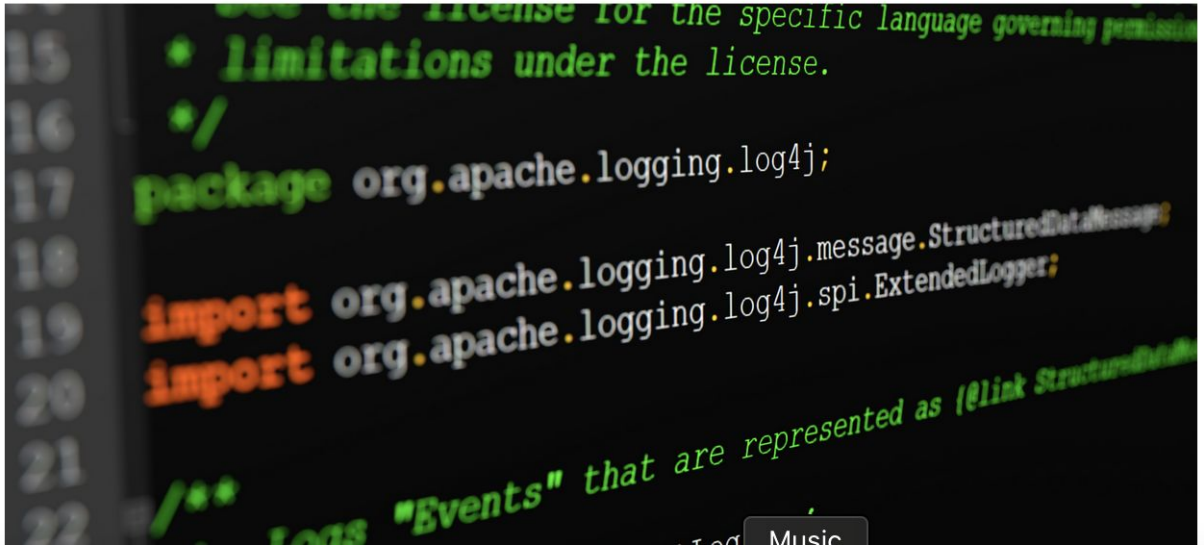

Happy birthday to the Nokia 3310: 20 years ago, it seemed like almost everyone owned this legendary mobile


Smash-and-grabbed: Chinese AI academic cuffed by Feds after 'binning hard drive' amid software leak probe

Log4Shell: Still out there, still dangerous, and how to protect your systems

by **Brandon Vigliarolo** in **Security**
on March 3, 2022, 11:12 AM PST

Barracuda researchers have noticed a steady stream of attacks attempting to exploit the Log4j vulnerability since it was found. What's interesting is where most attacks originate.



Security advisory: malicious crate rustdecimal

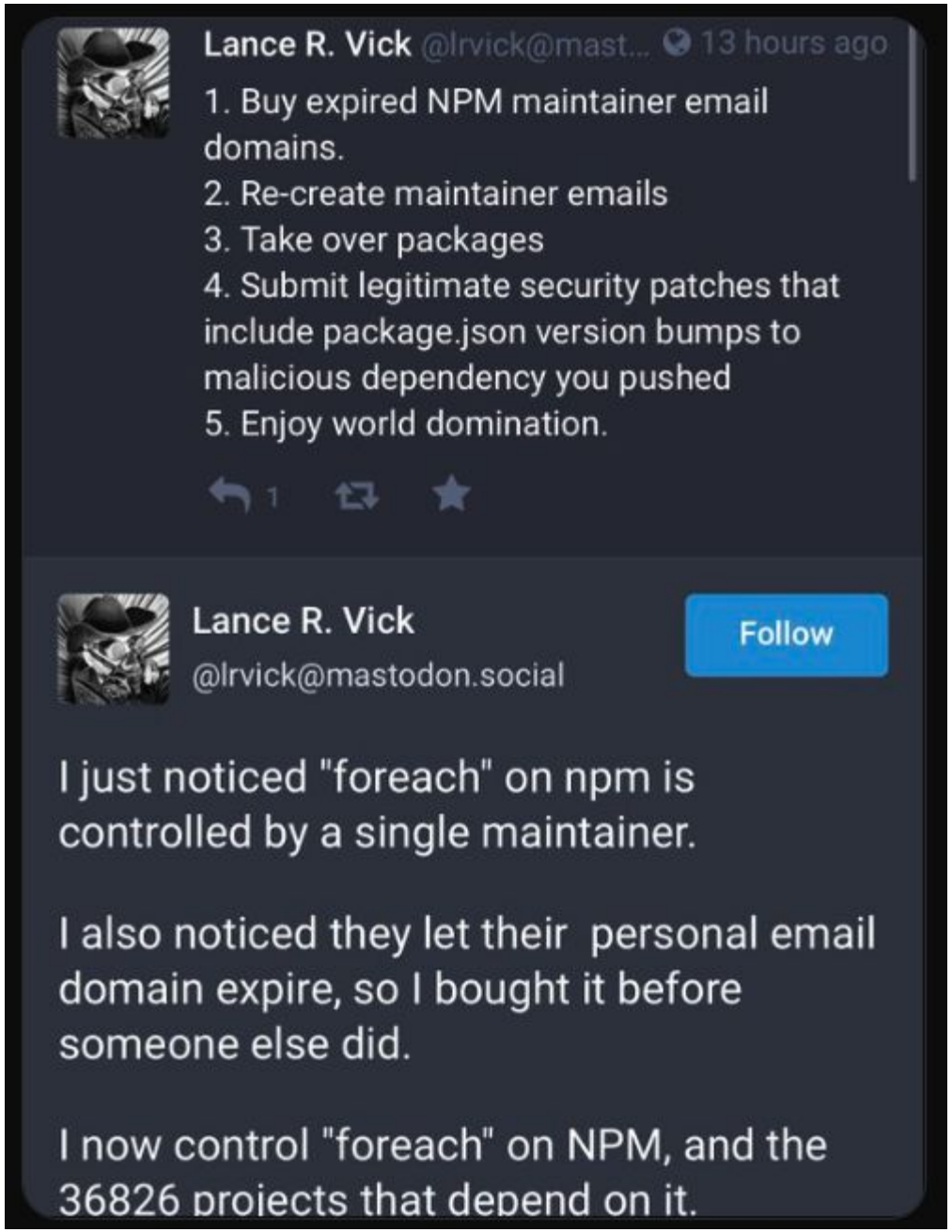
May 10, 2022 · The Rust Security Response WG

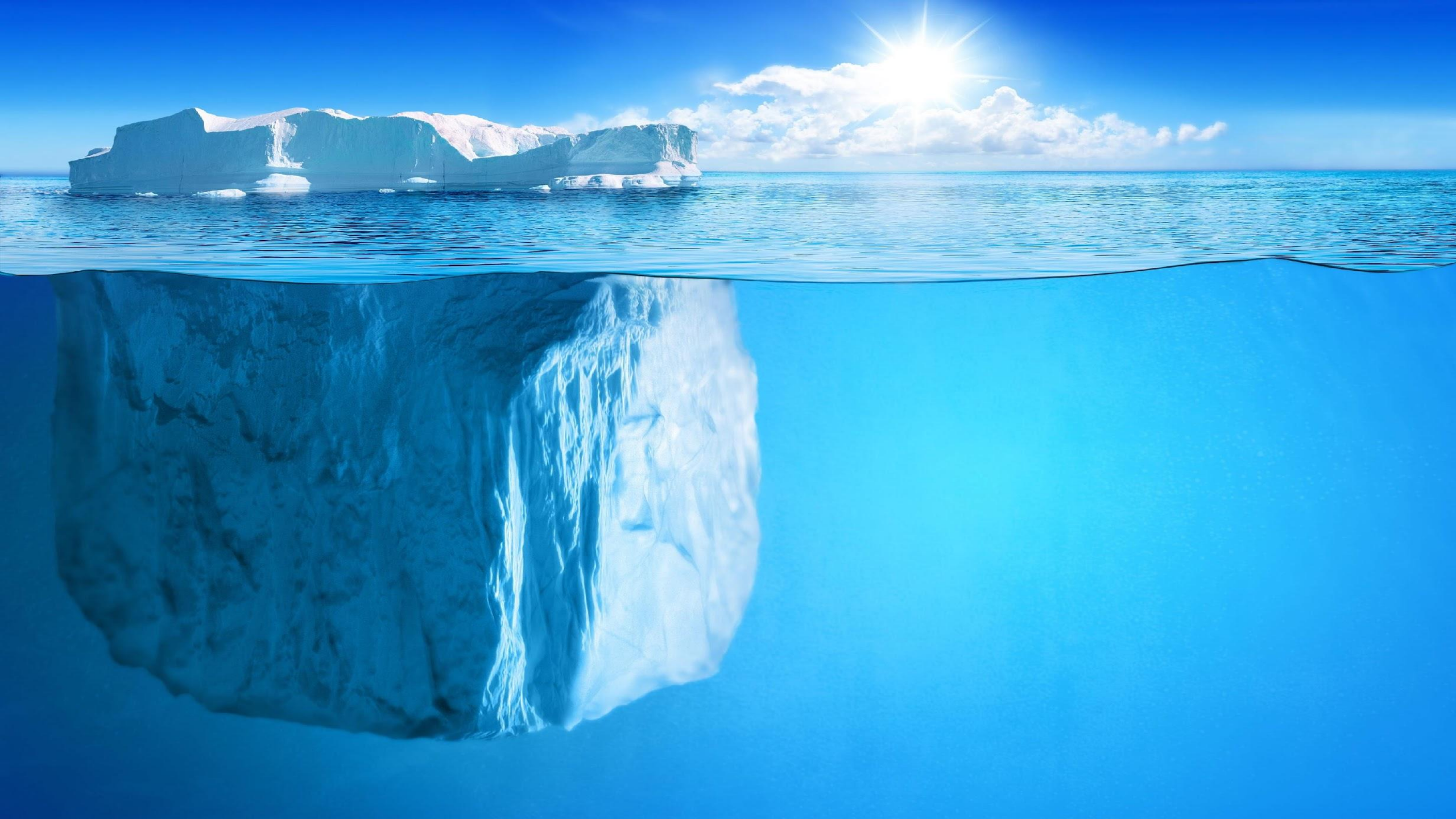
> *This is a cross-post of the official security advisory. The official advisory contains a signed version with our PGP key, as well.*

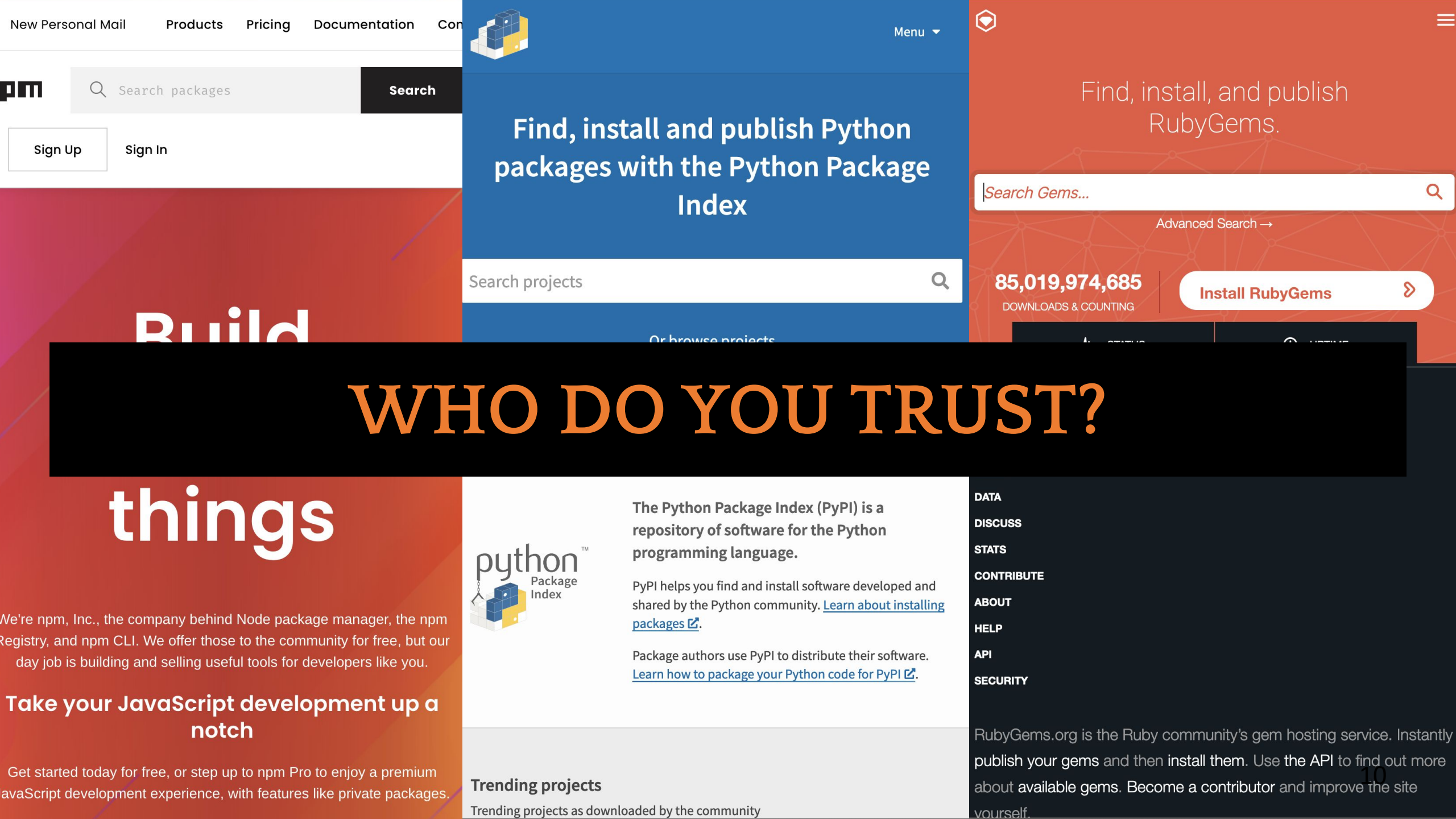
The Rust Security Response WG and the crates.io team were notified on 2022-05-02 of the existence of the malicious crate `rustdecimal`, which contained malware. The crate name was intentionally similar to the name of the popular `rust_decimal` crate, hoping that potential victims would misspell its name (an attack called "typosquatting").

To protect the security of the ecosystem, the crates.io team permanently removed the crate from the registry as soon as it was made aware of the malware. An analysis of all the crates on crates.io was also performed, and no other crate with similar code patterns was found.

Keep in mind that the `rust_decimal` crate was **not** compromised, and it is still safe to use.






New Personal Mail
Products
Pricing
Documentation
Search packages
Search
Sign Up
Sign In
Menu
Find, install and publish Python packages with the Python Package Index
Search projects
Find, install, and publish RubyGems.
Search Gems...
Advanced Search →
85,019,974,685
DOWNLOADS & COUNTING
Install RubyGems
WHO DO YOU TRUST?
Build
things
We're npm, Inc., the company behind Node package manager, the npm Registry, and npm CLI. We offer those to the community for free, but our day job is building and selling useful tools for developers like you.
Take your JavaScript development up a notch
Get started today for free, or step up to npm Pro to enjoy a premium JavaScript development experience, with features like private packages.
python Package Index
The Python Package Index (PyPI) is a repository of software for the Python programming language.
PyPI helps you find and install software developed and shared by the Python community. Learn about installing packages.
Package authors use PyPI to distribute their software. Learn how to package your Python code for PyPI.
Trending projects
Trending projects as downloaded by the community
DATA
DISCUSS
STATS
CONTRIBUTE
ABOUT
HELP
API
SECURITY
RubyGems.org is the Ruby community's gem hosting service. Instantly publish your gems and then install them. Use the API to find out more about available gems. Become a contributor and improve the site yourself.


Every time you pip install, go get, or mvn fetch something, you're doing the equivalent of plugging a thumb drive you found on the sidewalk into your production server.
--Dan Lorenc

Best Practices for Software Bill of Materials (SBOM) Management

Properly managing a Software Bill of Materials, or SBOM, has always been a best practice from a security and compliance point of view. However, it gained special urgency in May 2021, when the White House issued an executive order that requires software vendors who work with the federal government to provide SBOMs for their products.

Whether your business sells to U.S. government agencies or not, now is a good time to make SBOM management a core part of your process for building and shipping software. This article defines what an SBOM is, explains why it's important and offers tips for SBOM management.

What is a Software Bill of Materials?

A Software Bill of Materials is a list of the components that form a piece of software, as well as relevant metadata (such as licensing information) about those components.

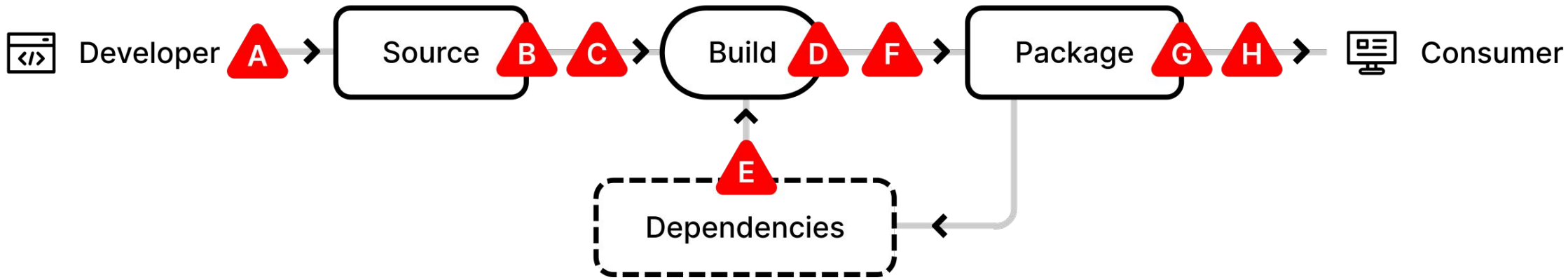
Common elements of an SBOM include:

- Open source libraries that an application imports or depends on.
- Plugins, extensions or other add-ons that an application uses.
- Custom source code written in-house by developers.
- Information about the versions, licensing status and patch status of these components.

In addition, an SBOM for a SaaS application could include information about APIs or third-party services that are required

Supply-chain Levels for Software Artifacts

https://slsa.dev/



A Bypassed code review

B Compromised source control system

C Modified code after source control

D Compromised build platform

E Using a bad dependency

F Bypassed CI/CD

G Compromised package repo

H Using a bad package

For Liquid Software ...

We need a supply chain that is

Automated

Trustworthy

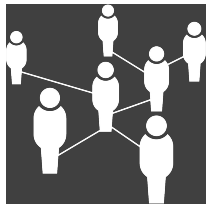
Dependable

Pyrsia - Key Features

- Consensus based build network
- Provenance Log
- Decentralized Package Registry

Pyrsia - Trusted Network

SECURE



RELIABLE

OPEN

TRUSTED

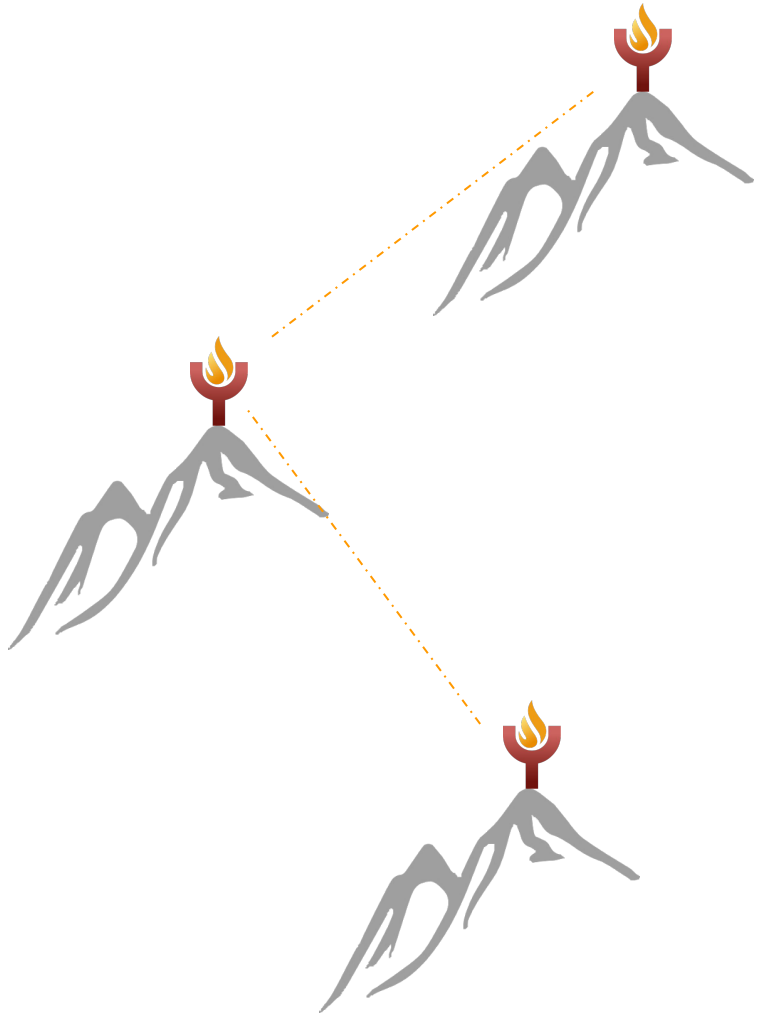
GREEK ORIGIN OF PYRSIA

https://www.greecehighdefinition.com/blog/communication-in-ancient-greece-how-did-the-ancient-greeks-communicate

2 sets of 5 torches

	1	2	3	4	5
1	A	B	Γ	Δ	E
2	Z	H	Θ	I	K
3	Λ	M	N	Ξ	O
4	Π	P	Σ	T	Y
5	Φ	X	Ψ	Ω	

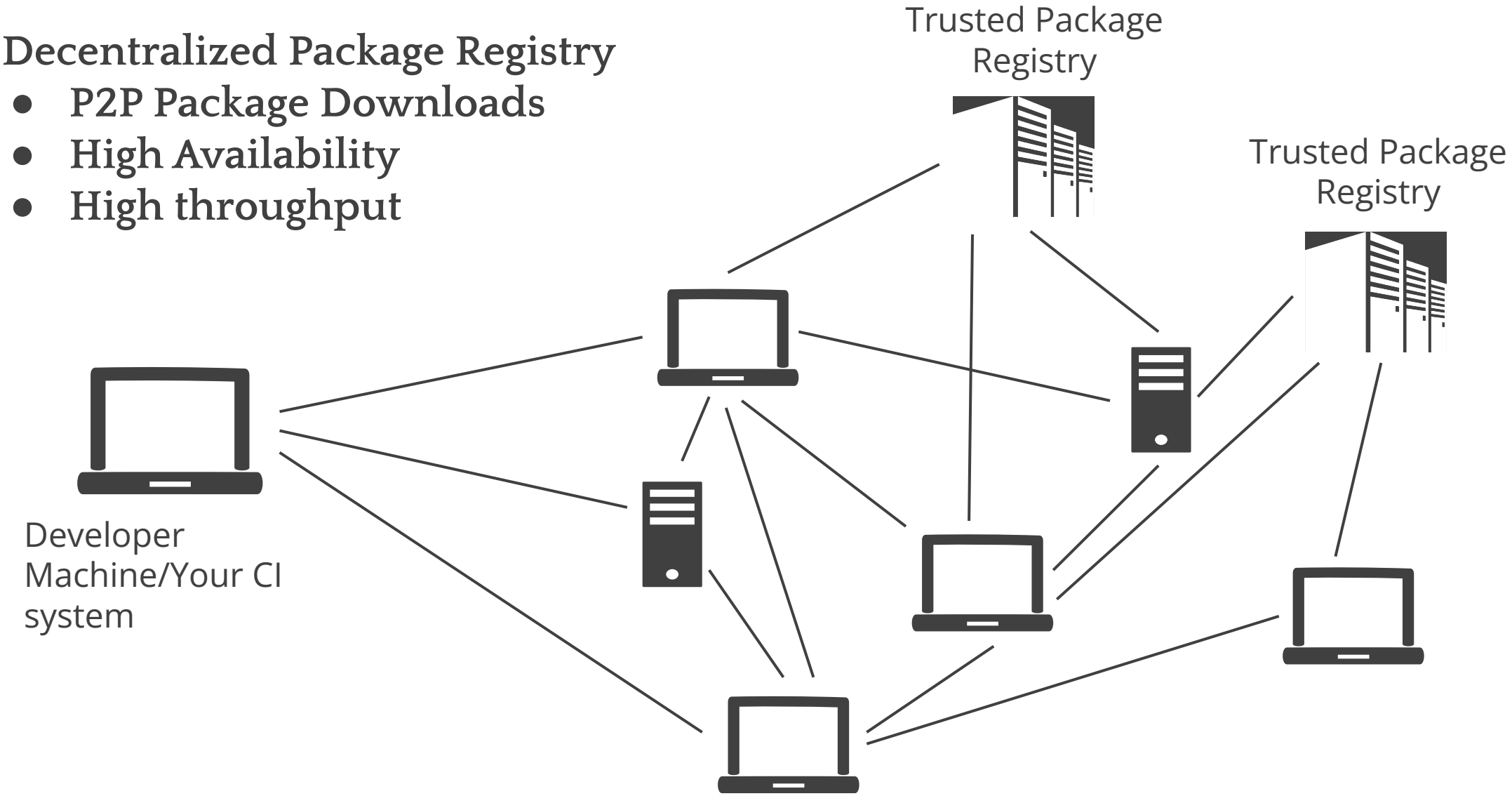
https://en.wikipedia.org/wiki/Polybius_square



Pyrsia Binary Distribution Network

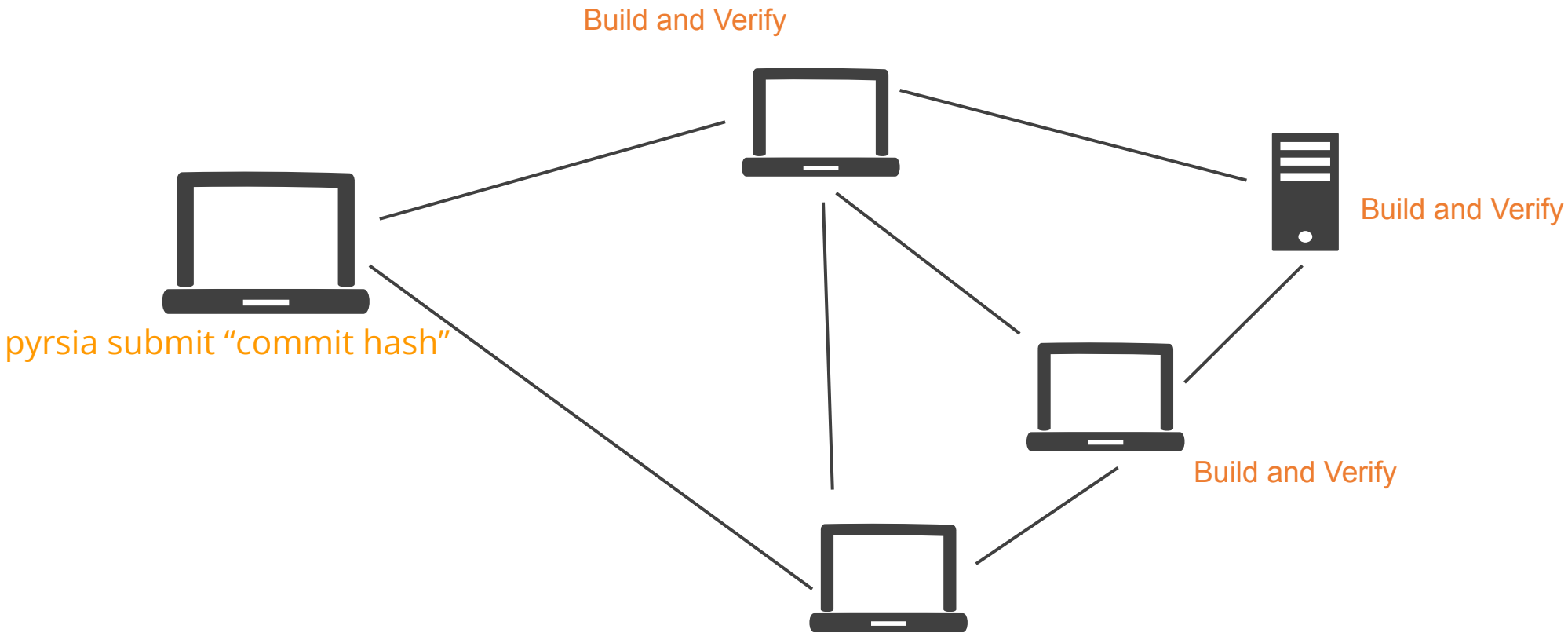
Decentralized Package Registry

- **P2P Package Downloads**
- **High Availability**
- **High throughput**



Pyrsia Consensus

- Consensus based build network



Pyrsia Provenance Log

Where did this binary come from?

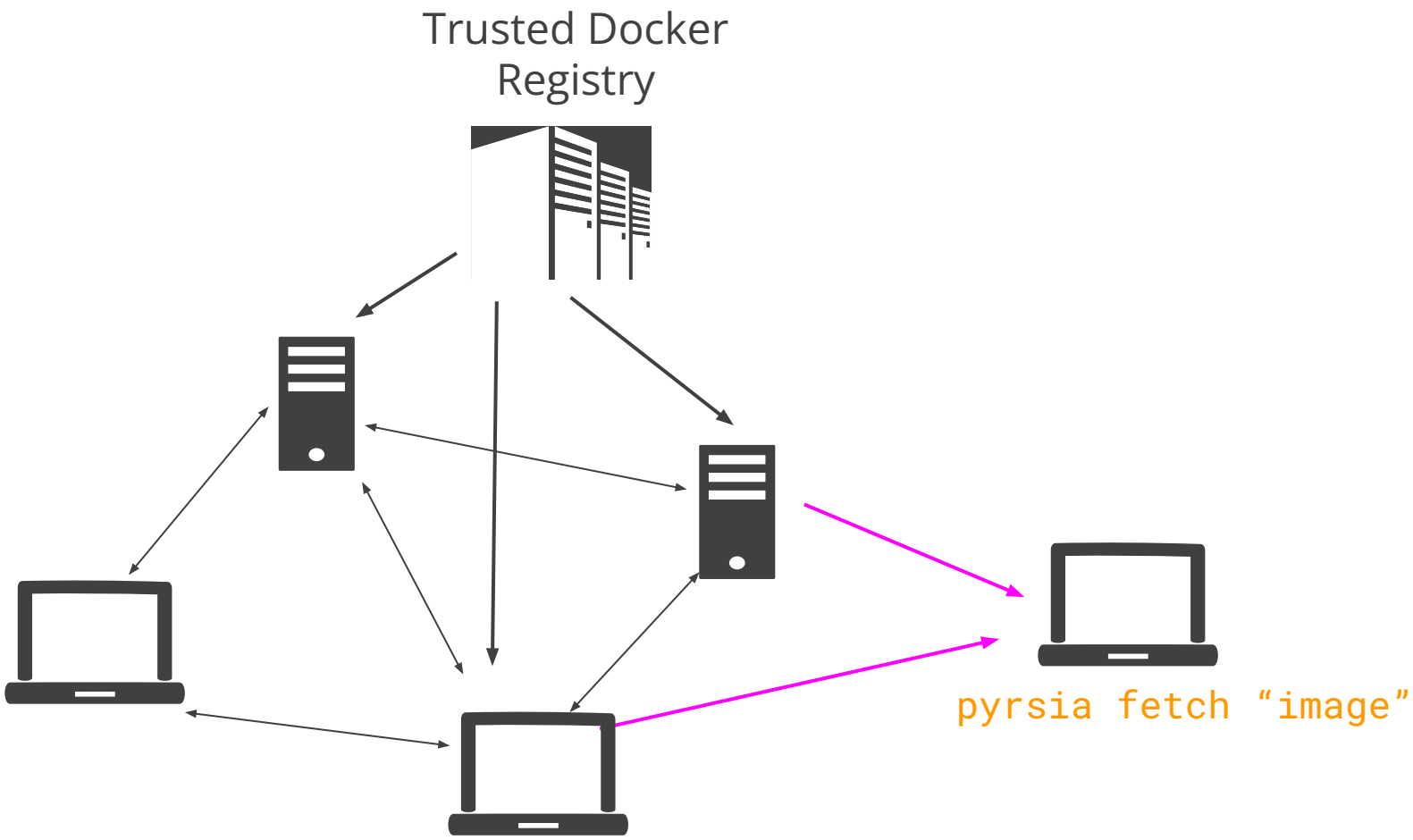
Who built this?

What happened after it was built? Any vulnerabilities?

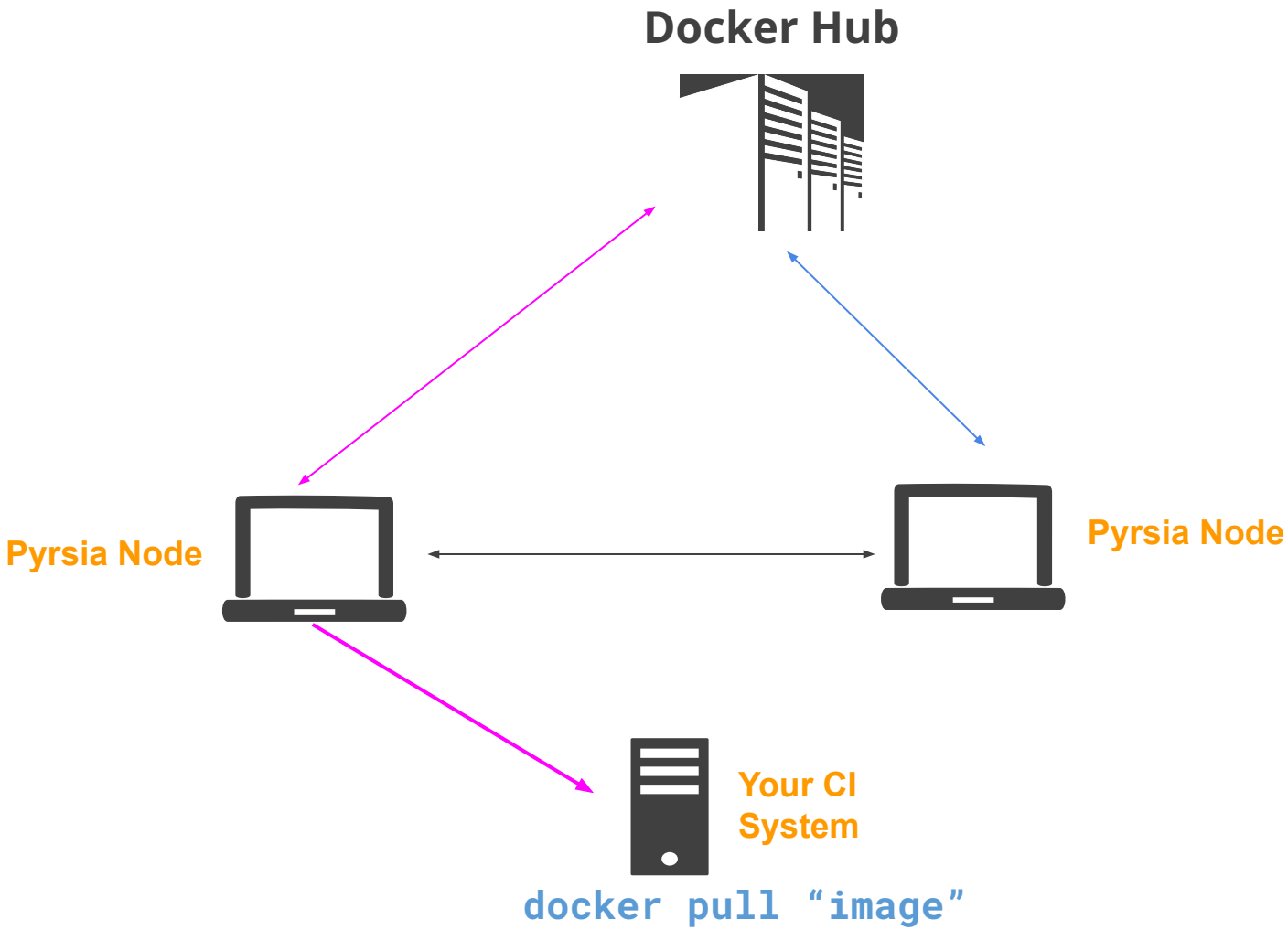
What can I add to SBOM about the binary and dependencies?

P R O V E N A N C E L O G ... ...

Pyrsia - Easy to Install and Use



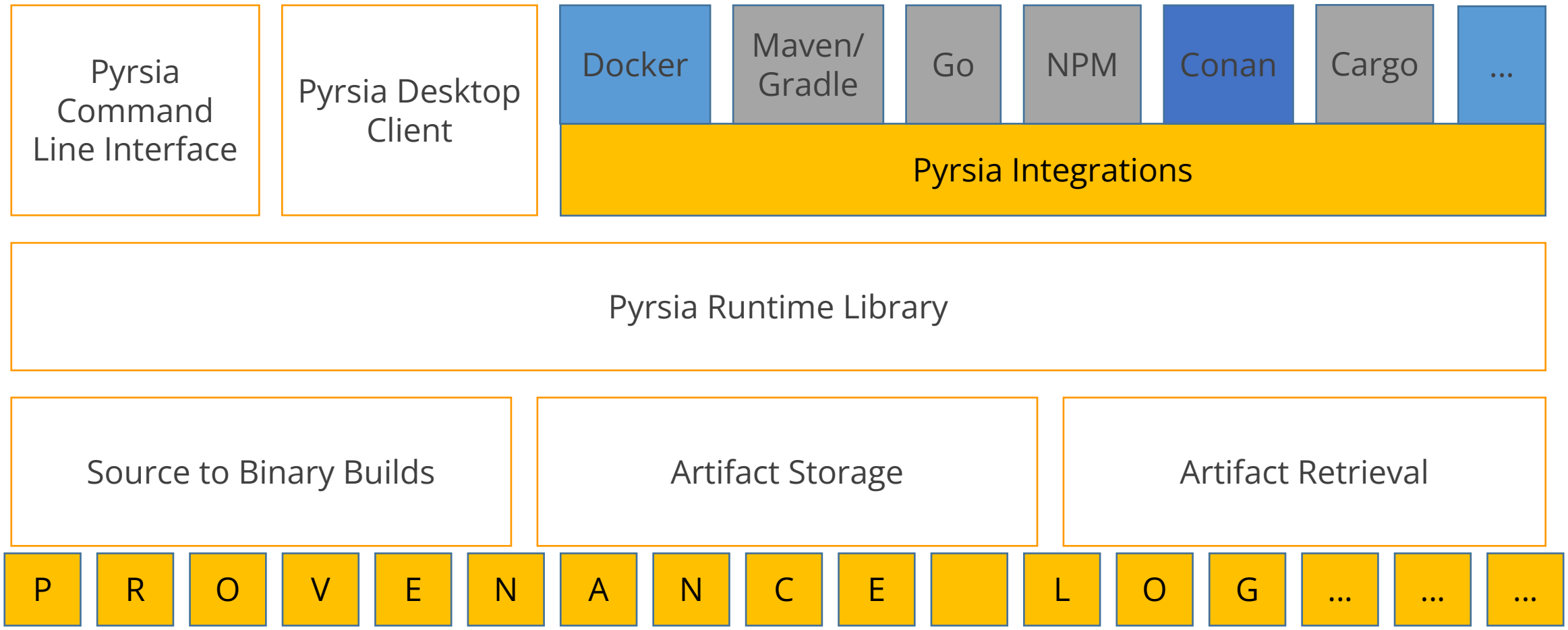
Pyrsia - Demo



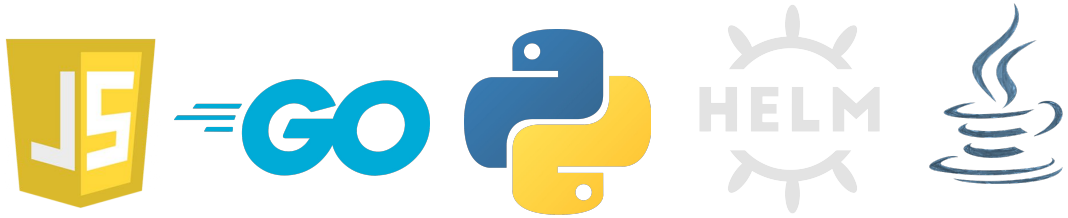
Demo

https://youtu.be/28T_sQDYhXE

Pyrsia Architecture



Pyrsia Security Model



- Reproducible Build Trust Model:
  - Network Consensus: A quorum of trusted registries and nodes agree on binary version
- Unreproducible Build Trust Model:
  - Trusted Registry: Built from source by a trusted registry

- Domain Verification (for domain prefixed releases):
  - Option 1: Source lives on domain (e.g. github repo or domain redirect)
  - Option 2: Private key domain challenge – verify against public key hosted on domain

Getting Started

Install: apt-get install pyrsia

Use:

- pyrsia -s (status of the node)
- pyrsia -l (list peers)

With CI system

- Configure docker desktop
- **You do not need to change your CI code/scripts**
- docker pull
- Docker images now will be delivered via Pyrsia

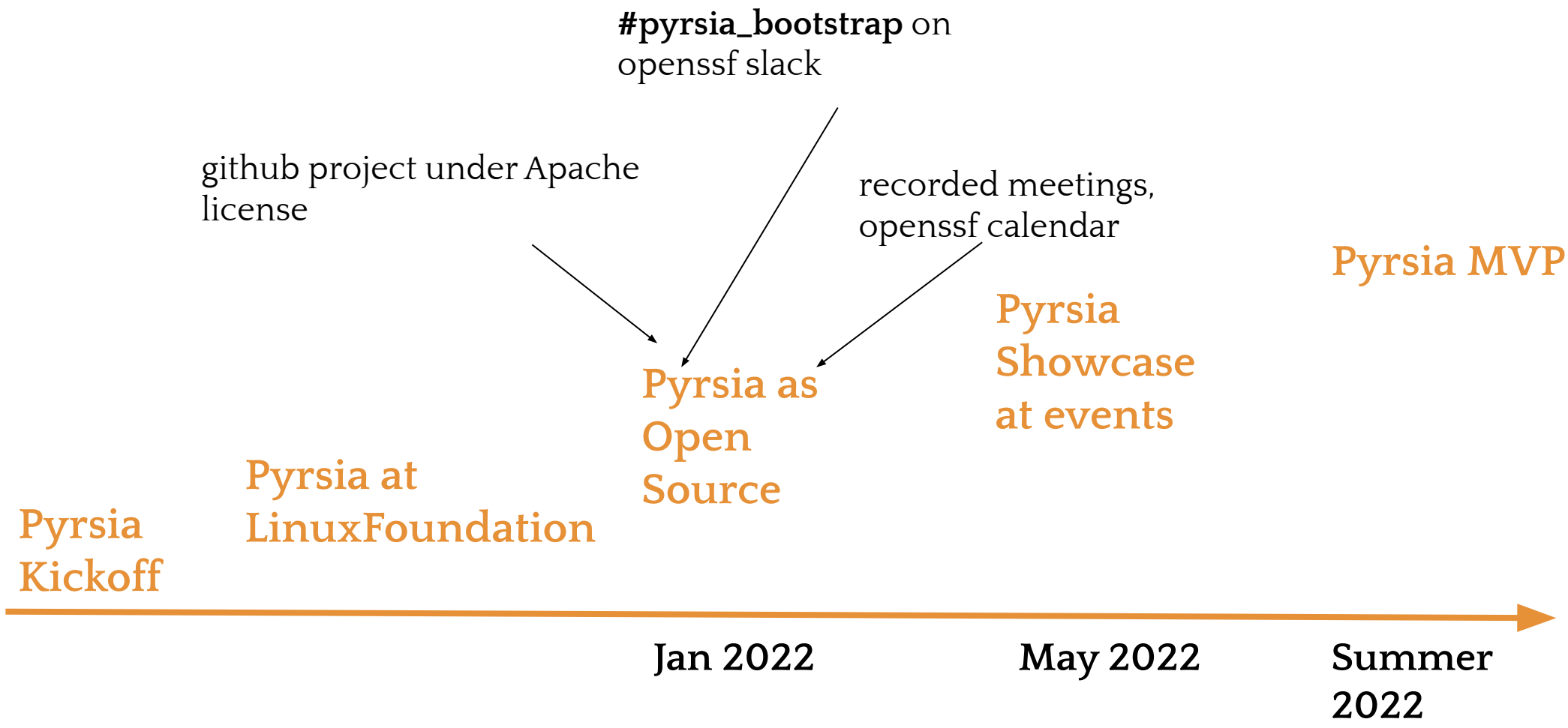
What's Inside?

- Rust lang for development - Support Multiple OSes
- Integration with Docker
- Automatic joining for peer nodes
  - libp2p (part of ipfs)
- Blockchain implementation for provenance log
  - AlephBFT - for Blockchain implementation

What's Next?

- Provenance Log
  - Build your SBOM
  - Query elements in your SBOM
  - Make Security Decisions
- Streaming of Large binaries over the P2P network
- Building your binaries on Pyrsia network

Pyrsia Timeline



Pyrsia Collaboration

- Collaborating with OpenSource
  - libp2p rust implementation
  - AlephBFT rust implementation
- Engaged with SigStore and Notary V2 for future integration

Pyrsia is Open Source

- 25 public general meetings
- Public daily standups and periodic Sprint meetings
- Contributing organizations
  - JFrog, Docker, DeployHub
- 27 individual contributors
- 38 on #pyrsia_bootstrap slack channel
- 220 commits on github - actively releasing minor versions nightly

GET INVOLVED

- https://pyrsia.io
- Download and install - Give us feedback @PyrsiaOSS
- Use your CI systems with Pyrsia Nodes
- Join team meetings
- Listen to recordings and help us document
- Find good first issues
- Showcase Pyrsia to our customers

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CNBC TV

TECH

Ex-NSA hacker says a supply chain cyberattack is one of the things that keeps him up at night

PUBLISHED MON, OCT 25 2021•4:16 PM EDT

Rich Mendez
@RICHMENDEZCNBC

SHARE

KEY POINTS

- A former Marine who conducted cyber missions for the U.S. told CNBC on Monday that the threat of a cyberattack on the U.S. supply chain keeps him awake at night.
- David Kennedy, also the founder of cybersecurity companies TrustedSec and Binary Defense, said successful attacks may embolden adversarial nations.
- Kennedy's comments came after cybersecurity experts at Microsoft revealed that the Russian-linked hacker group behind the SolarWinds breach are still at it.

in is stressed from Covid. That makes it SHARE THIS –

ng supply chain is stressed t makes it ripe for hackers.

ecome significantly more reliant on robotic operations human labor, making them particularly easy to disrupt.

CNBC MARKETS BUSINESS INVESTING TECH POLITICS CN

ECH

Solarwinds hackers are targeti global IT supply chain, Microso

UBLISHED MON, OCT 25 2021•7:46 AM EDT

am Shead
SAM_L_SHEAD

SHARE

EY OINTS

- Nobelium, as the hacking group is known, has "been attempting replicate the approach it has used in past attacks by targeting organizations integral to the global IT supply chain" according t Burt, corporate vice president of customer security and trust at
- The hackers have been using phishing emails and a technique k as password spray, which involves trying commonly used passw such as Password1 or 1234 against multiple accounts before mo on to try a second password.
- Some 140 resellers and technology service providers have beer targeted by Nobelium so far, according to Microsoft, which said believes 14 have been compromised.

Supply Chain Needs to be Secured NOW!

THANK YOU!

https://pyrsia.io
@PyrsiaOSS

@sudhindraRao