State of open source security

Fridolin Pokorny <fridolin.pokorny@datadoghq.com>

DATADOG

$ whoami

DATADOG

~$ whoami

Fridolín "*fridex*" Pokorný

@fridex

- First open source contributions in ~2011
- Professionally in open source since 2013
- I like Linux/C/C++/Python, road cycling, psychology & philosophy
- I used to be a goal keeper, now keeper of few open-source projects on GitHub

@fridex

~$ whoami

Fridolín "*fridex*" Pokorný

@fridex

- First open source contributions in ~2011
- Professionally in open source since 2013 + *Golang*
- I like Linux/C/C++/Python, road cycling, psychology & philosophy
- I used to be a goal keeper, now keeper of few open-source projects on GitHub

@fridex

+ *keeping systems secure*

AI -> security

-> DATADOG

Lenovo -> Apple

DATADOG

Agenda

1. Why all this security stuff?
2. Selected open-source projects and initiatives
    a. OpenSSF
    b. TUF
    c. SLSA
    d. …
3. Securing your environments
4. Q&A

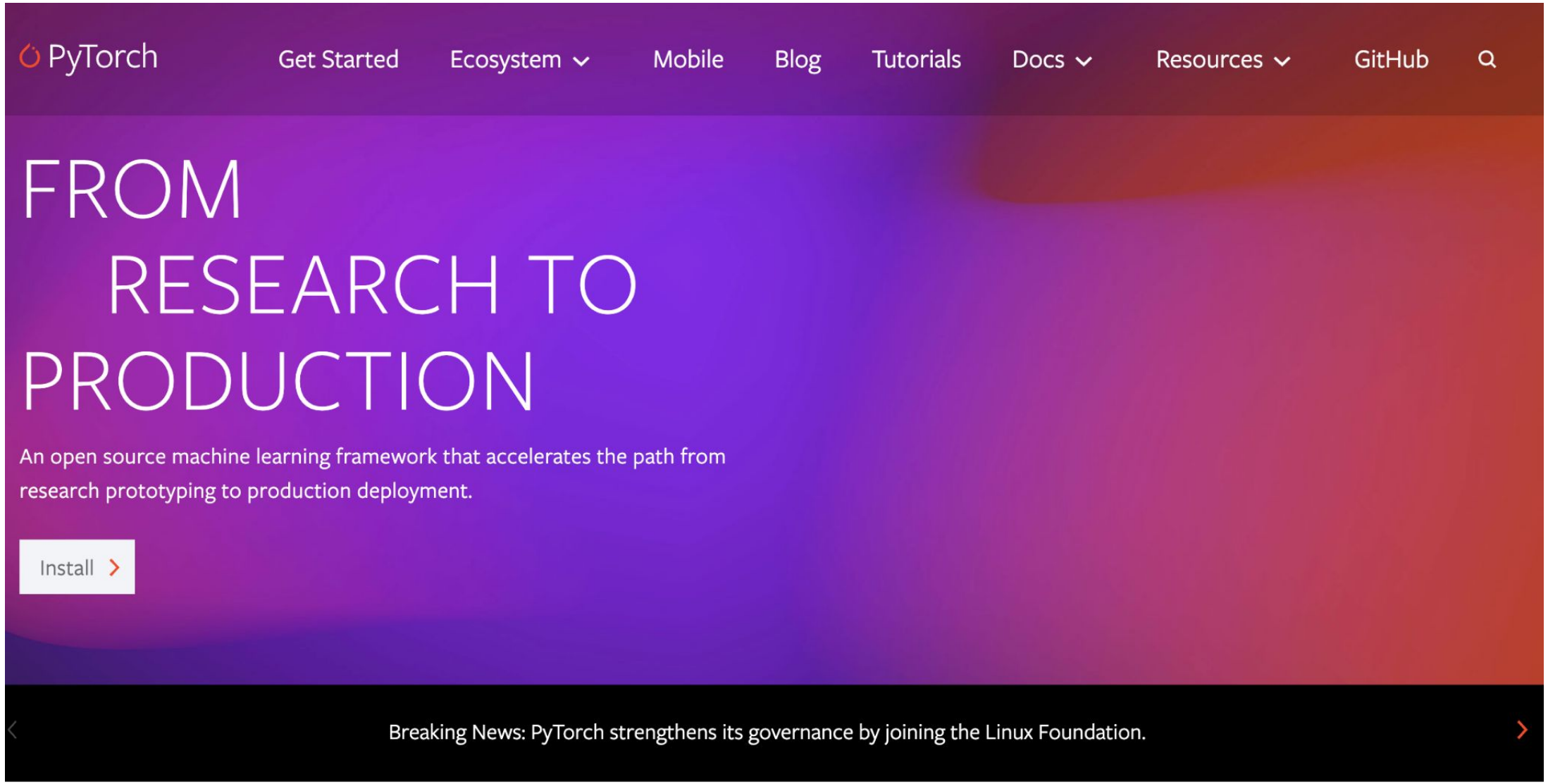
🔐 Why all this security stuff?

DATADOG

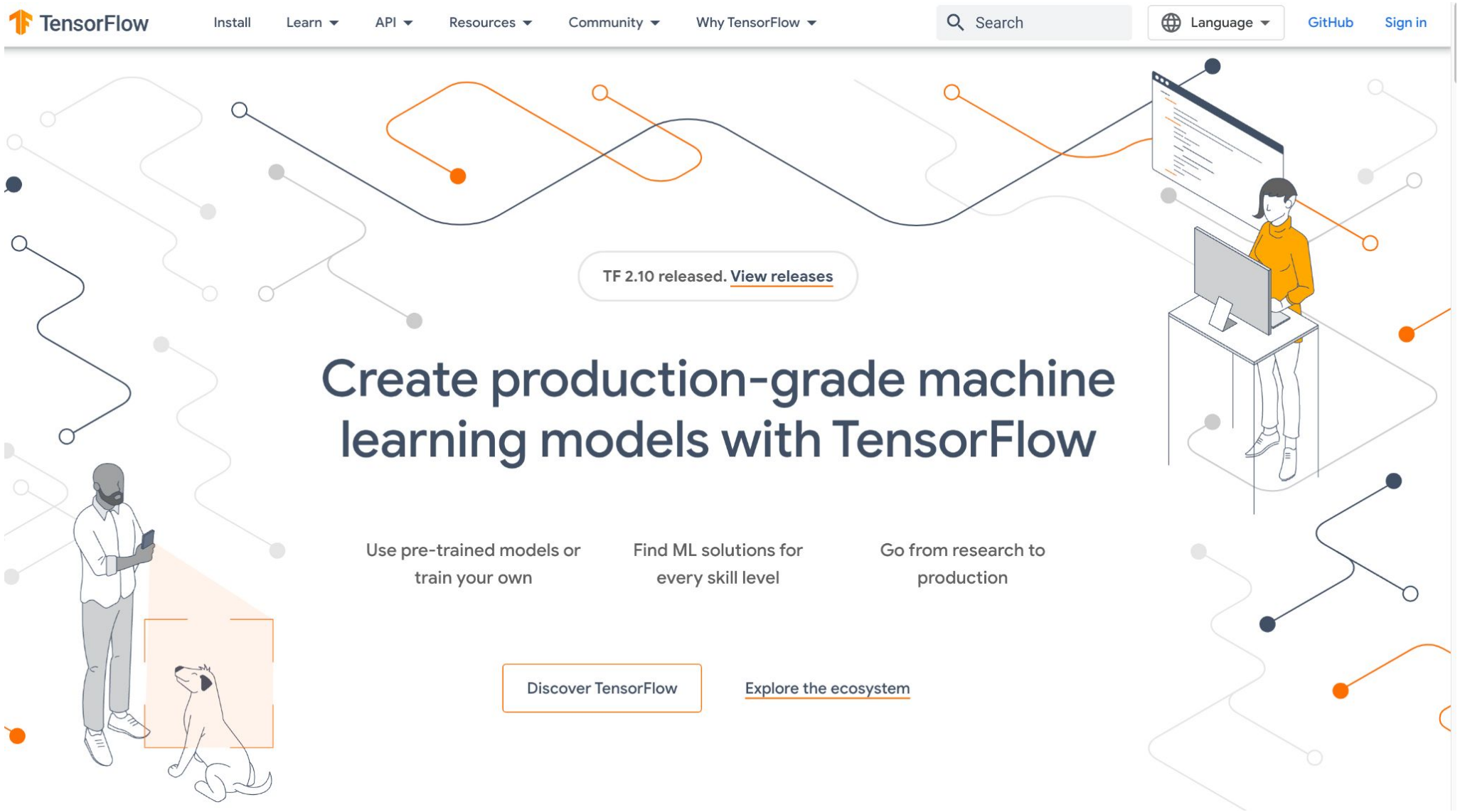
Why all this security stuff?

- Software is everywhere
- Securing our data
- Securing our privacy
- Securing our work
- …

Why all this security stuff?



Why all this security stuff?



Why all this security stuff?

kubernetes

Documentation Kubernetes Blog Training Partners Community Case Studies Versions English

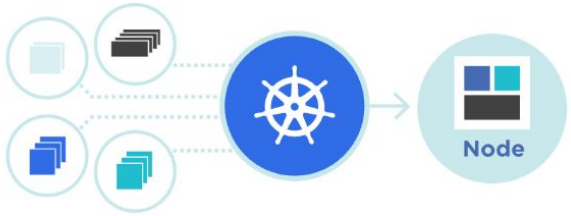
KubeCon + CloudNativeCon NA 2022 *Detroit, Michigan + Virtual.*

5 days of incredible opportunities to collaborate, learn + share with the entire community!
October 24 - 28, 2022.

KubeCon CloudNativeCon
North America 2022

Kubernetes, also known as K8s, is an open-source system for automating deployment, scaling, and management of containerized applications.

It groups containers that make up an application into logical units for easy management and discovery. Kubernetes builds upon 15 years of experience of running production workloads at Google, combined with best-of-breed ideas and practices from the community.



Planet Scale

Designed on the same principles that allow Google to run billions of containers a week, Kubernetes can scale without increasing your operations team.

Why all this security stuff?

- Example - ...

Why all this security stuff?

- Example - SolarWinds Orion Platform (Sunburst)
  - Supply chain breach
  - Injected malicious code
  - 30,000+ public and private organizations

Why all this security stuff?

Executive order by president Biden

THE WHITE HOUSE

MAY 12, 2021

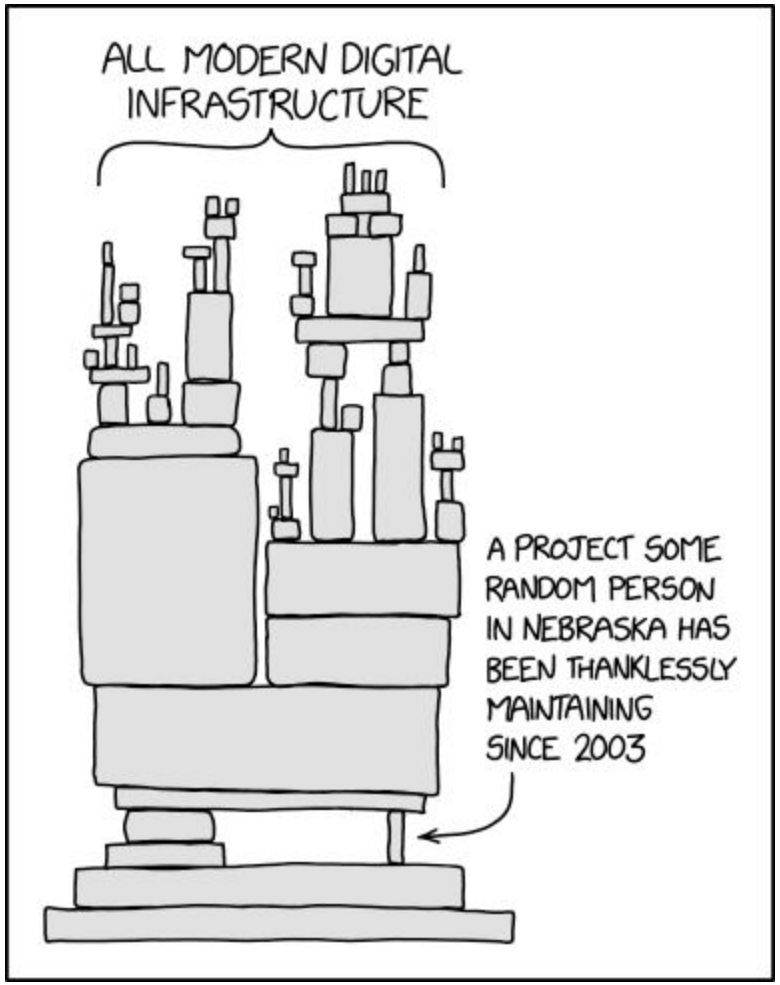
Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these

Is open source affected?

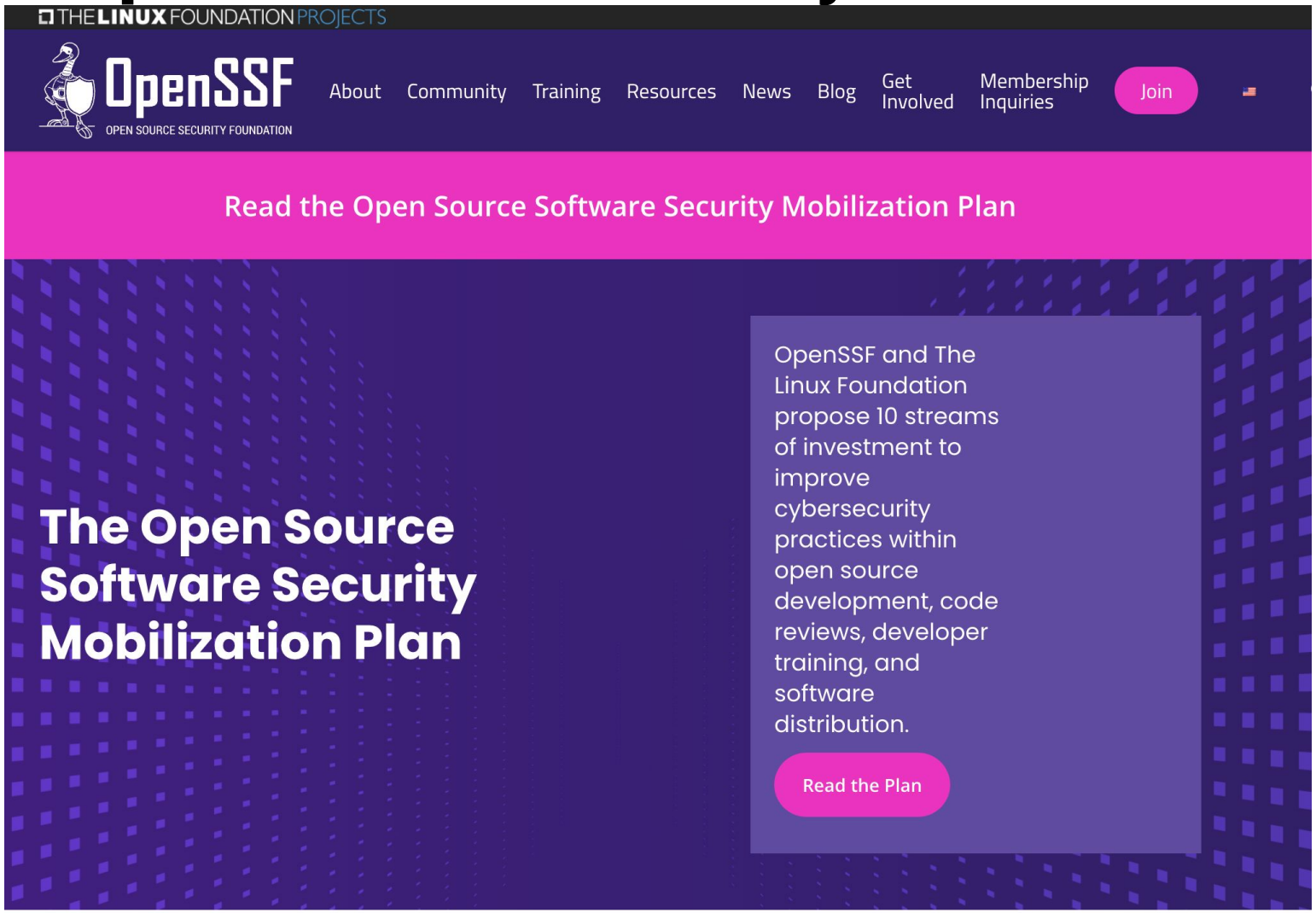


Source: xkcd#2347

🔐 Selected open-source projects and initiatives

DATADOG

OpenSSF - Open Source Security Foundation

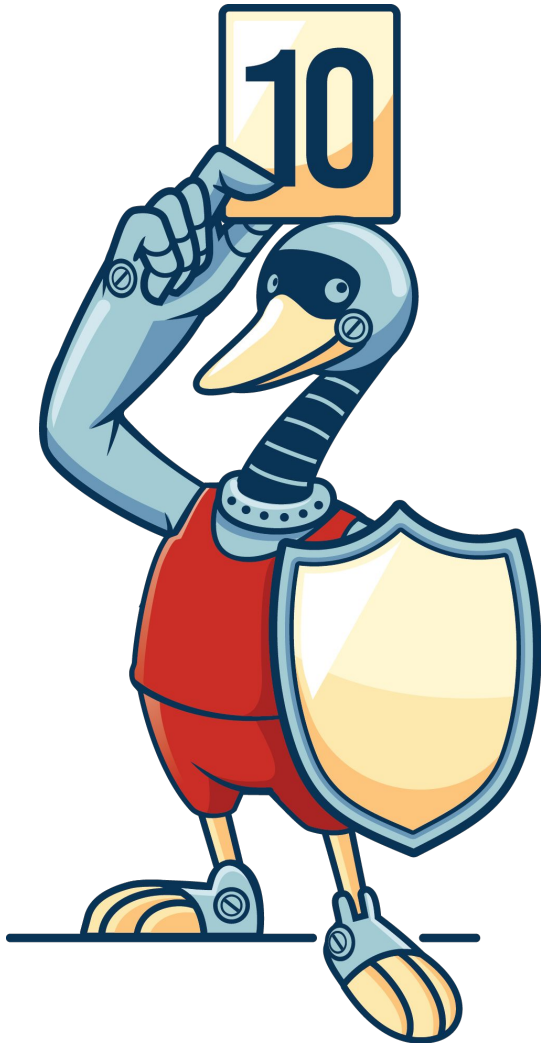


OpenSSF is committed to collaboration and working both upstream and with existing communities to advance open source security for all.

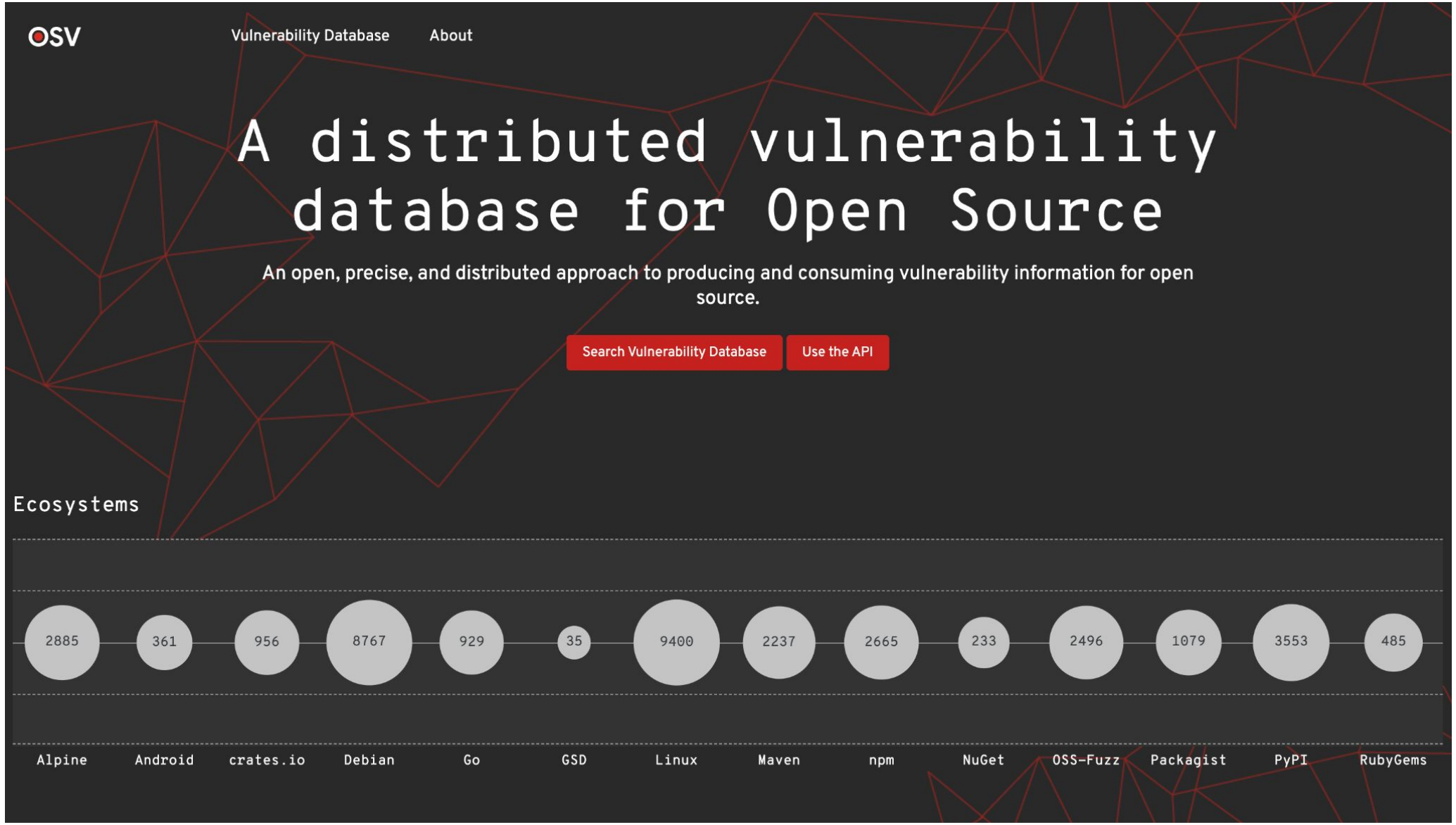
DATADOG

OpenSSF - Security Scorecards

- Security scorecards
  - Binary artifacts
  - Branch protection
  - CI tests
  - Dependency update tool
  - Pinned dependencies
  - Signed releases
  - Vulnerabilities
  - …



OSV database



DATADOG

OSV database

OSV

Vulnerability Database | About

Vulnerability Library

Package or ID search

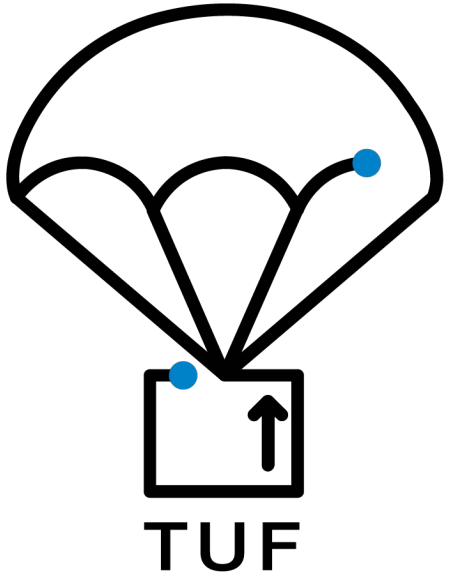
All ecosystems 36130 | Alpine 2885 | Android 361 | crates.io 957 | Debian 8769 | DWF 15 | GitHub Actions 5 | Go 929 | GSD 34 | Hex 19 | Linux 9400 | Maven 2238 | npm 2665 | NuGet 235 | OSS-Fuzz 2497 | Packagist 1079 | Pub 3 | PyPI 3554 | RubyGems 485 | UVI 0

ID	Packages	Summary	Affected versions		Last modified	Fix
DLA-3159-1	Debian:10/libbluray	libbluray - bugfix update	1:1.1.0-1		2 hours ago	Fix available
OSV-2022-525	OSS-Fuzz/spirv-tools	Heap-buffer-overflow in spvtools::CFA<spvtools::val::BasicBlock>::CalculateDominators	sdk-1.3.224.0 v2022.3 sdk-1.3.231.0	sdk-1.3.224.1 v2022.4	11 hours ago	No fix available
OSV-2022-51	OSS-Fuzz/c-blosc2	Negative-size-param in ndlz4_decompress	v2.0.0 v2.0.2 v2.0.4 v2.1.1	v2.0.1 v2.0.3 v2.1.0 ...	11 hours ago	No fix available

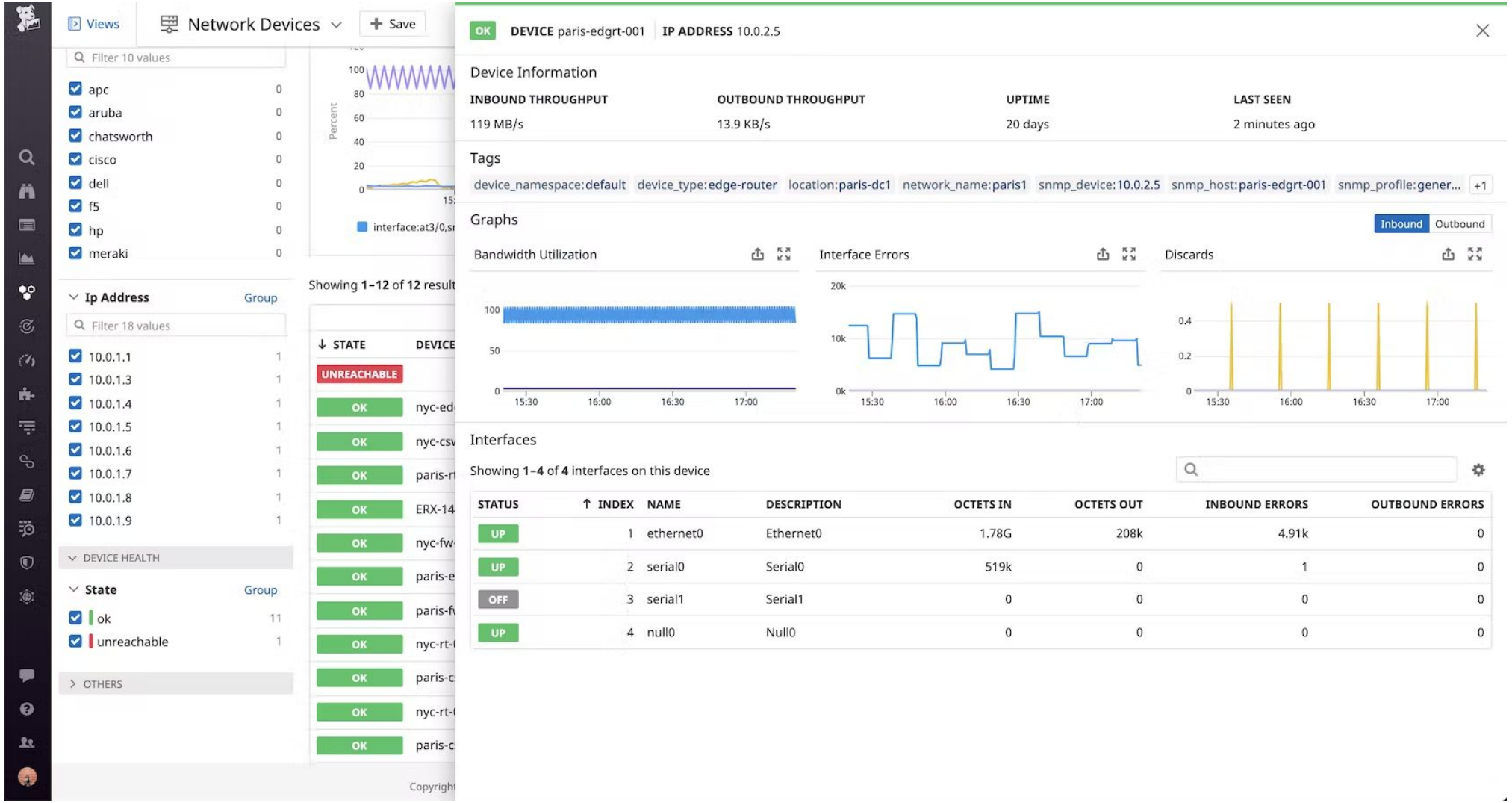
DATADOG

The Update Framework

- a.k.a. TUF
- How to make sure software updates are shipped in a secure way
- Datadog uses TUF to secure Datadog agent
  - PEP-458: Secure PyPI downloads with signed repository metadata
  - PEP-480: Surviving a compromise of PyPI: End-to-end signing of packages
- Uptane
  - Over-the-air software updates for automobile electronic control units
- Transparent TUF



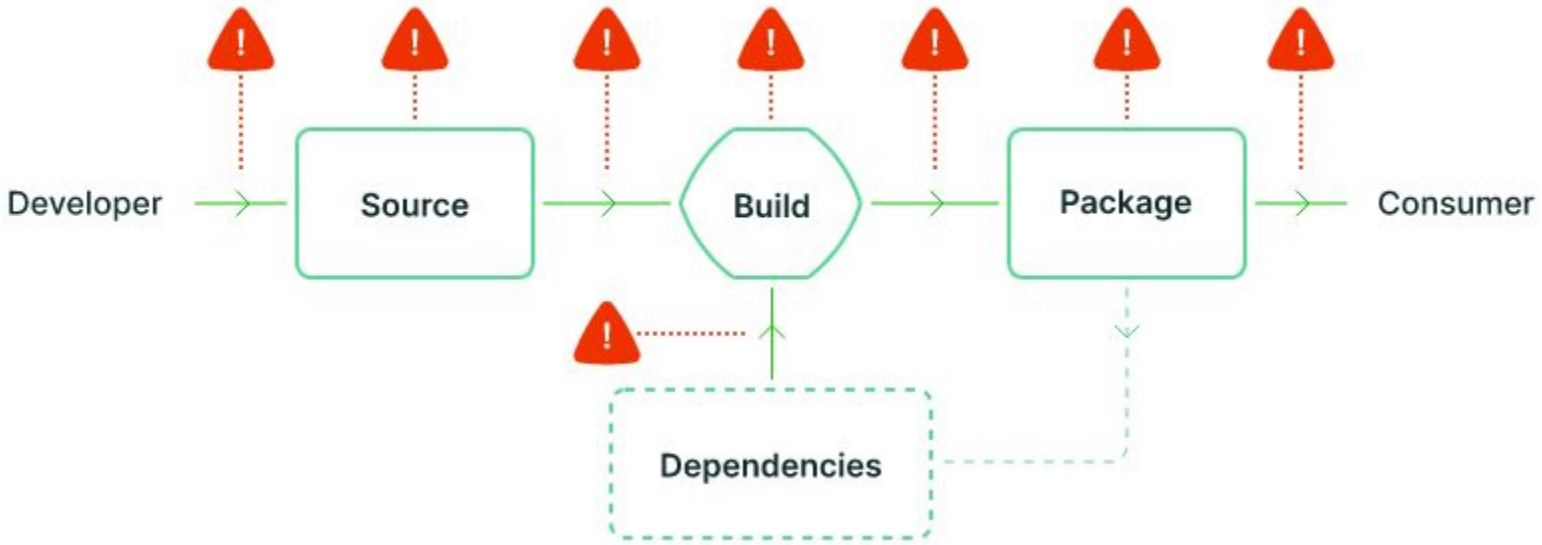
Datadog



DATADOG

SLSA

- 💃 🕺
- 🥫
- Supply Chain Levels for Software Artifacts



SLSA levels

Level	Description	Example
1	Documentation of the build process	Unsigned provenance
2	Tamper resistance of the build service	Hosted source/build, signed provenance
3	Extra resistance to specific threats	Security controls on host, non-falsifiable provenance
4	Highest levels of confidence and trust	Two-party review + hermetic builds

in-toto attestations

- signed metadata about a set of software artifacts
- Examples of hypothetical attestations:
  - Provenance: GitHub Actions attests to the fact that it built a container image with digest "sha256:87f7fe…" from git commit "f0c93d…" in the "main" branch of "https://github.com/example/foo".
  - Vulnerability scan: Google Container Analysis attests to the fact that no vulnerabilities were found in container image "sha256:87f7fe…" at a particular time.

Sigstore

sigstore

Overview | Community | How sigstore works | Trust and security | Blog | Docs

A new standard for signing, verifying and protecting software

Making sure your software's what it claims to be.

In collaboration with

OpenSSF | Chainguard | Cisco | Google | Hewlett Packard Enterprise | Purdue University | Red Hat | vmware

Thoth - AIDevSecOps

YouTube channel | News | Talks | Datasets | Documentation | Package index | API | Status | Tutorial | Help | Get involved

Project Thoth

Using Artificial Intelligence to analyse and recommend software stacks for Python applications.

Get started

Red Hat | IBM

DATADOG

deps.dev

open/source/insights

About Documentation Blog

Understand your dependencies

Your software and your users rely not only on the code you write, but also on the code your code depends on, the code *that* code depends on, and so on. An accurate view of the complete dependency graph is critical to understanding the state of your project. And it's not just code: you need to know about security vulnerabilities, licenses, recent releases, and more.

Search for open source packages | All systems | Search

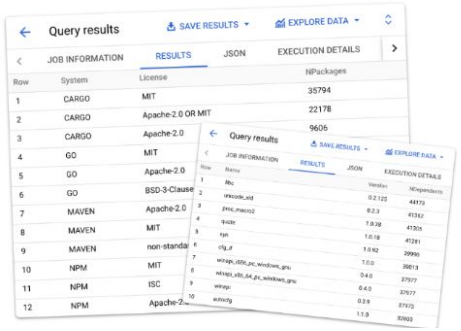
npm PACKAGES	2.14M
Go MODULES	903k
Maven ARTIFACTS	501k
PyPI PACKAGES	389k
Cargo CRATES	95k
NuGet PACKAGES	Coming soon

NEW

BigQuery Public Dataset

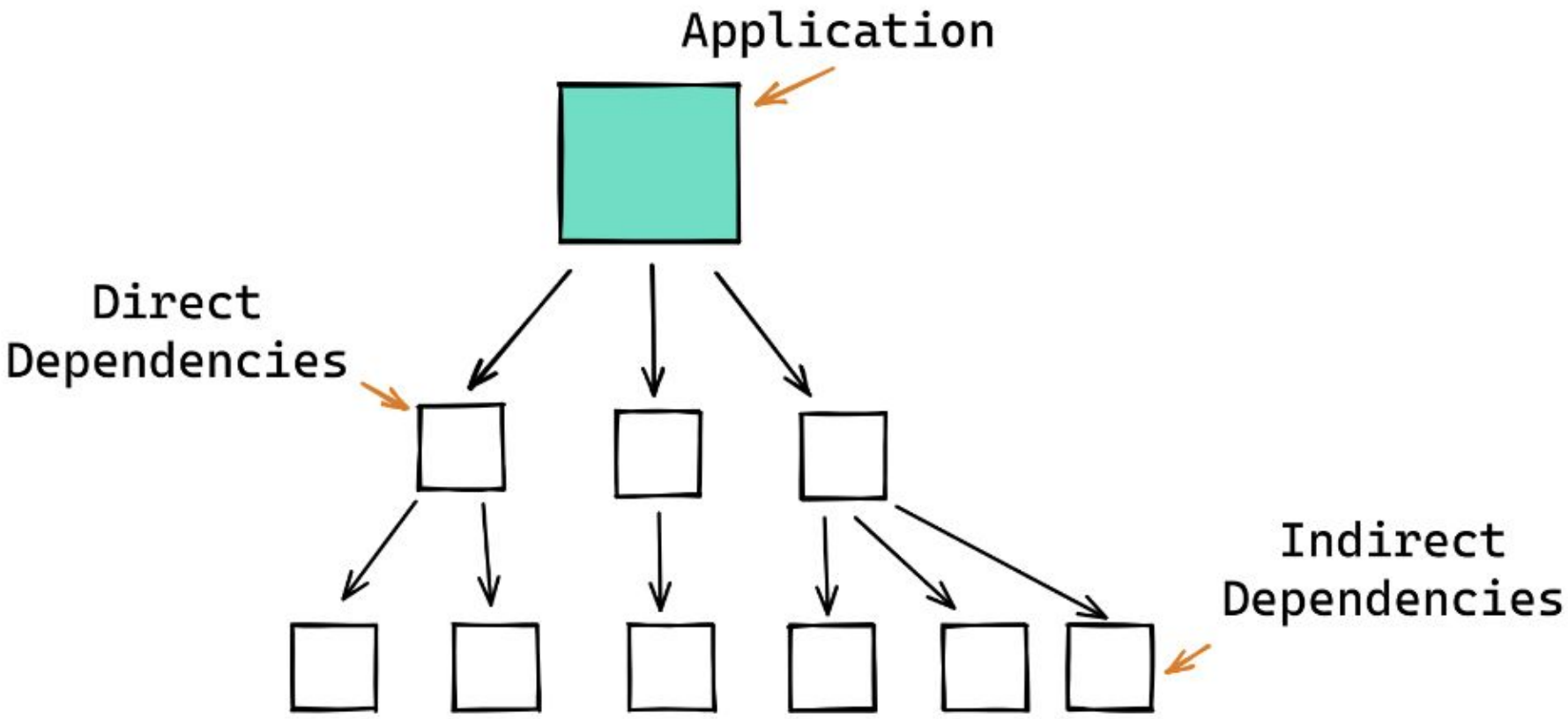
The data that powers this website is now also available as part of the Google Cloud Public Dataset Program, and can be explored using BigQuery.

For more information, please check out the dataset on the Google Cloud Platform Marketplace, or have a look at the schema documentation.



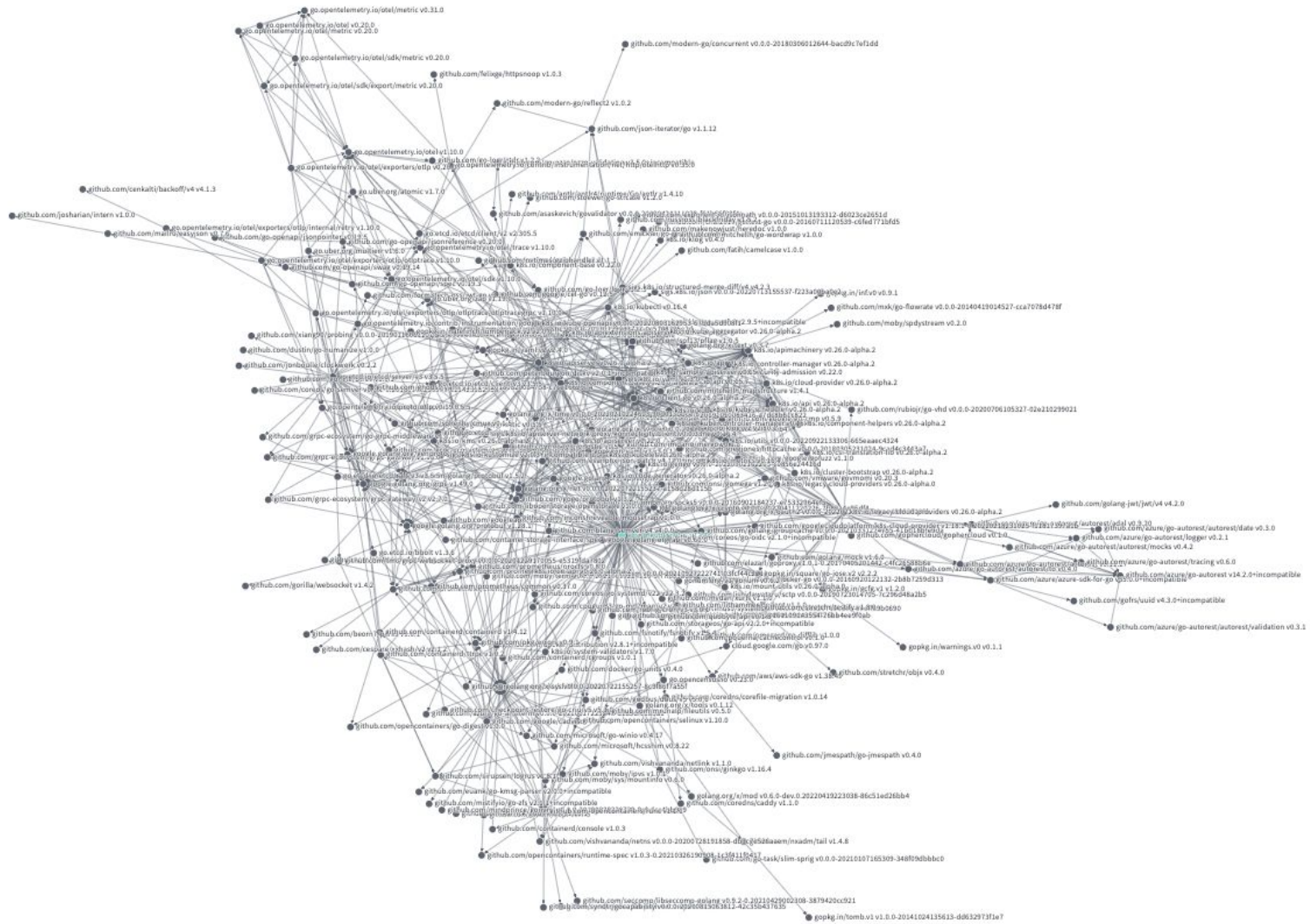
DATADOG

deps.dev



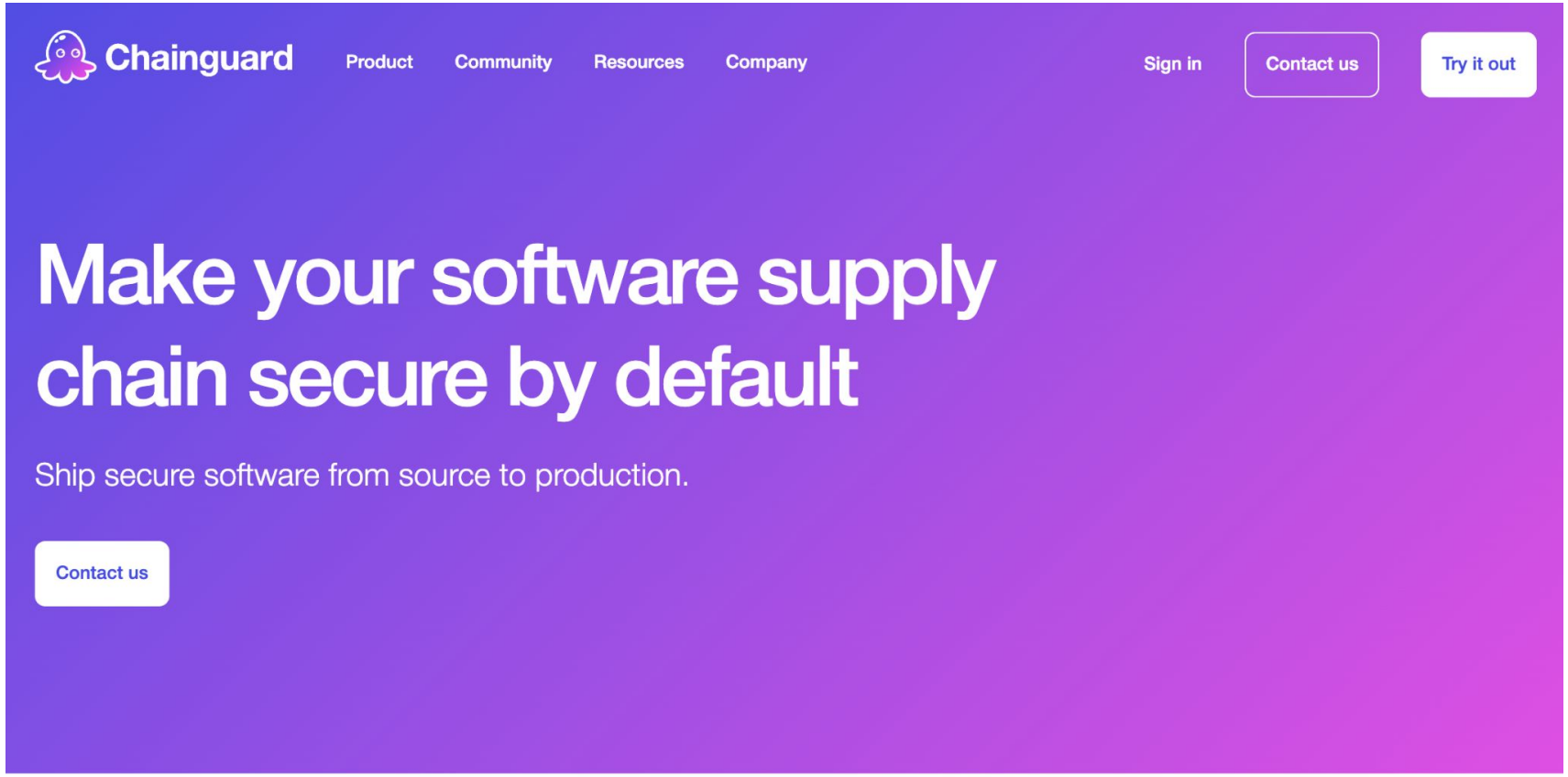
An application may have direct and indirect dependencies.

deps.dev



DATADOG

Chainguard



The first developer platform built for software supply chain security

DATADOG

TrailOfBits - pip-audit

TRAIL OF BITS

Home | Services | Products | Resources | Careers | About | Blog | Contact

HIRE US FOR YOUR HARDEST SECURITY PROBLEMS

We don't just fix bugs, we fix software.

Since 2012, Trail of Bits has helped secure some of the world's most targeted organizations and products.
We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code.

REQUEST A QUOTE

Services

Software Assurance

Get a comprehensive understanding of your security landscape and be absolutely confident in your technology and infrastructure. Our software assurance team are experts in systems software, blockchain, cryptography, and more.

HARDEN YOUR ENVIRONMENT

Security Engineering

Trail of Bits Engineering is your support team for security projects. Our experts work with you to build custom tools and remediate system vulnerabilities to keep your software secure—from development to testing and throughout continuous deployment.

OUR PROCESS + OUTCOMES

Other projects…

- govulncheck, pip-audit, …
- Chainguard - container images, VEX
- SBOM
  - Software Bill of Materials
- guac
  - Graph for Understanding Artifact Composition (GUAC) aggregates software security metadata into a high fidelity graph database
  - normalizing entity identities and mapping standard relationships between them
- VEX
  - Vulnerability Exploitability eXchange

🔐 Securing your environments

DATADOG

Securing your environments

- Know your dependencies
  - Is it possible? 🤔
- Consume only known signed software and artifacts
- Pin your dependencies
  - Avoid dependency confusion
- Sign artifacts, commit hashes
- Produce SBOM
- Mind vulnerabilities in your dependencies
- Consider adoption of the mentioned initiatives

Securing your environments

- If you are an open-source software maintainer:
  - Consider installing OpenSSF Security Scorecards on your repository
  - 2FA (ex PyPI)
  - Report vulnerabilities!
  - Care about vulnerabilities in your application stack
  - Be kind to your community 🤗

Thanks for your attention.