Signature Approved ✅

SECURING KUBERNETES WORKLOADS WITH KYVERNO & AWS SIGNER

notary project

aws

aws COMMUNITY DAY TÜRKİYE

#awscommunityday

#awscommunitydayturkiye

About us

Hi 👋,

I’m Koray Oksay, a Kubernetes Consultant & Instructor at KUBERMATIC

Find me on X at: **@korayoksay**

CNCF Ambassador | Kubestronaut

Kubernetes Contributor #k8s-sig-infra

GitHub Profile: **koksay**

aws COMMUNITY DAY TÜRKİYE

About us

Hi 👋,

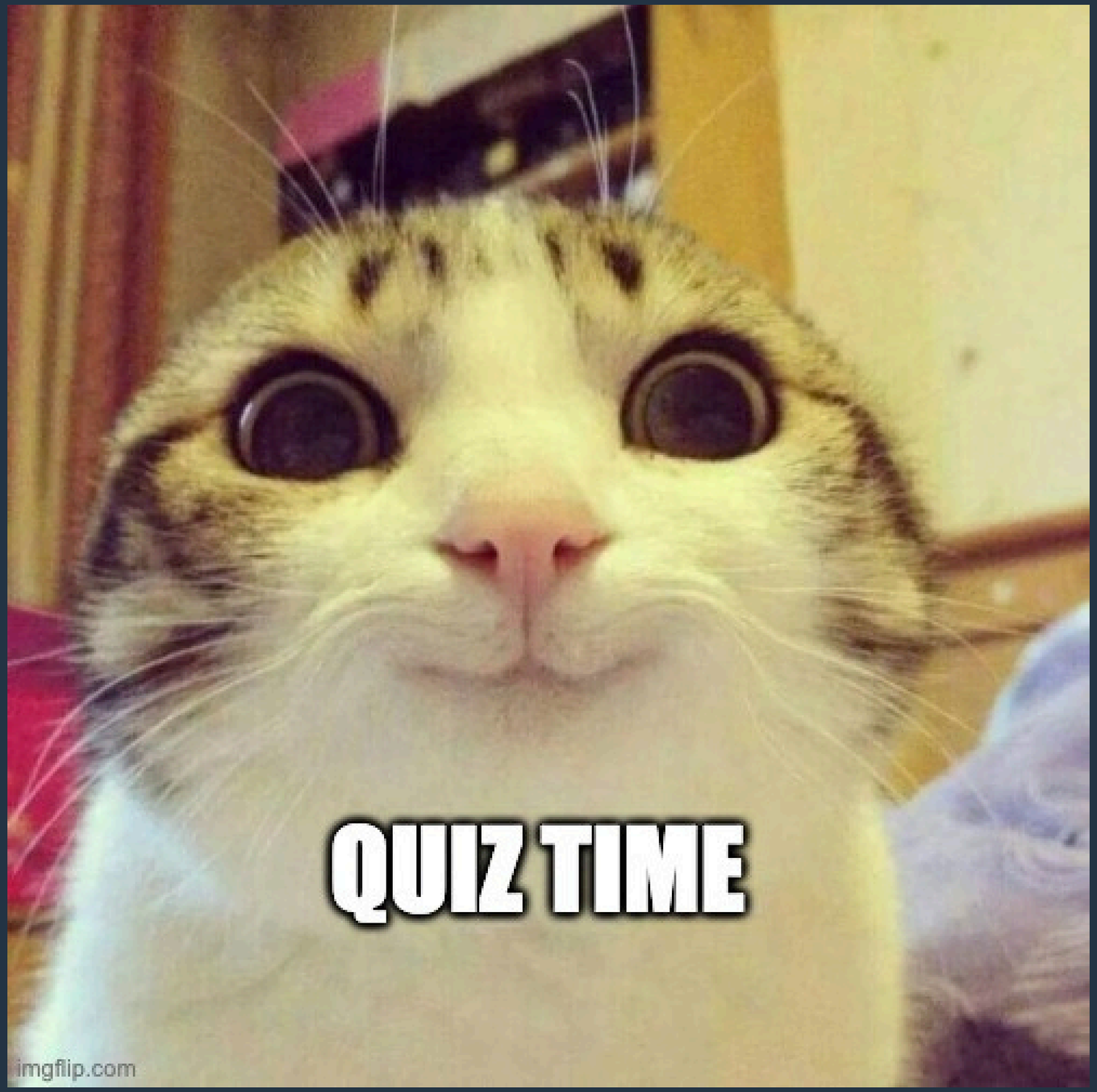
I’m Batuhan Apaydın, a Platform Engineer at trendyol.com

Find me on X at: @**developerguyba**

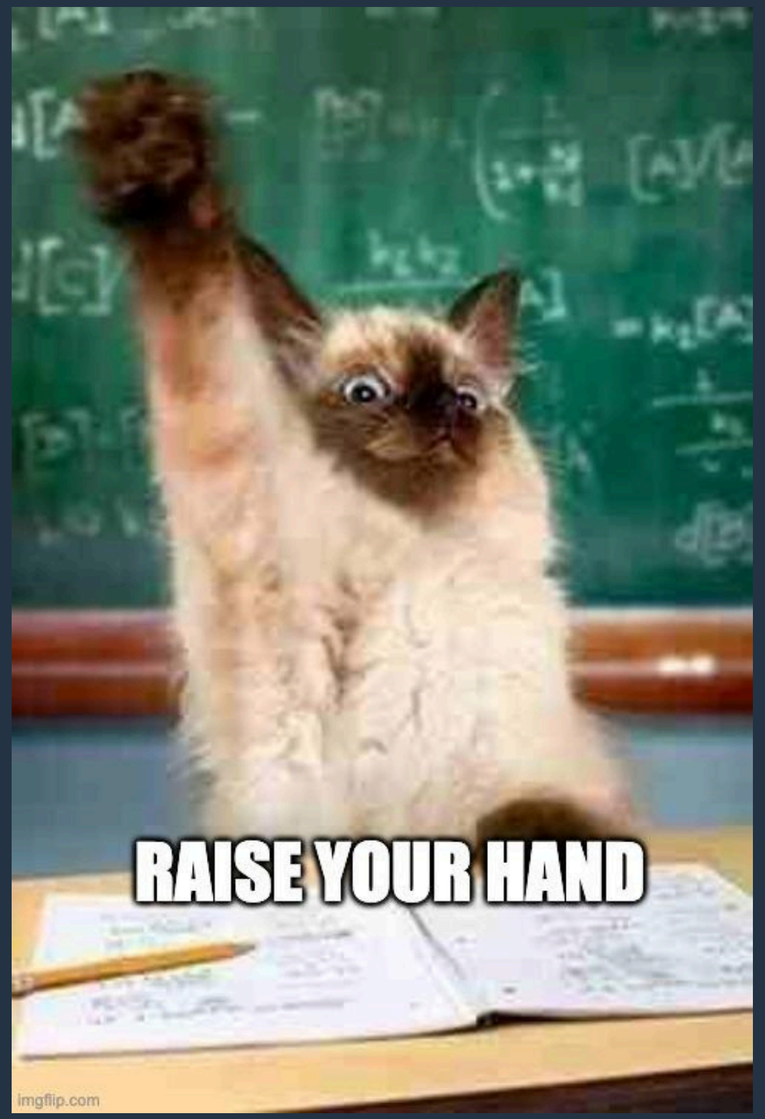
CNCF Ambassador | Kubestronaut

First ever Docker from Turkey 🇹🇷

GitHub Profile: **developer-guy**


QUIZ TIME
imgflip.com

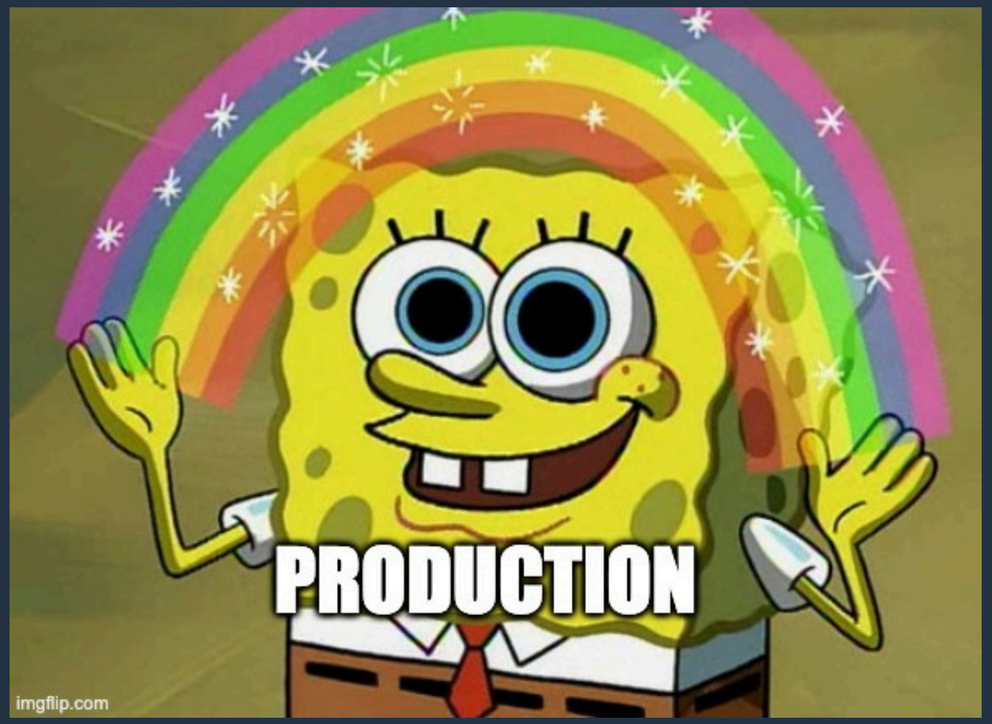
Have you ever heard of Software Supply Chain Security before?



Are you familiar with these tools?

- Kyverno
- Notation
- AWS Signer

How many of you are using one of these tools in production?



Software Supply Chain attacks are real **threats** for everyone else! 😰

Some notable metrics from **10 Year Look Back**:

- Low-severity vulnerabilities; which previously took 300-400 days to fix, are now **seeing delays of 500-700 days** or more, with some stretching out nearly **800 days in 2024.**

- For high-severity vulnerabilities; earlier in the decade, the average fix times ranged between 150 and 300 days, but in recent years, **these have extended beyond 400 days.**

- Nearly three years after the discovery of the Log4Shell vulnerability, **13% of Log4j downloads are still for known vulnerable versions.**

https://www.sonatype.com/state-of-the-software-supply-chain/2024/10-year-look

Software Supply Chain attacks are real **threats** for everyone else! 😰

Key Concerns

Safe Origin

How do you ensure that all container images running in the cluster come from an approved source?

Integrity

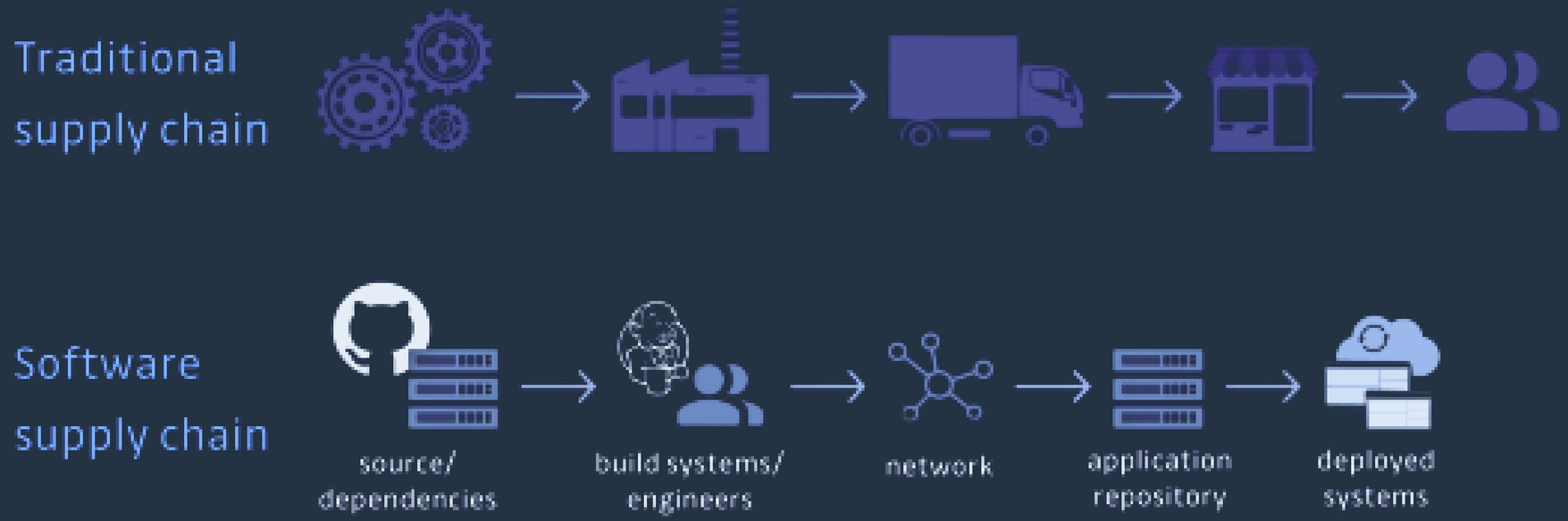
How do you ensure that containers were not modified before running after their provenance was proven?

A definition of the **Traditional Supply Chain!**

Traditionally, **a supply chain is anything that's needed to deliver your product**

For a chocolate bar you buy at the store,

- it's the list of ingredients, the packaging, the information on nutritional contents,
- and maybe information on organic ingredients or production facilities
- also more than that: it's anything that can affect your delivery of that product, too.

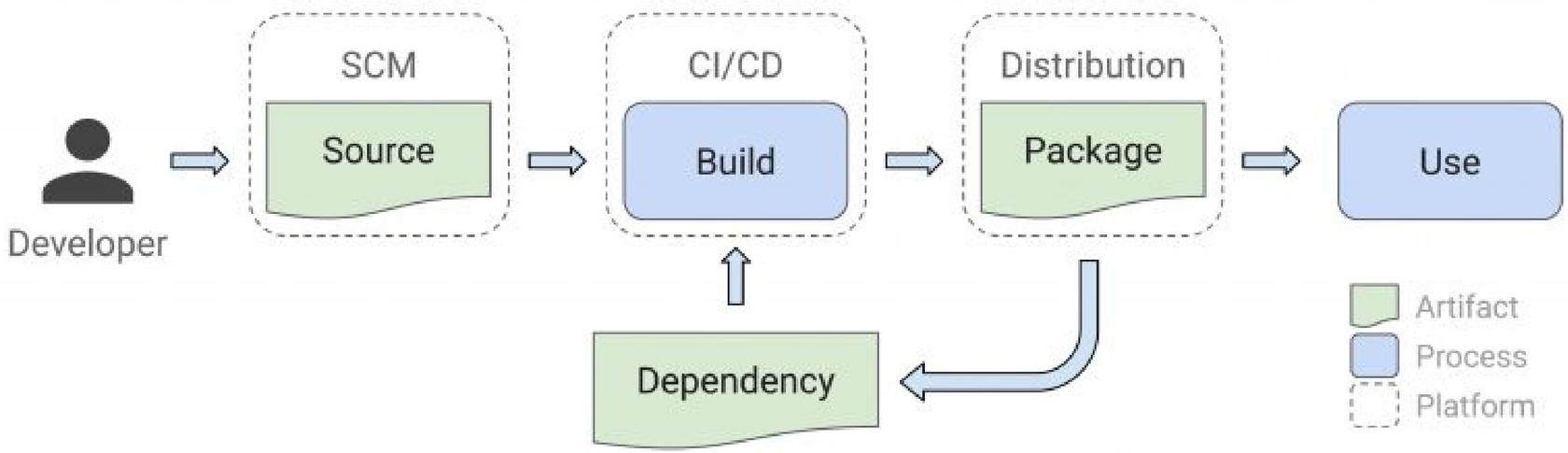


https://www.gitguardian.com/nhi-hub/software-supply-chain-security

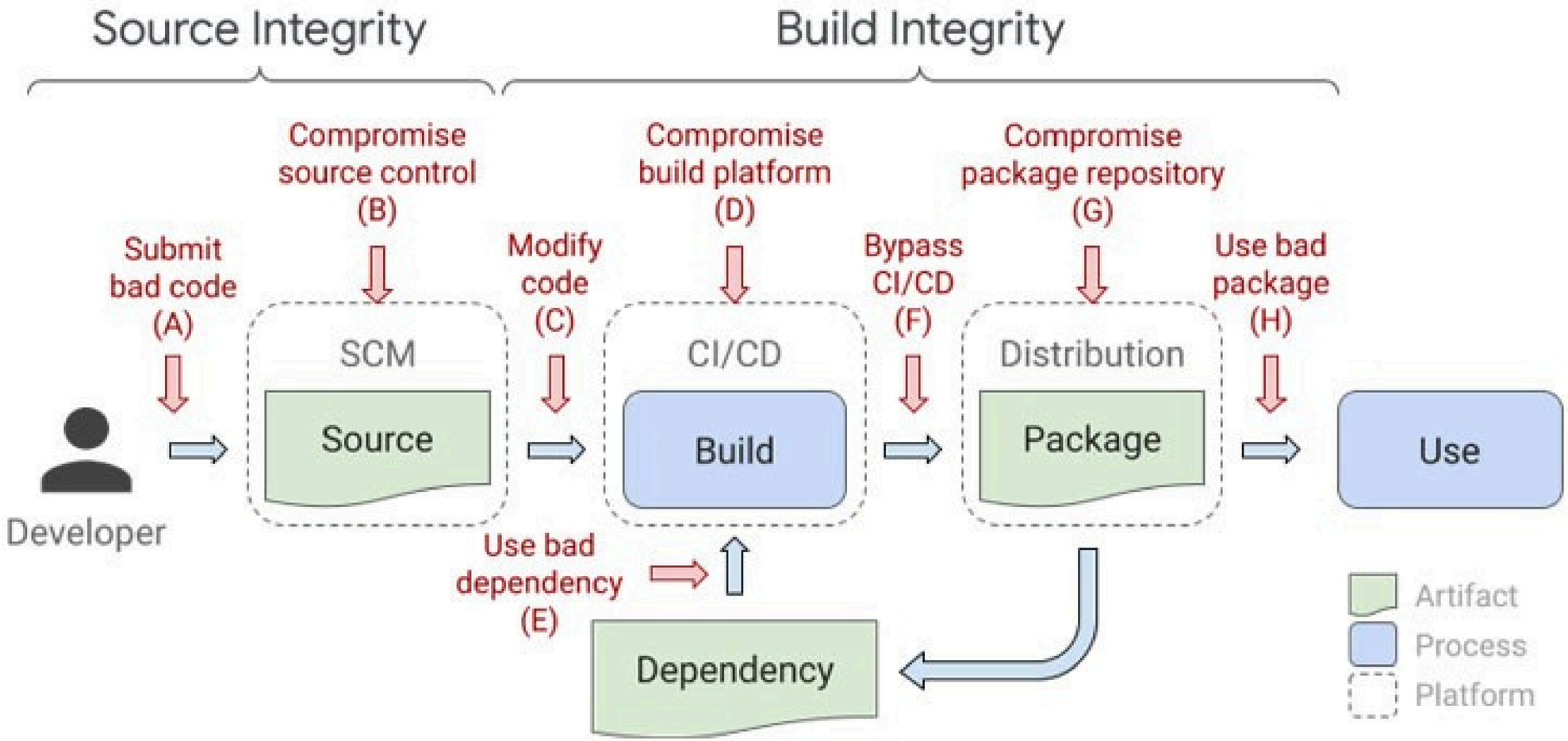
A definition of the Software Supply Chain!

Swapping from chocolate to codebase,

A software supply chain is anything that goes into or affects your code from development, through your CI/CD pipeline, until it gets deployed into production



A definition of the Software Supply Chain Security!



“low-hanging fruit” is defined by Merriam-Webster as “the obvious or easy things that can be most readily done or dealt with in achieving success or making progress toward an objective”)

Container images are new way of shipping software to the Production land!

Gartner predicts:

*“By 2027, more than **75%** of all AI deployments will use container technology as the underlying compute environment, **up from less than 50% today.**”*

and

*“By 2028, **80%** of custom software running at the physical edge will be deployed in containers, which is an increase from **10% in 2023.**”*

87% of Container Images in Production Have Critical or High-Severity Vulnerabilities! 😢

There has been an astonishing

742%

average annual increase in Software Supply Chain attacks *over the past 3 years!*

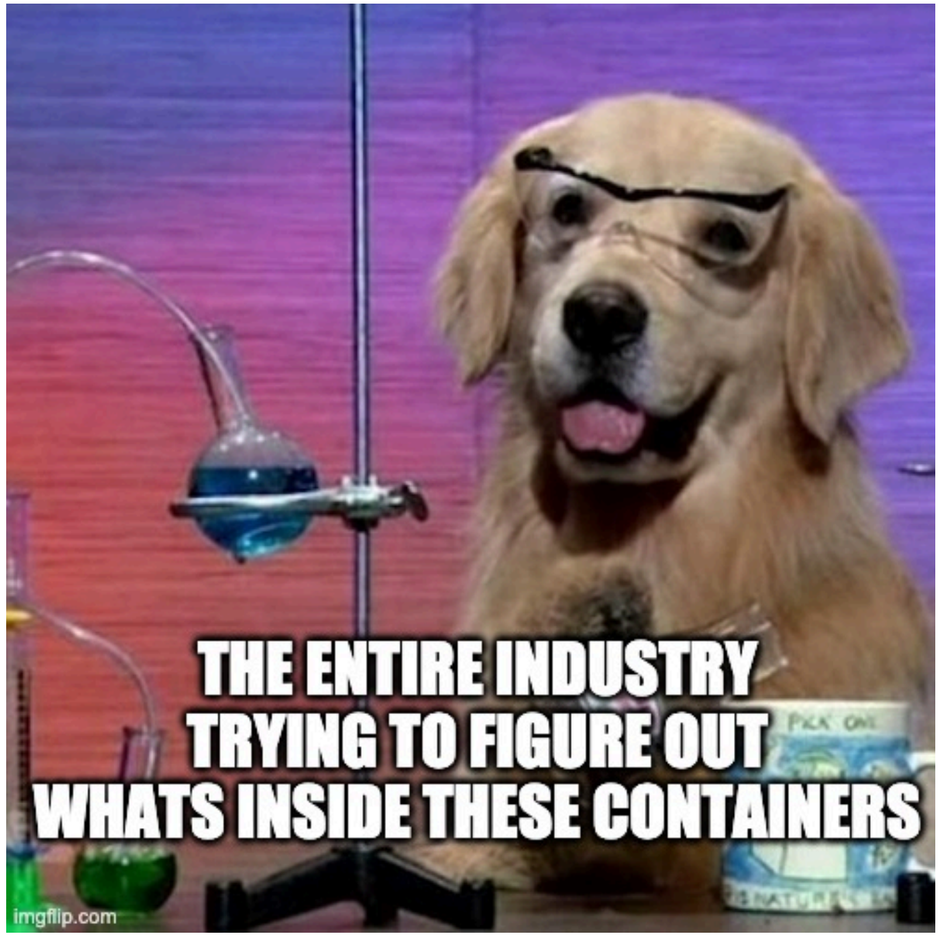
⇑ **75%**

up from a year ago!

About

6 out of every 7

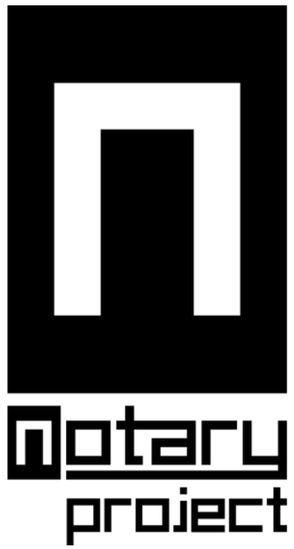
project vulnerabilities come from *transitive dependencies*!

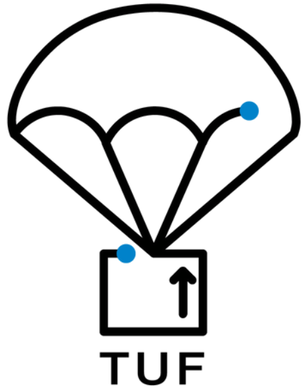


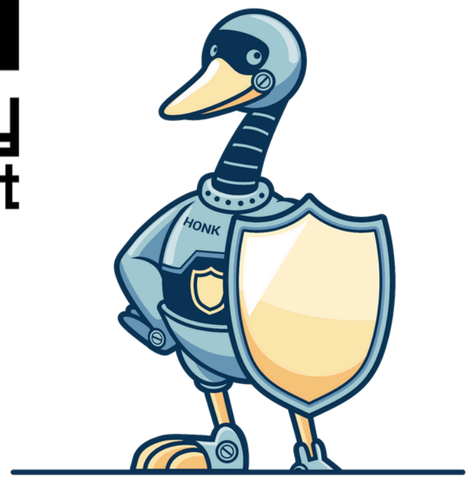
60%

The percentage of top public containers that have more vulnerabilities today than they did a year ago.

Current state of the Art








SIT TIGHT
WE ARE GOING
TO DO SPEED RUN
imgflip.com

Kyverno

A policy enforcement tool based on the policies you write in **YAML.**

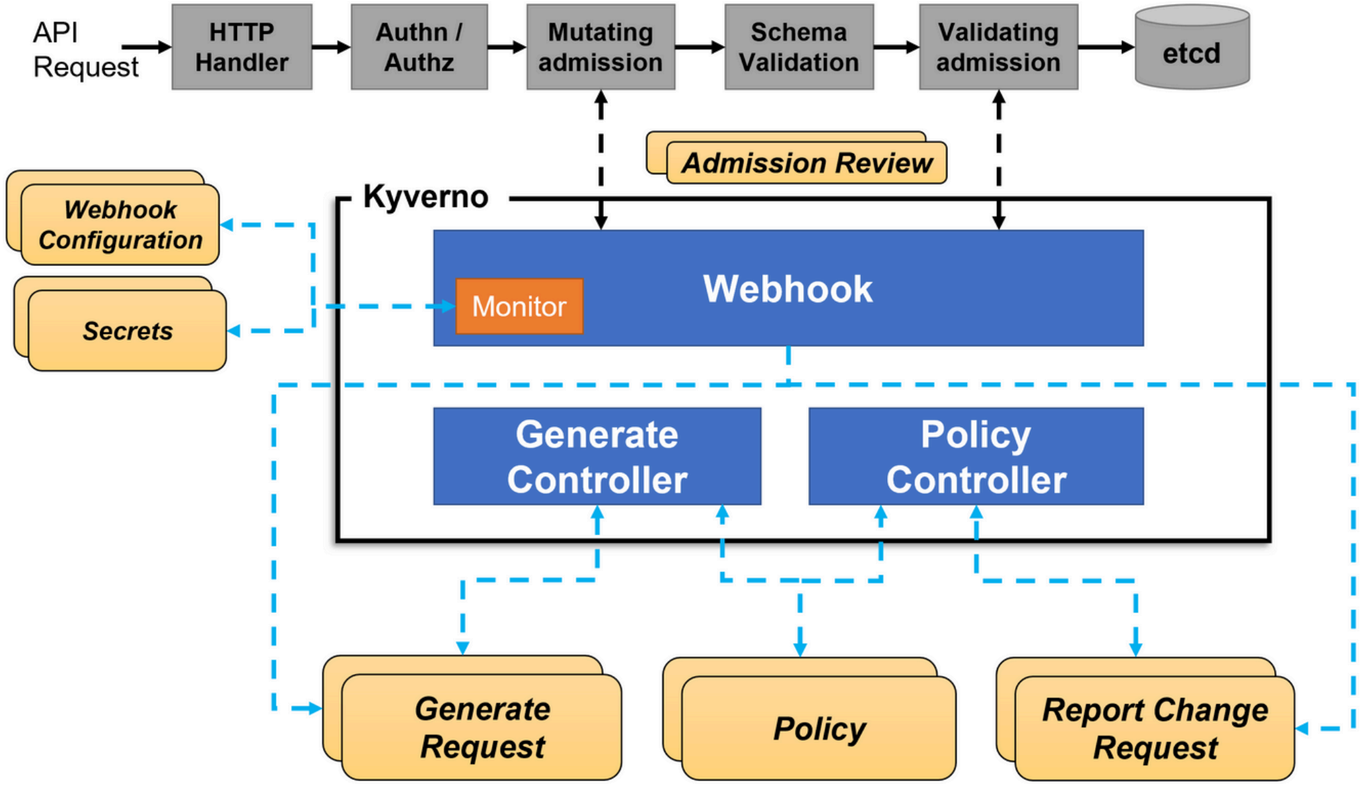
No new language to learn!

CNCF Incubating project

Released 1.0 which means it is now **GA!**

Integrated image signature:

- cosign
- Notation



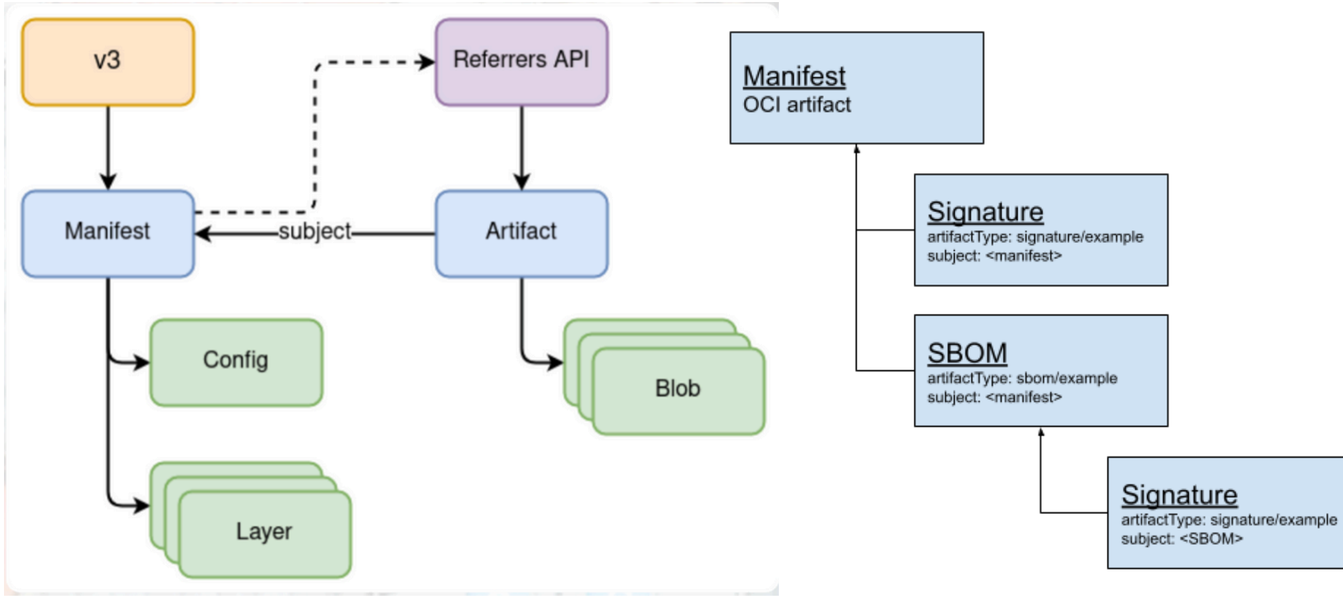
OCI v1.1 Referrers API: standard way of creating relations between container images and software supply chain materials!

Storing and managing relevant artifacts together with the primary artifact simplifies querying and visualization, improving both manageability and performance.

- If a registry supports the Referrers API, no additional tags are needed since a new field on the OCI Image Manifest called **subject**.

Using the OCI referrers API, image signature verification becomes a standardized and easy process.

- Relevant artifacts can be copied together between registries also can be deleted easily with a garbage collection!



Documentation > Amazon ECR > User Guide

Private images in Amazon ECR

PDF RSS Focus mode

Amazon ECR stores Docker images, Open Container Initiative (OCI) images, and OCI compatible artifacts in private repositories. You can use the Docker CLI, or your preferred client, to push and pull images to and from your repositories.

With Amazon ECR support for OCI v1.1, you can store and manage reference artifacts that are defined by the OCI Referrers API. Artifacts include signatures, Software Bill of Materials (SBoMs), Helm charts, scan results, and attestations. A set of artifacts for a container image is transferred with that container and stored as a separate image that counts as an image consumed for your repository.

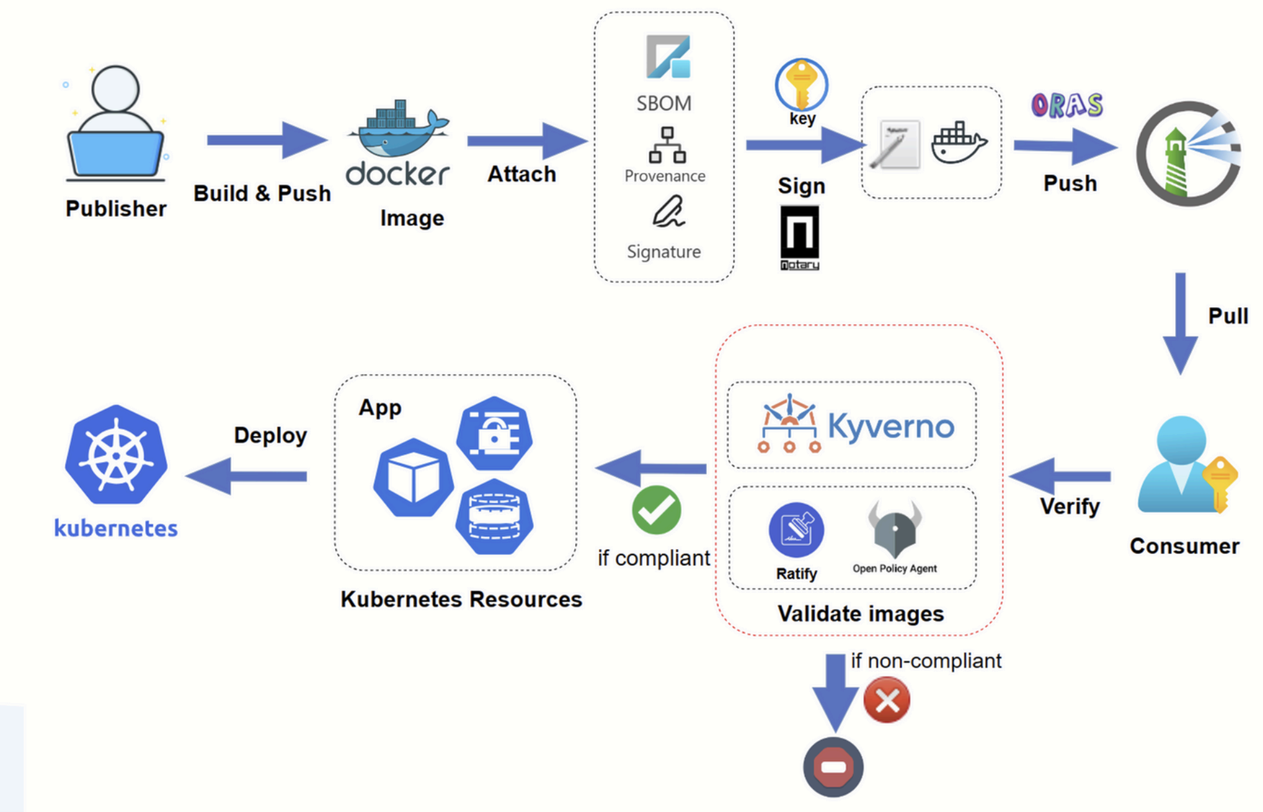
Notation: A CLI tool to sign and verify artifacts!

Notary v2 improves on v1, enabling users to sign multiple artifacts (e.g., container images, SBOMs, scan results)

Notary v2 was launched in December 2022, it aims to be a cross-industry, cross-registry specification for signing and verifying OCI images

Notation CLI integrates with 3rd party key management solutions through a plugin model.

Notation CLI Supports two signature formats. By default, a textual (JSON-based) format is used (JWS), you can also use COSE, which is a *binary* format producing smaller signature file sizes.

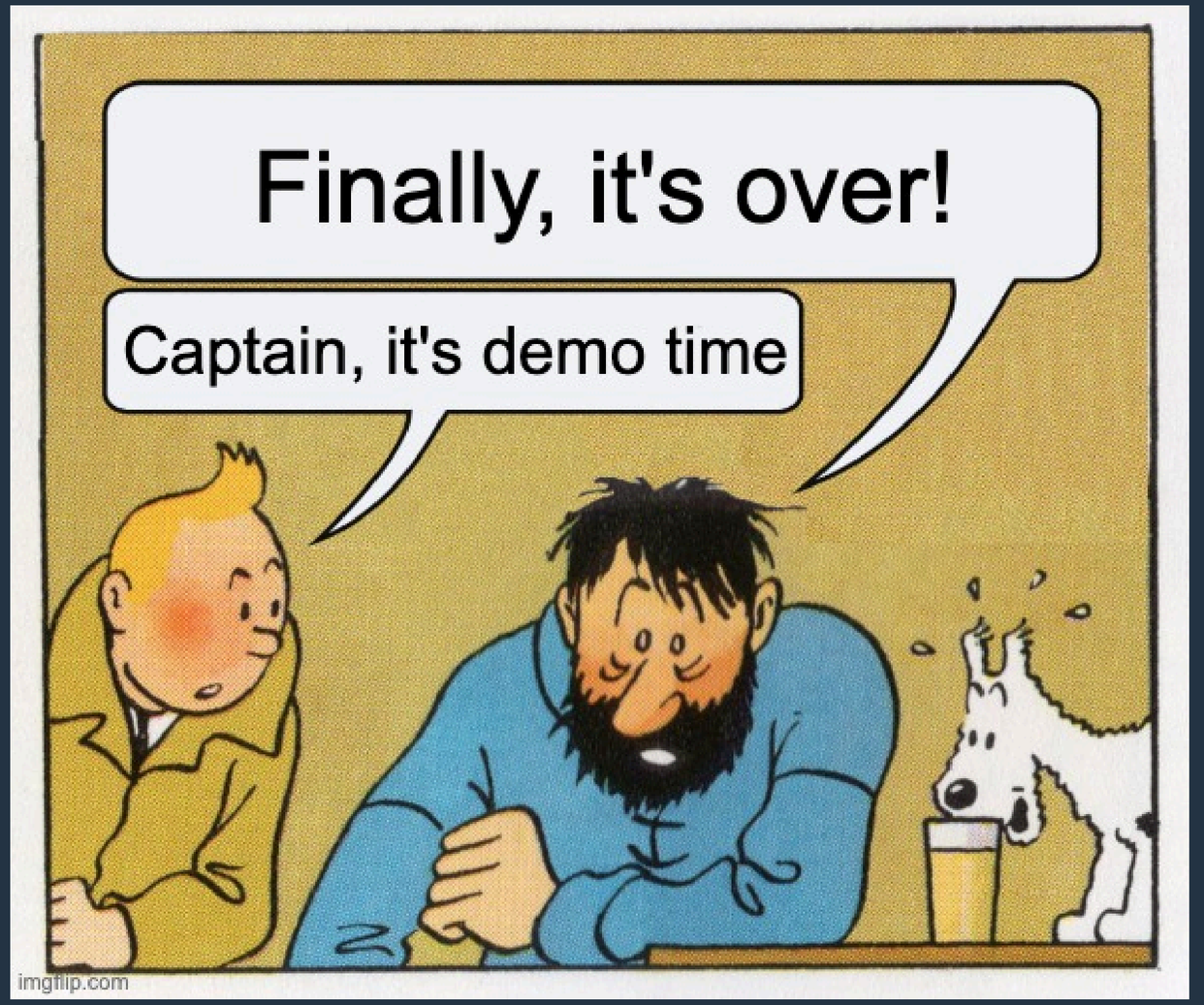


AWS Signer: fully managed code-signing service to ensure the trust and integrity of your code!

AWS Signer is a new capability that gives customers native AWS support for signing and verifying container images stored in container registries like Amazon Elastic Container Registry (Amazon ECR)

Signer eliminates customer overhead of managing cryptographic resources

Available at no additional charge for Lambda code signing, container images, and IoT firmware



https://github.com/koksay/signature-approved

Q&A / Feedback

THANKS

@developerguyba

@korayoksay

aws COMMUNITY DAY TÜRKİYE