Trivy Open Source Scanner for Container Images
Just Download and Run

Teppei Fukuda (@knqyf263)
Maintainer, Trivy
Open Source Team, Aqua Security

What this webinar will cover today

- Introduction
  - What is a vulnerability?
  - Why is a vulnerability scanner necessary?
- About Trivy
  - What is Trivy?
  - Basic features
  - Advanced features
  - New features

Vulnerability (computing)

From Wikipedia, the free encyclopedia

In computer security, a **vulnerability** is a weakness which can be exploited by a Threat Actor, such as an attacker, to perform unauthorised actions within a computer system.

Software vulnerabilities

aqua

Common Vulnerabilities & Exposures

CVE® is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

aqua

General +

Vulnerabilities +

Vulnerability Metrics +

Products +

Configurations (CCE)

Contact NVD

Other Sites +

Search +

Vulnerabilities

CVE defines a vulnerability as:
"A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."
All vulnerabilities in the NVD have been assigned a CVE identifier and thus, abide by this definition.

Using Vulnerabilities within the NVD

1. Vulnerability Search and Detail Pages
2. Download vulnerability information for all published CVE vulnerabilities from the NVD Data Feeds

A CVE that is in the **RESERVED** state in the CVE Dictionary will not appear in the NVD.

Heartbleed (CVE-2014-0160)

Technical Details

Vulnerability Type (View All)

- Buffer Errors (CWE-119)

Vulnerable software and versions Switch to CPE 2.2

+ Configuration 1

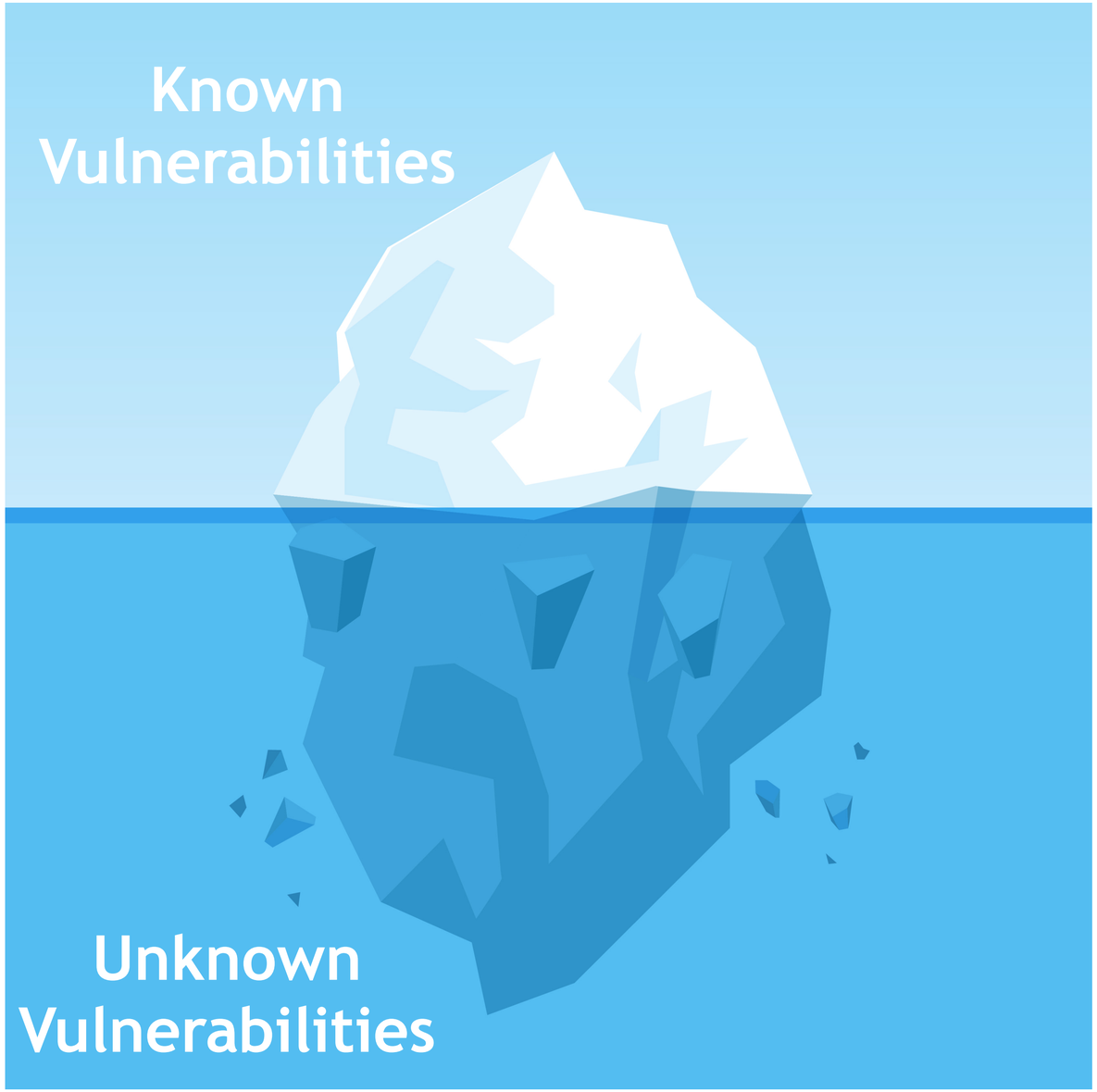
+ OR

- ✱ cpe:2.3:a:openssl:openssl:1.0.1:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1:beta1:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1:beta2:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1:beta3:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1a:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1b:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1c:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1d:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1e:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.1f:*:*:*:*:*:*:*
- ✱ cpe:2.3:a:openssl:openssl:1.0.2:beta1:*:*:*:*:*:*

aqua

Vulnerabilities

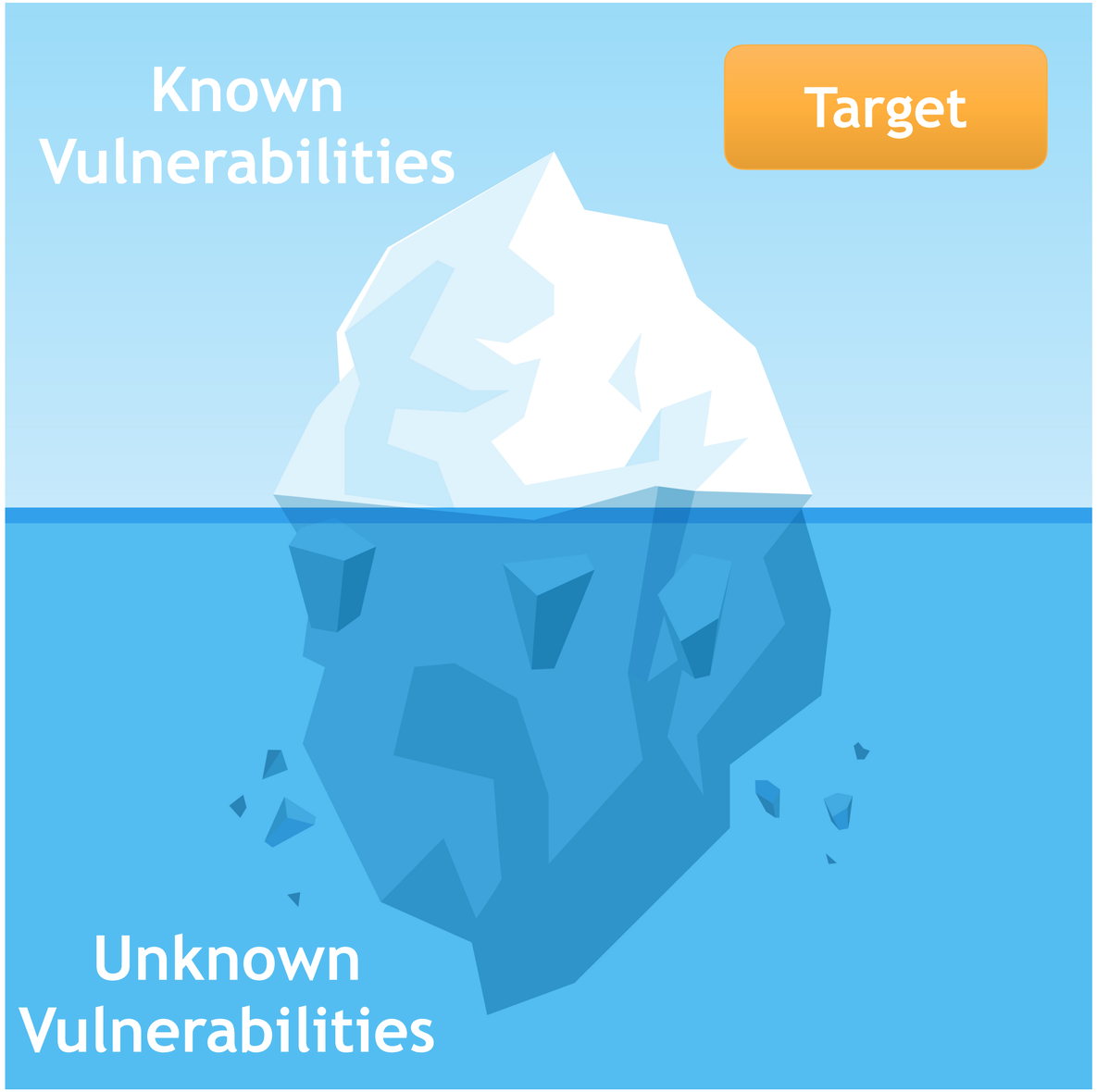
- Known vulnerabilities
  - ID assigned
- Unknown vulnerabilities
  - Your code
  - Undisclosed



Designed by vvstudio / Freepik

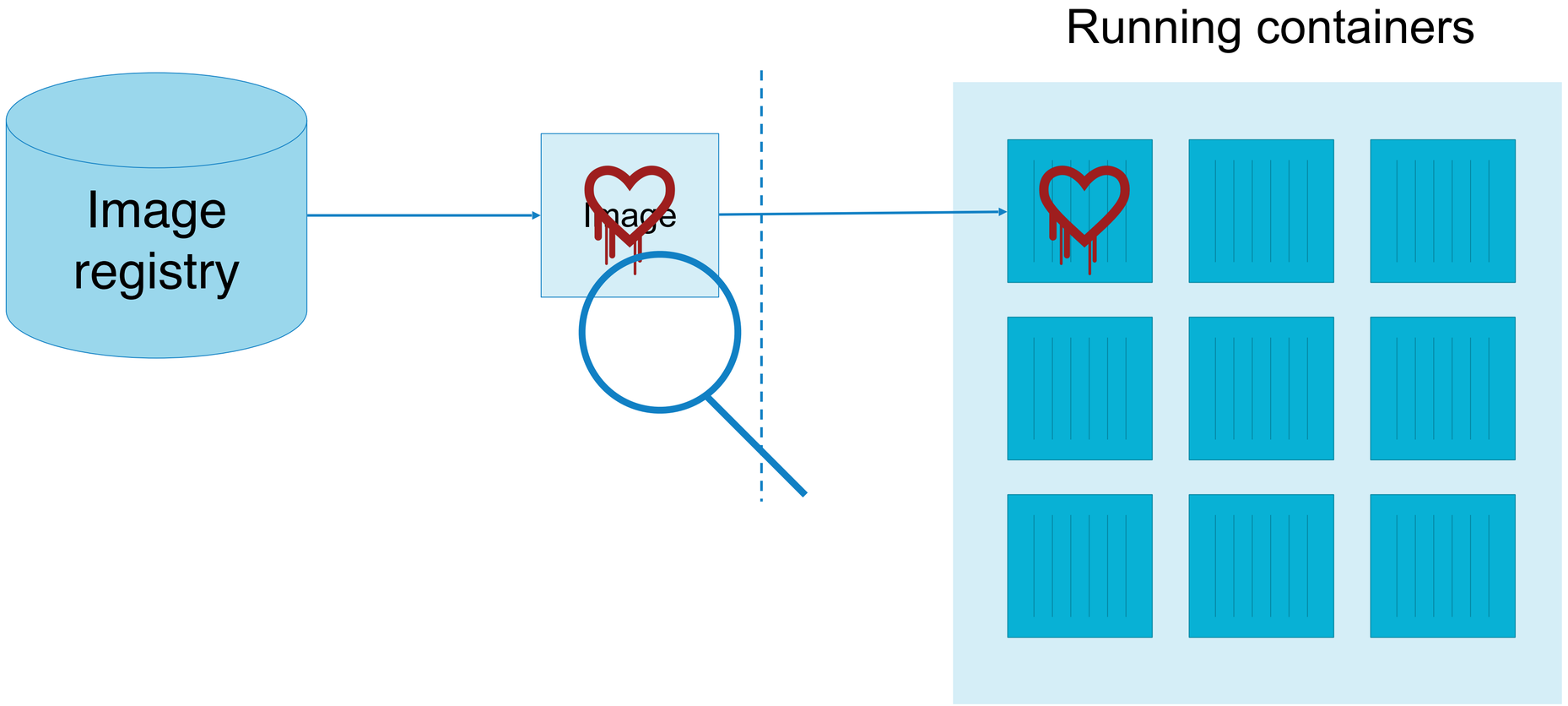
Vulnerabilities

- Known vulnerabilities
  - Scanner identifying components with known vulnerabilities
  - e.g. Trivy, Clair, Aqua
- Unknown vulnerabilities
  - Web application vulnerability scanners, fuzzing tools
  - e.g. OWASP ZAP, OSS-Fuzz



Designed by vvstudio / Freepik

Containers, images and vulnerabilities



Vulnerability scanner

From Wikipedia, the free encyclopedia

A **vulnerability scanner** is a computer program designed to assess computers, computer systems, networks or applications for known weaknesses.

Image vulnerability scanning

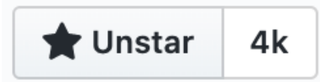
- Identify the packages & versions in the image
- Cross-reference with vulnerability database
  - There are distributions: Linux kernel + shell, init system, package manager, etc.
  - A vendor backports security fixes
    - Upstream: 1.0.1 fixes CVE-2020-XXXX
    - Red Hat: 1.0.0-2.el7 fixes CVE-2020-XXXX
    - Debian: 1.0.0-deb9u1 fixes CVE-2020-XXXX

Trivy

aqua

Trivy

- Open source scanner for container images
- Developed in 2019



trivy

https://github.com/aquasecurity/trivy

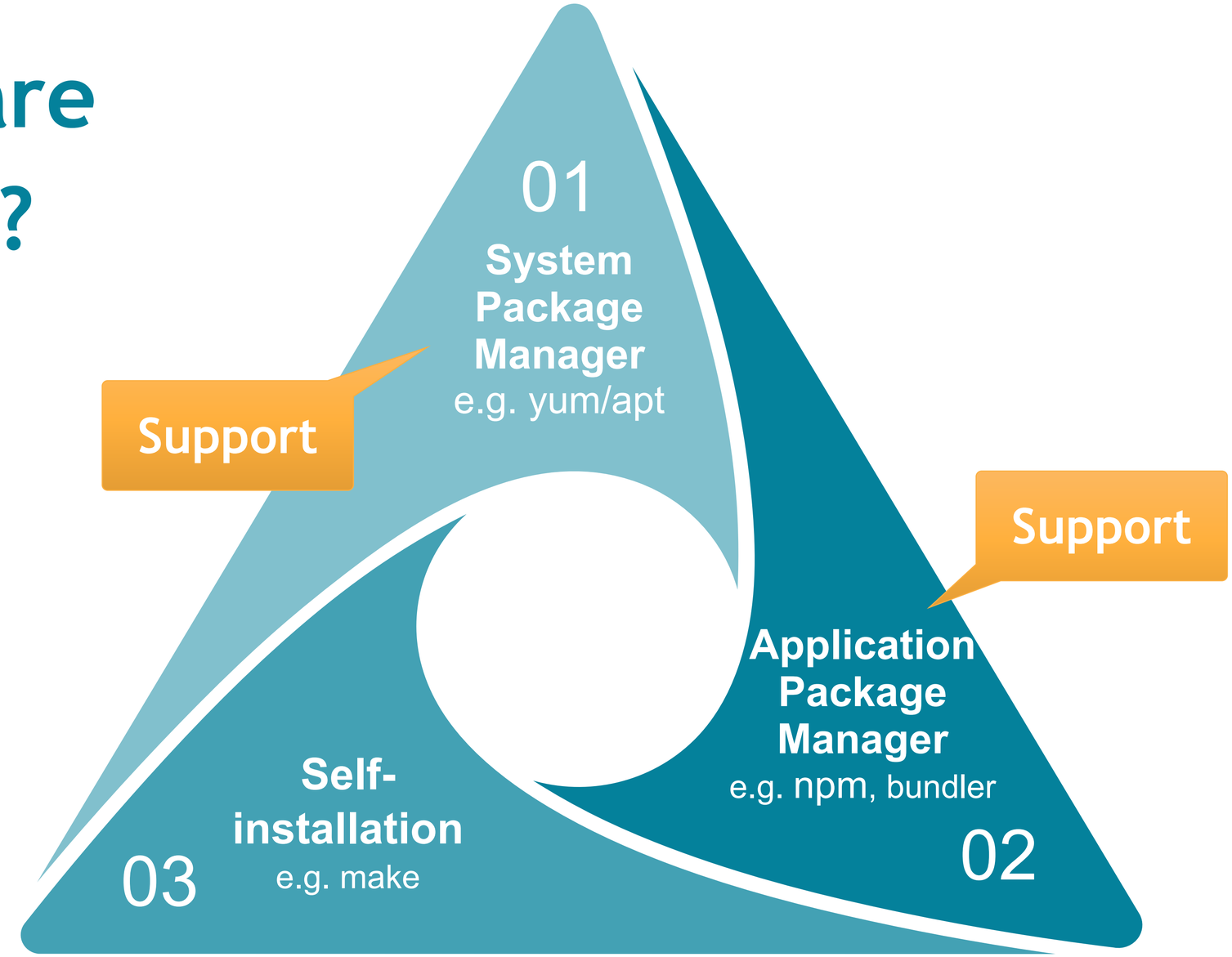
Features

- Detect comprehensive vulnerabilities
- Easy installation
- Simple
- High accuracy
- DevSecOps
- Support multiple formats

Features

- Detect comprehensive vulnerabilities
- Easy installation
- Simple
- High accuracy
- DevSecOps
- Support multiple formats

How does software get into a server?



aqua

Detect comprehensive vulnerabilities

- System Package Manager
  - apt
  - yum
  - apk
- Application Package Manager
  - Bundler
  - Composer
  - Pipenv
  - Poetry
  - npm
  - yarn
  - Cargo

Support OS

Alpine Linux	Red Hat Universal Base Image	Red Hat Enterprise Linux	CentOS	Debian GNU/ Linux	Ubuntu	Amazon Linux
✓	✓	✓	✓	✓	✓	✓

Oracle Linux	openSUSE	SUSE Enterprise Linux	Photon OS	Google Distroless	Fedora	Windows
✓	✓	✓	✓	✓		

Features

- Detect comprehensive vulnerabilities
- Easy installation
- Simple
- High accuracy
- DevSecOps
- Support multiple formats

Installation

RHEL/CentOS

```
$ sudo vim /etc/yum.repos.d/trivy.repo
[trivy]
name=Trivy repository
baseurl=https://aquasecurity.github.io/trivy-repo/rpm/
releases/$releasever/$basearch/
gpgcheck=0
enabled=1
$ sudo yum update
$ sudo yum install trivy
```

Installation

macOS

```
$ brew install aquasecurity/trivy/trivy
```

Install script

The install script downloads the trivy binary based on your OS and architecture

```
$ curl -sfL https://raw.githubusercontent.com/aquasecurity/
trivy/master/contrib/install.sh | sh -s -- -b /usr/local/bin
```

Features

- Detect comprehensive vulnerabilities
- Easy installation
- Simple & Fast
- High accuracy
- DevSecOps
- Support multiple formats

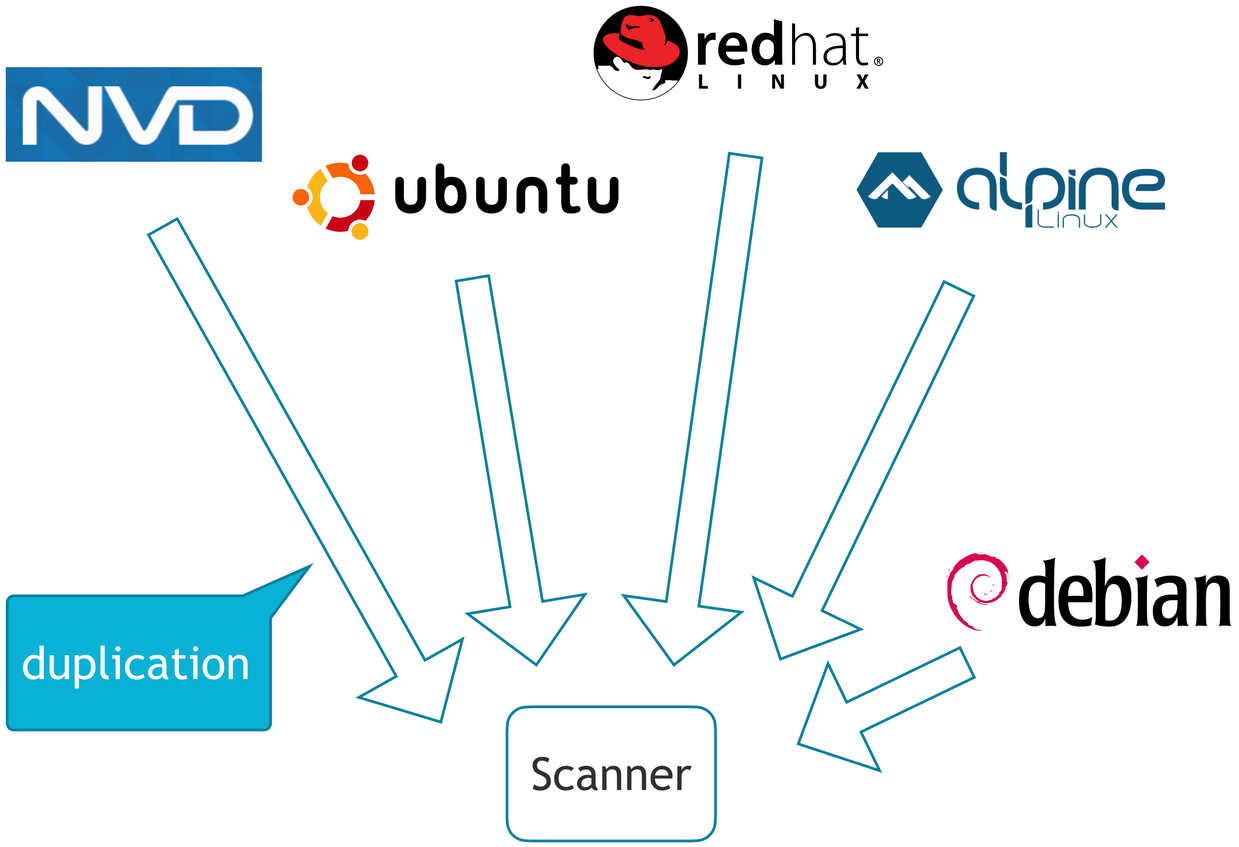
Run

```
$ trivy image [YOUR_IMAGE_NAME]
```

Fast

- Downloading vulnerability information usually takes a while
  - Full database (default)
    - includes description and references
    - It takes about 10 seconds on the first run
  - Light database (--light option)
    - doesn't include the details
    - It takes a few seconds on the first run

Security advisory



Normal way

Security advisory

Download
security advisories

GitHub

Remove duplication
and build DB
on GitHub Actions
every 12 hours

Download DB

trivy

aqua

Vulnerability DB

Bolt DB

- Single file database
- Embedded key/value database

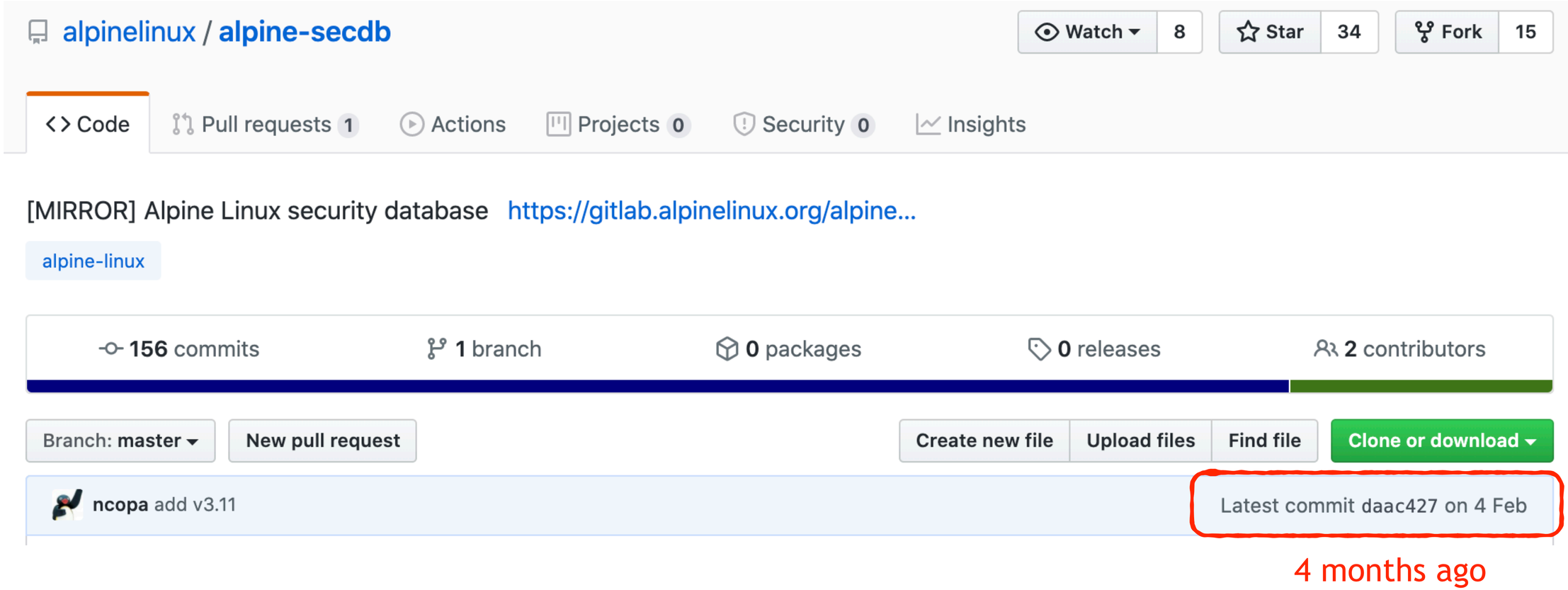
aqua

Features

- Detect comprehensive vulnerabilities
- Easy installation
- Simple & Fast
- High accuracy
- DevSecOps
- Support multiple formats

High accuracy

- Alpine
  - alpine-secdb
    - Many open source scanners depend on this database
    - The purpose of this database is to make it possible to know what packages has backported fixes.
    - https://github.com/alpinelinux/alpine-secdb


alpinelinux / alpine-secdb
Watch 8
Star 34
Fork 15
Code
Pull requests 1
Actions
Projects 0
Security 0
Insights
[MIRROR] Alpine Linux security database https://gitlab.alpinelinux.org/alpine...
alpine-linux
156 commits
1 branch
0 packages
0 releases
2 contributors
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
ncopa add v3.11
Latest commit daac427 on 4 Feb
4 months ago

aqua

High accuracy

- Alpine
  - alpine-secdb
    - https://github.com/alpinelinux/alpine-secdb
  - **Alpine packages**
    - Alpine Linux aports repository
    - This repository contains the APKBUILD files for each and every Alpine Linux package, along with the required patches and scripts, if any.
    - https://gitlab.alpinelinux.org/alpine/aports

Closed Opened 5 days ago by **Alicha CH** 4 of 4 tasks completed Report abuse New issue

json-c: integer overflow and out-of-bounds write (CVE-2020-12762)

json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.

References:

- https://nvd.nist.gov/vuln/detail/CVE-2020-12762
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2020-12762

Patches:

- https://github.com/json-c/json-c/pull/608 (0.14)
- https://github.com/json-c/json-c/pull/607 (0.13.x)

Affected branches:

- [x] master
- [x] 3.11-stable
- [x] 3.10-stable
- [x] 3.9-stable

Edited 3 days ago by Leo

0.14-0 or less is vulnerable

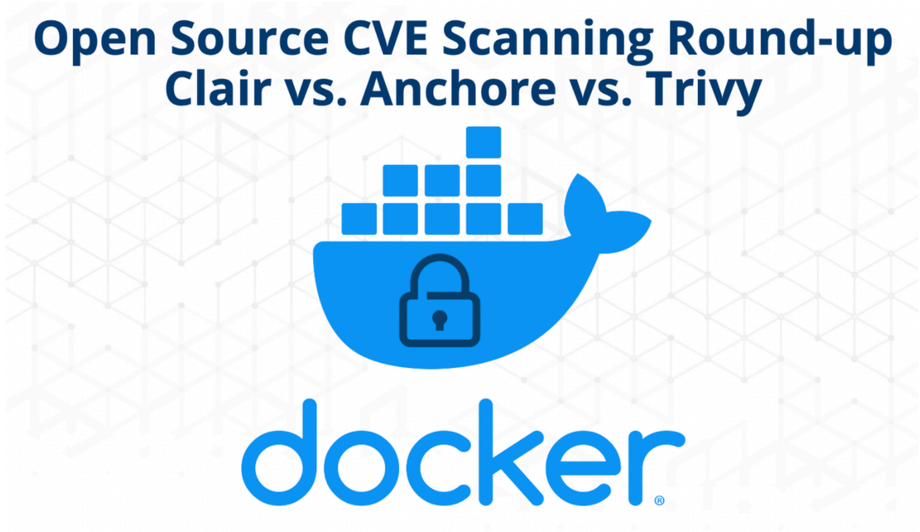
main/json-c/APKBUILD +10 -3

```
1  1  # Maintainer: Natanael Copa <ncopa@alpinelinux.org>
2  2  pkgname=json-c
3  3  pkgver=0.14
4     - pkgrel=0
   4  + pkgrel=1
5  5  pkgdesc="A JSON implementation in C"
6  6  url="https://github.com/json-c/json-c/wiki"
7  7  arch="all"
8  8  license="MIT"
9  9  makedepends="cmake"
10 10 subpackages="$pkgname-dev"
```

aqua

Open Source CVE Scanner Round-Up: Clair vs Anchore vs Trivy

by David Widen | Friday, Apr 24, 2020 | Docker Security



Anchore Scan Results for Alpine

< Projects< Repositories< anchore-test/alpine

anchore-test/alpine:latest

Author	anonymity	No vulnerability
Architecture	amd64	
OS	linux	
OS Version		
Docker Version	18.09.7	

Clair Scan Results for Alpine

< Projects< Repositories< clair-test/alpine

clair-test/alpine:latest

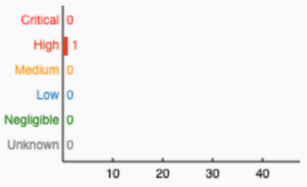
Author	anonymity	No vulnerability
Architecture	amd64	
OS	linux	
OS Version		
Docker Version	18.09.7	

Trivy Scan Results for Alpine

< Projects< Repositories< trivy-test/alpine

trivy-test/alpine:latest

Author	anonymity
Architecture	amd64
OS	linux
OS Version	
Docker Version	18.09.7
Scan Completed	Apr 22, 2020



https://boxboat.com/2020/04/24/image-scanning-tech-compared/

aqua

High accuracy - Use multiple data sources

- PHP
  - FriendsOfPHP
  - GitHub Advisory Database
- Python
  - Safety DB
  - GitHub Advisory Database
- Ruby
  - Rubysec
  - GitHub Advisory Database
- Node.js
  - Node.js Security Working Group
  - GitHub Advisory Database

v0.9.0 supports GitHub Advisory Database
(achieved by @masahiro331)

Features

- Detect comprehensive vulnerabilities
- Easy installation
- Simple & Fast
- High accuracy
- DevSecOps
- Support multiple formats

DevSecOps

With Travis CI

```
script:
  - trivy image --exit-code 0 --severity HIGH --no-progress --auto-refresh [YOUR_IMAGE]
  - trivy image --exit-code 1 --severity CRITICAL --no-progress --auto-refresh [YOUR_IMAGE]
...
```

DevSecOps

GitHub Action

Marketplace / Actions / Trivy Vulnerability Scanner

GitHub Action

Trivy Vulnerability Scanner

0.0.4 Latest version

Use latest version

Trivy Action

> GitHub Action for Trivy

Table of Contents

Stars

Star 0

Contributors

Categories

Security Code review

Links

https://github.com/aquasecurity/trivy-action

aqua

DevSecOps

GitHub Action from Azure

GitHub Action

Container image scan

v0 Pre-release

Use latest version

Container Scan

This action can be used to help you add some additional checks to help you secure your Docker Images in your CI. This would help you attain some confidence in your docker image before pushing them to your container registry or a deployment.

It internally uses `Trivy` and `Dockle` for running certain kinds of scans on these images.

- `Trivy` helps you find the common vulnerabilities within your docker images.
- `Dockle` is a container linter, which helps you identify if you haven't followed
  - Certain best practices while building the image
  - CIS Benchmarks to secure your docker image

Verified creator

GitHub has verified that this action was created by **Azure**.

Learn more about verified Actions.

Stars

Unstar 41

Contributors

https://github.com/Azure/container-scan

aqua

DevSecOps

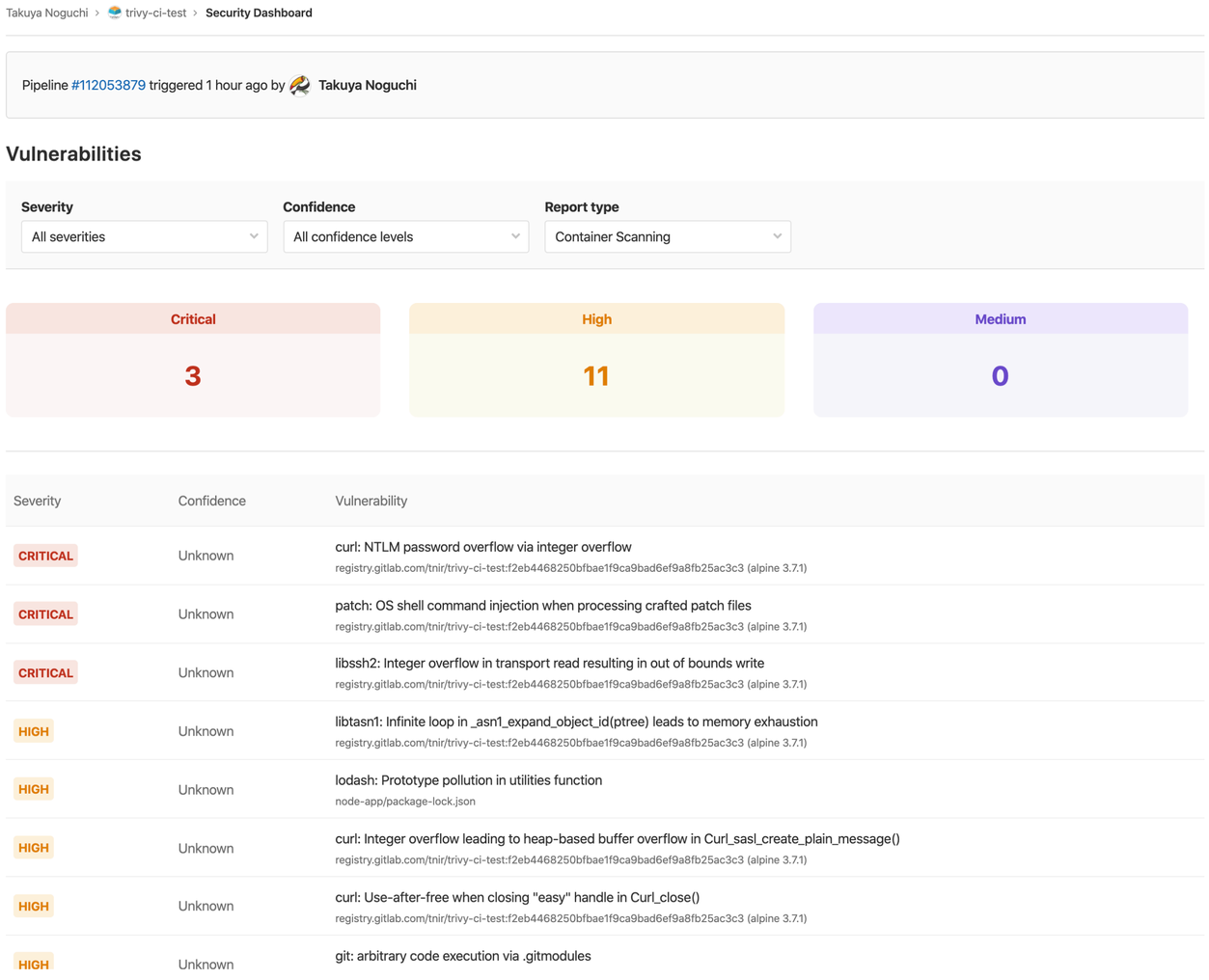
GitLab Integration

```
include:
 - remote: "https://github.com/aquasecurity/
trivy/raw/master/contrib/Trivy.gitlab-ci.yml"

build:
   ...

Trivy_container_scanning:
  artifacts:
    paths: [gl-container-scanning-report.json]
```

Added by @mrueg and @tnir



aqua

Features

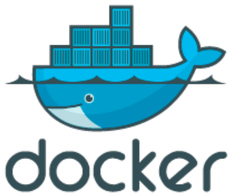
- Detect comprehensive vulnerabilities
- Easy installation
- Simple
- High accuracy
- DevSecOps
- Support multiple formats

Support multiple formats

Registry

An image in a container registry

Docker Engine



An image in a Docker Engine

Kaniko

Docker Archive

An image stored
in a "docker save"-formatted file

OCI

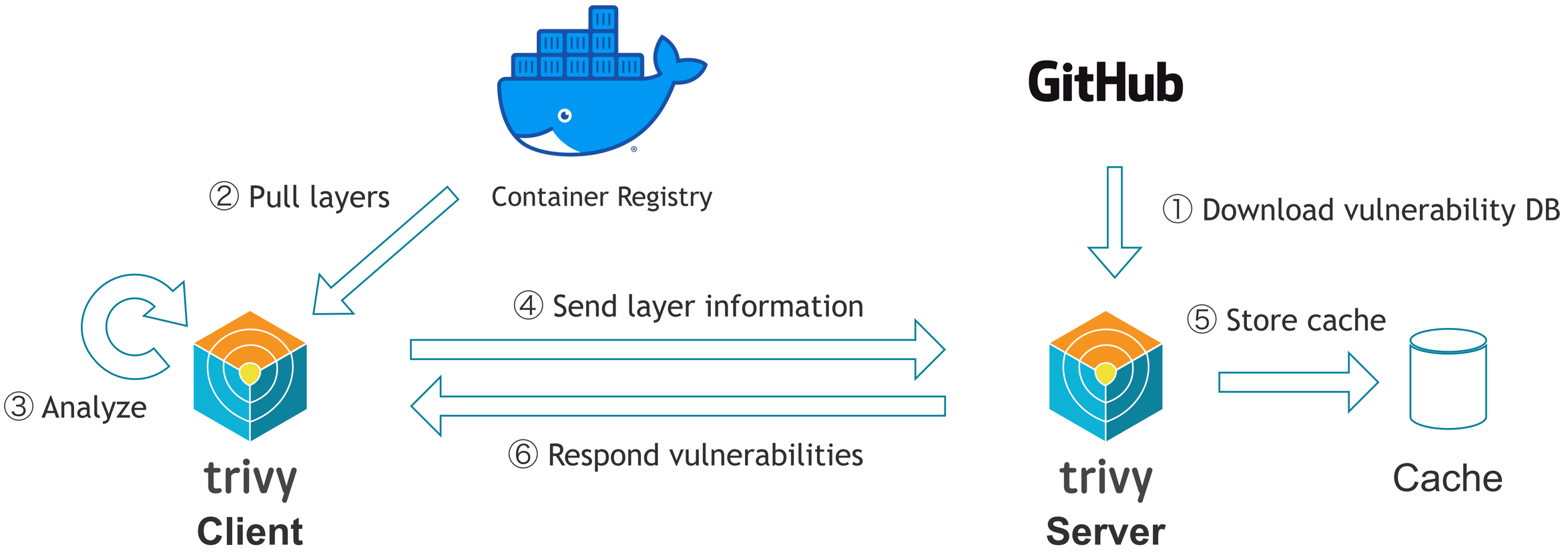
An image directory compliant with
"Open Container Image Layout Specification"

aqua

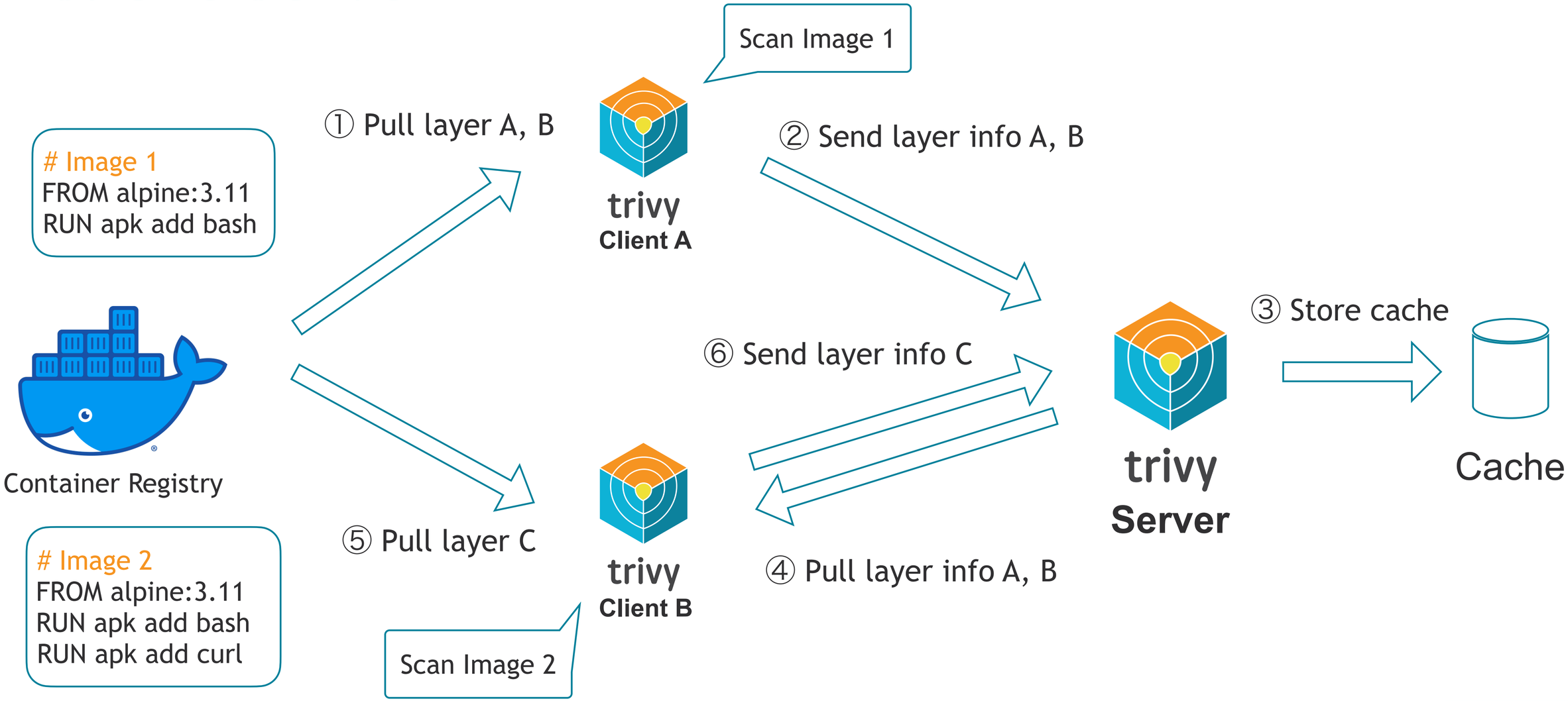
Advanced Features

aqua

Client/Server



Client/Server

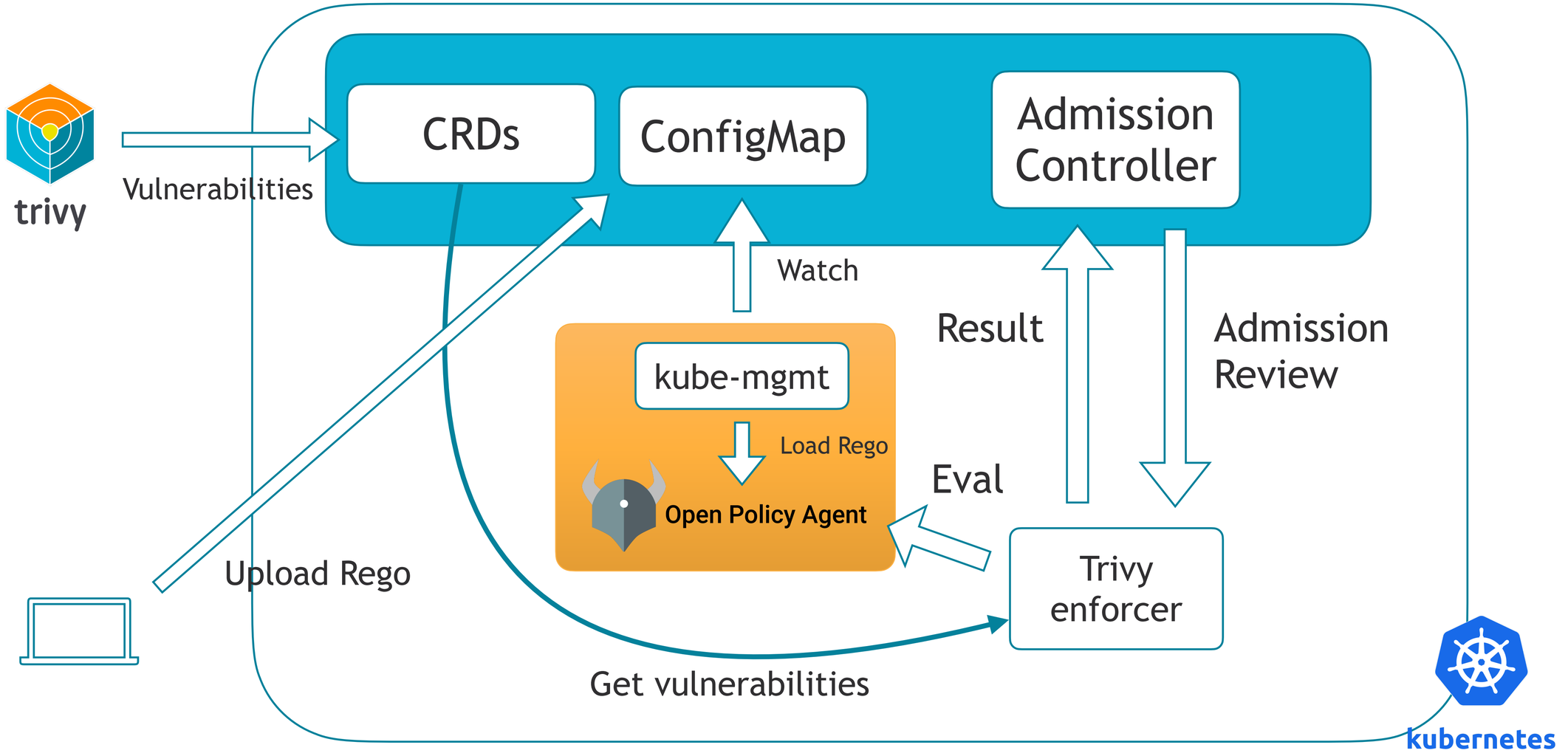


OPA Integration (not released yet)

- Standalone integration
  - Apply complicated rules to filter detected vulnerabilities
- Kubernetes integration
  - Run as Admission Controller and deny launching Pod with critical vulnerabilities

More details in KubeCon Europe 2020

Kubernetes integration



aqua

New Features

aqua

Harbor integration

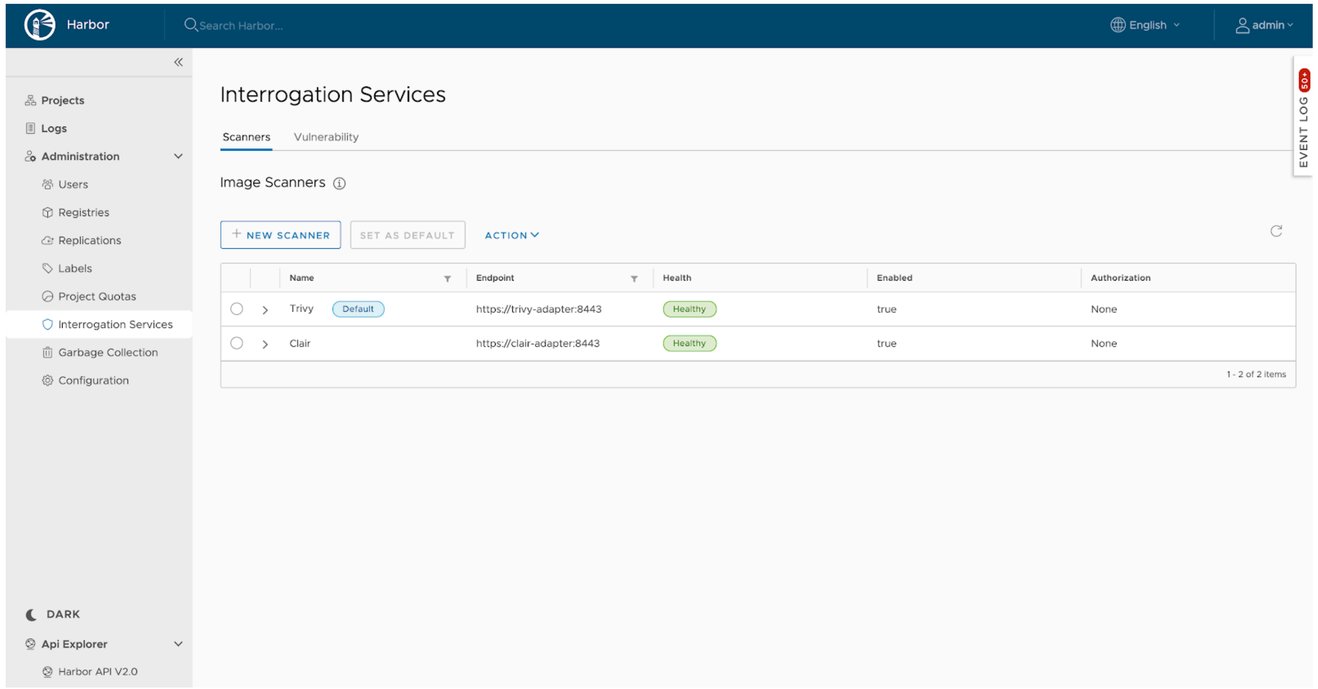
HARBOR

Search

Home Getting Start

Shipping Aqua Trivy as the default scanner

This release also replaces Clair with Aqua's Trivy as the default image scanner. Trivy takes container image scanning to higher levels of usability and performance than ever before. Since adding support for Trivy through our pluggable scanning framework in

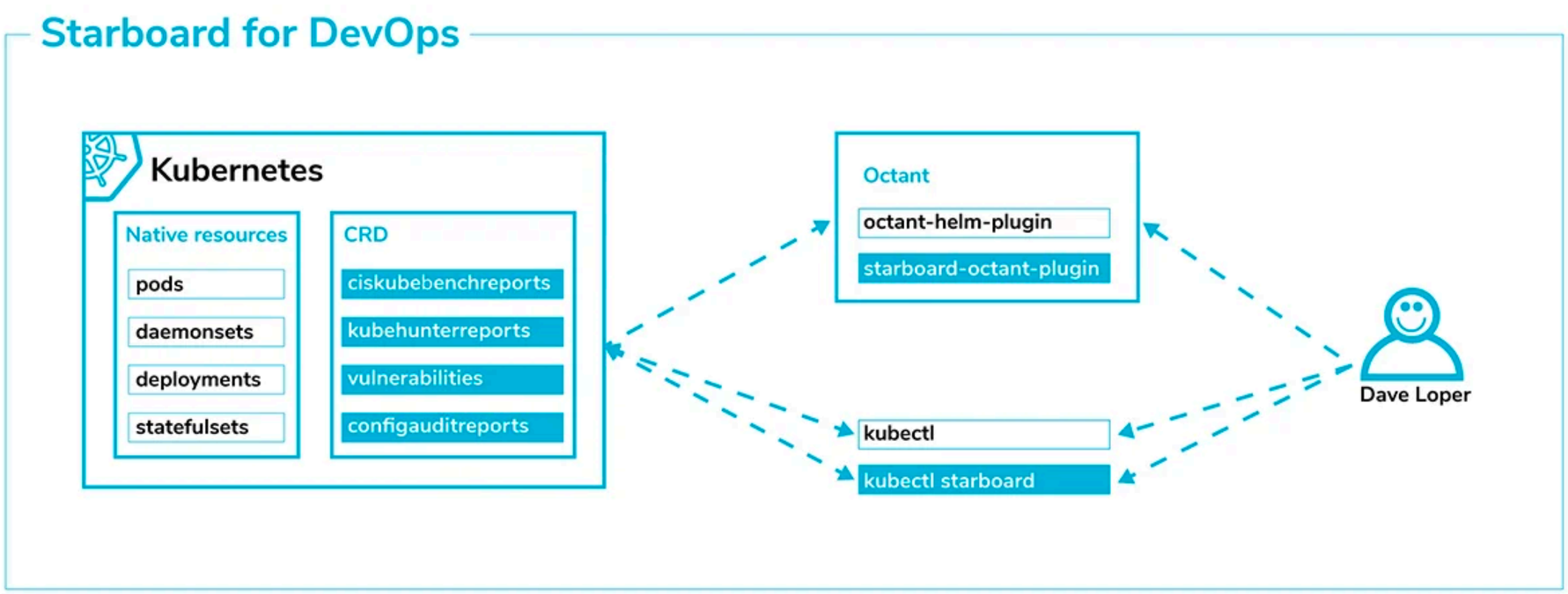


https://goharbor.io/blog/harbor-2.0/
https://www.cncf.io/webinars/harbor-the-trusted-cloud-native-registry-for-kubernetes/

aqua

Starboard

- Kubernetes-native security tool kit
  - Starboard integrates existing security tools into the Kubernetes environment



Starboard

https://github.com/aquasecurity/starboard
https://blog.aquasec.com/starboard-kubernetes-tools

aqua

Trivy

Open source scanner for ~~container images~~

Open source scanner for Artifacts

Support filesystem (v0.9.0)

Scan your project including a lock file with "filesystem" or "fs" subcommand

```
$ trivy fs /path/to/project

Pipfile.lock
============
Total: 9 (UNKNOWN: 1, LOW: 0, MEDIUM: 6, HIGH: 2, CRITICAL: 0)

+---------------------+------------------+----------+-------------------+-----------------------+-----------------------------------+
|       LIBRARY       | VULNERABILITY ID | SEVERITY | INSTALLED VERSION |     FIXED VERSION     |               TITLE               |
+---------------------+------------------+----------+-------------------+-----------------------+-----------------------------------+
| django              | CVE-2020-7471    | HIGH     | 2.0.9             | 3.0.3, 2.2.10, 1.11.28 | django: potential                 |
|                     |                  |          |                   |                       | SQL injection via                 |
|                     |                  |          |                   |                       | StringAgg(delimiter)              |
+                     +------------------+----------+                   +-----------------------+-----------------------------------+
|                     | CVE-2019-19844   | MEDIUM   |                   | 3.0.1, 2.2.9, 1.11.27 | Django: crafted email address     |
|                     |                  |          |                   |                       | allows account takeover           |
+---------------------+------------------+----------+-------------------+-----------------------+-----------------------------------+
```

aqua

Support filesystem (v0.9.0)

Scan the container image from inside the container, specifying "trivy fs /"

```
$ docker run -it alpine:3.10.2
/ # apk add curl
/ # curl -sfL https://raw.githubusercontent.com/aquasecurity/trivy/
master/contrib/install.sh | sh -s -- -b /usr/local/bin
/ # trivy fs /

3bee67d24f08 (alpine 3.10.2)
============================
Total: 5 (UNKNOWN: 0, LOW: 1, MEDIUM: 4, HIGH: 0, CRITICAL: 0)
```

Embed in Dockerfile (v0.9.0)

Scan the container image in Dockerfile

```
FROM alpine:3.7

RUN apk add curl \
    && curl -sfL https://raw.githubusercontent.com/aquasecurity/trivy/master/contrib/install.sh | sh -s -- -b /usr/local/bin \
    && trivy filesystem --exit-code 1 --no-progress /

$ docker build -t test .
...
Step 3/3 : RUN trivy filesystem --exit-code 1 --no-progress /
 ---> Running in 861287ea13cf

861287ea13cf (alpine 3.7.3)
============================
Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

...

The command '/bin/sh -c trivy filesystem --exit-code 1 --no-progress /' returned a non-zero code: 1
```

aqua

Support git repository (v0.9.0)

Scan a remote git repository with "repository" or "repo" subcommand

```
$ trivy repo https://github.com/aquasecurity/trivy-ci-test
Enumerating objects: 25, done.
Counting objects: 100% (25/25), done.
Compressing objects: 100% (18/18), done.
Total 25 (delta 4), reused 19 (delta 2), pack-reused 0

Pipfile.lock
============
Total: 9 (UNKNOWN: 1, LOW: 0, MEDIUM: 6, HIGH: 2, CRITICAL: 0)
```

Collaborate with the Aqua team

https://github.com/aquasecurity/trivy/issues

@AquaSecTeam

slack

slack.cncf.io
@liz @knqyf263
@simar

opensourceteam@aquasec.com

aqua

Thank you for your attention

aqua