
AWS
re:Invent

COM302

Vulnerability scanning for Kubernetes applications: Why and how

Liz Rice

VP Open Source Engineering

Aqua Security

AWS re:Invent

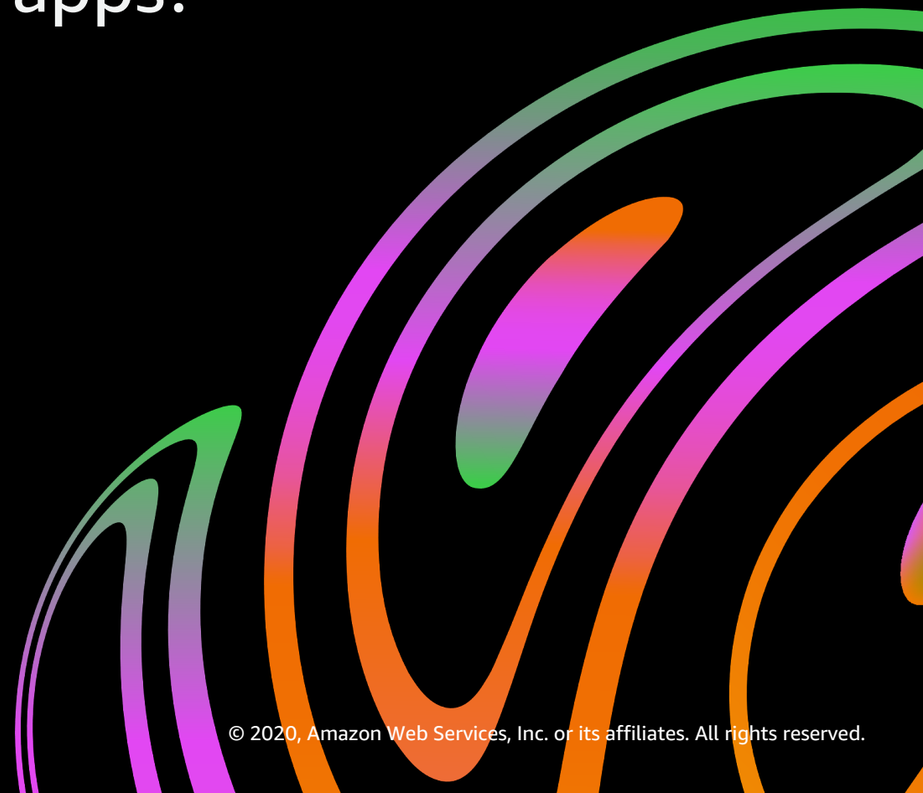
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Vulnerability scanning

What’s a vulnerability and why should you care?

What do container image scanners do?

How can you automate scanning for Kubernetes apps?



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

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.


MELTDOWN






DIRTY COW

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.

Example: CVE-2017-8807

NVD reports this in Varnish HTTP Cache versions 4.1.0–5.2.0

CVE-2017-8807 Detail

Current Description

vbf_stp_error in bin/varnishd/cache/cache_fetch.c in Varnish HTTP Cache 4.1.x before 4.1.9 and 5.x before 5.2.1 allows remote attackers to obtain sensitive information from process memory because a VFP_GetStorage buffer is larger than intended in certain circumstances involving -sfile Stevedore transient objects.

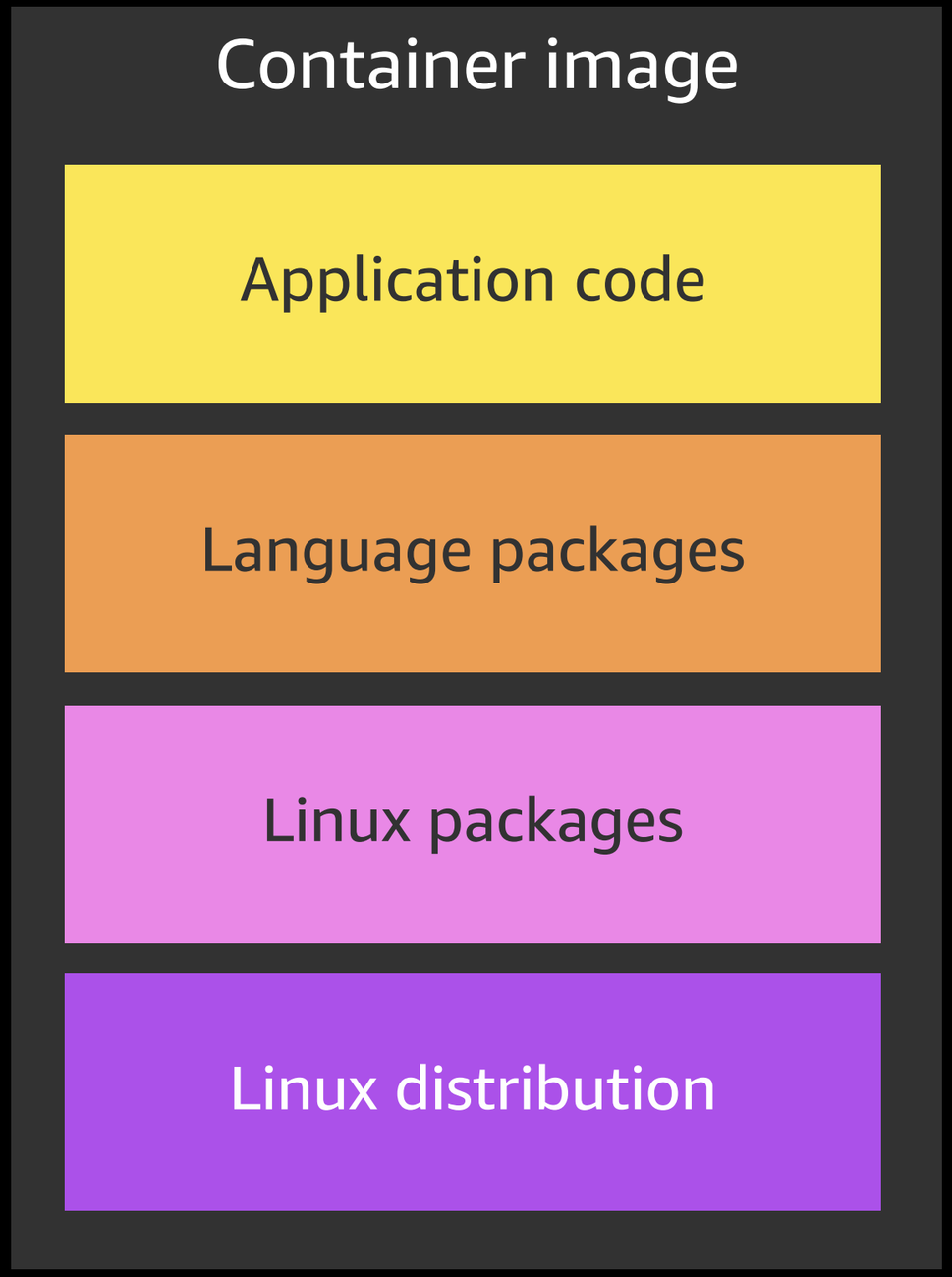
Example: CVE-2017-8807

Debian applied patch to version 5.0.0

Vulnerable and fixed packages

The table below lists information on source packages.

Source Package	Release	Version	Status
varnish (PTS)	wheezy, wheezy (security)	3.0.2-2+deb7u2	fixed
	jessie (security), jessie	4.0.2-1+deb8u1	fixed
	stretch (security), stretch	5.0.0-7+deb9u2	fixed
	sid	5.2.1-1	fixed



What packages are installed in this image?

Do these package versions have known vulnerabilities?

Language package management
npm, pip, dep, lock files, etc.

Package manager – apt, yum, apk, dpkg, etc.

Ubuntu, CentOS, RHEL, SUSE, Amazon Linux, Alpine, etc.

Example – Vulnerabilities in container images



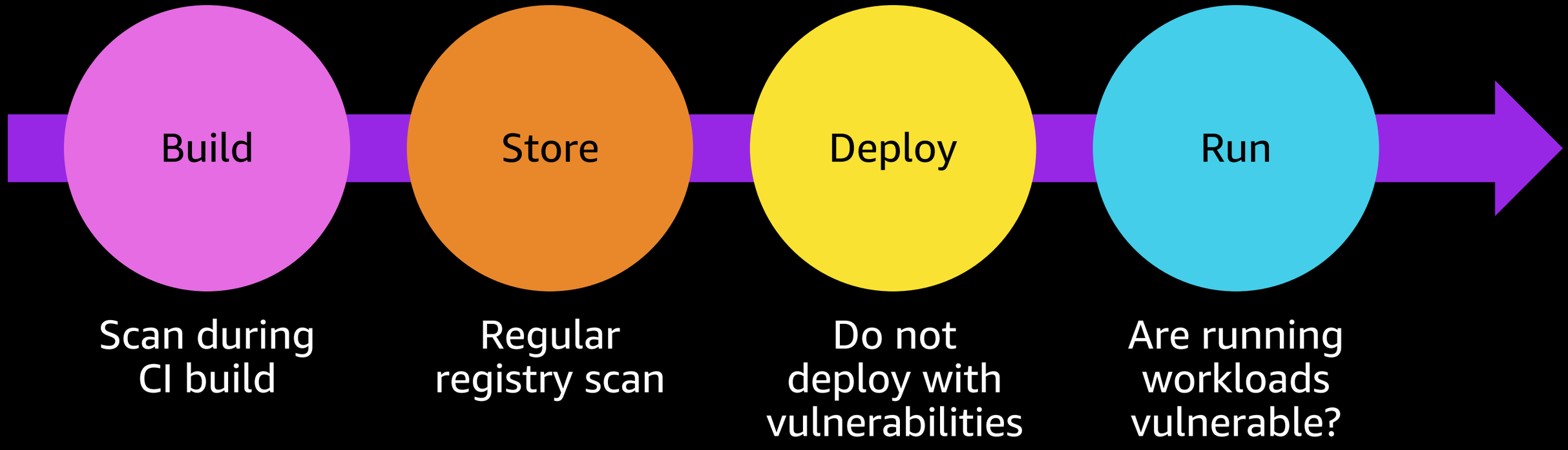
© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

```
~/w/reinvent ❯❯❯ trivy image nginx:1.16
2020-11-02T09:41:47.024Z        INFO    Need to update DB
2020-11-02T09:41:47.024Z        INFO    Downloading DB...
18.78 MiB / 18.78 MiB [-------------------------------------------------------------------------------------------------------] 100.00% 3.39 MiB p/s 6s
2020-11-02T09:41:56.538Z        INFO    Detecting Debian vulnerabilities...

nginx:1.16 (debian 10.3)
========================
Total: 132 (UNKNOWN: 0, LOW: 88, MEDIUM: 11, HIGH: 32, CRITICAL: 1)
```

LIBRARY	VULNERABILITY ID	SEVERITY	INSTALLED VERSION	FIXED VERSION	TITLE
apt	CVE-2020-3810	MEDIUM	1.8.2	1.8.2.1	Missing input validation in the ar/tar implementations of APT before version 2.1.2...
	CVE-2011-3374	LOW			It was found that apt-key in apt, all versions, do not correctly...
bash	CVE-2019-18276		5.0-4		bash: when effective UID is not equal to its real UID the...
	TEMP-0841856-B18BAF				
coreutils	CVE-2016-2781		8.30-3		coreutils: Non-privileged session can escape to the parent session in chroot
	CVE-2017-18018				coreutils: race condition vulnerability in chown and chgrp
gcc-8-base	CVE-2018-12886	HIGH	8.3.0-6		gcc: spilling of stack protection address in cfgexpand.c and function.c leads to...
	CVE-2019-15847				gcc: POWER9 "DARN" RNG intrinsic produces repeated

Scanning in the image lifecycle

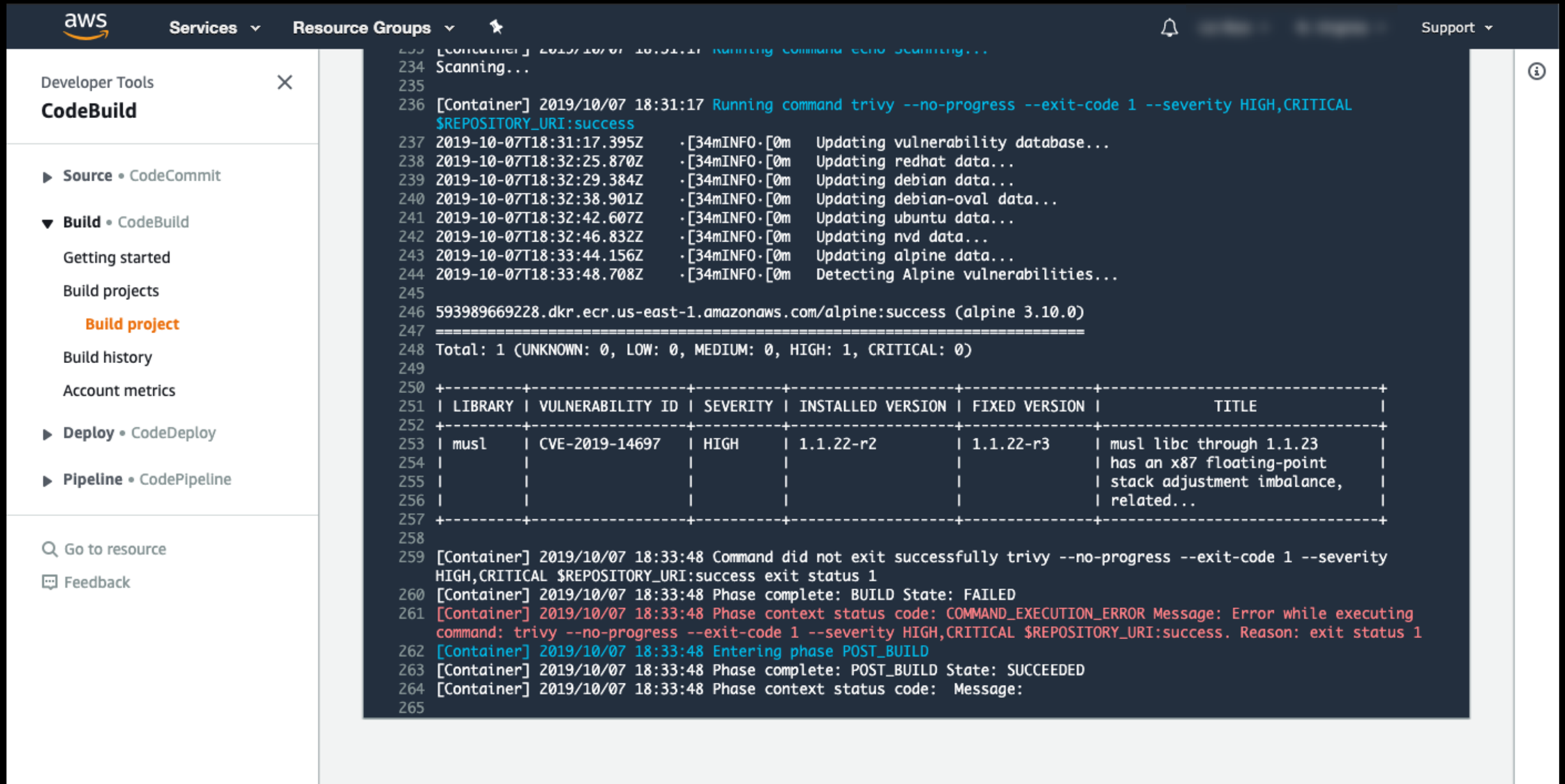


Scanning in the build



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

High-severity vulnerability fails the build



Scanning in the registry



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Overview



Critical	High	Medium	Low	Informational	Undefined
0	1	23	19	50	1

Vulnerabilities (94)

Find vulnerabilities

1

Name	Package	Severity	Description
CVE-2020-10878	perl:5.28.1-6	HIGH	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
CVE-2020-3810	apt:1.8.2	MEDIUM	Missing input validation in the ar/tar implementations of APT before version 2.1.2 could result in denial of service when processing specially crafted deb files.
CVE-2018-12886	gcc-8:8.3.0-6	MEDIUM	stack_protect_prologue in cfgexpand.c and stack_protect_epilogue in function.c in GNU Compiler Collection (GCC) 4.1 through 8 (under certain circumstances) generate instruction sequences when targeting ARM targets that spill the address of the stack protector guard, which allows an attacker to bypass the protection of -fstack-protector, -fstack-protector-all, -fstack-protector-strong, and -fstack-protector-explicit against stack overflow by controlling what the stack canary is compared against.

Result comparison

	Trivy	Clair
Critical	1	0
High	32	1
Medium	11	23
Low	88	19

Result comparison

libbsd0	CVE-2019-20367	CRITICAL	0.9.1-2

CVE-2019-20367	libbsd:0.9.1-2	MEDIUM	nlist.c in libbsd before 0.10.0 has an out-string table (strtab).

CVSS V2 / V3

CVE-2019-20367 Detail

Current Description

nlist.c in libbsd before 0.10.0 has an out-of-bounds read during a comparison for a symbol name from the string table (strtab).

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 9.1 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

CVSS V2 / V3

CVE-2019-20367 Detail

Current Description

nlist.c in libbsd before 0.10.0 has an out-of-bounds read during a comparison for a symbol name from the string table (strtab).

View Analysis Description

Severity

CVSS Version 3.x | CVSS Version 2.0

CVSS 2.0 Severity and Metrics:

NIST: NVD **Base Score:** 6.4 MEDIUM **Vector:** (AV:N/AC:L/Au:N/C:P/I:N/A:P)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

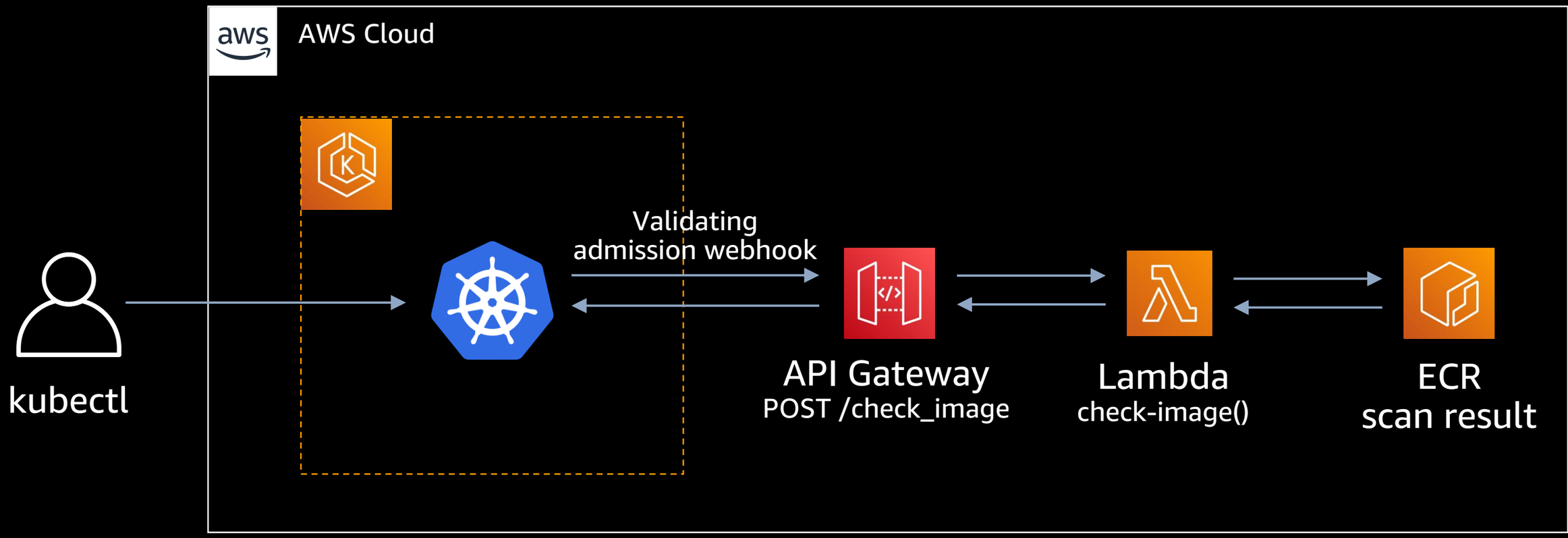
Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Scanning before deployment



© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Serverless admission webhooks for Kubernetes

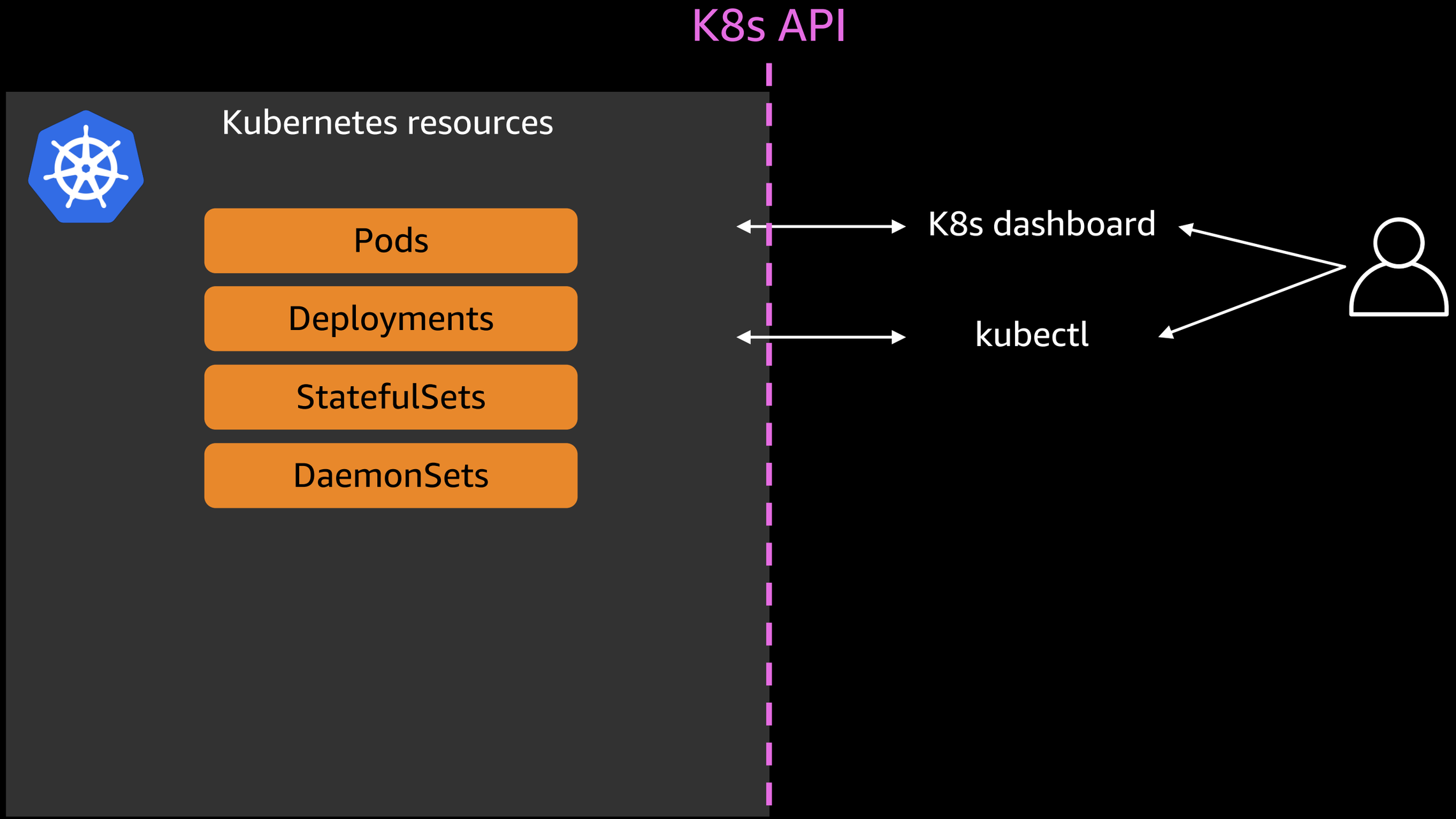


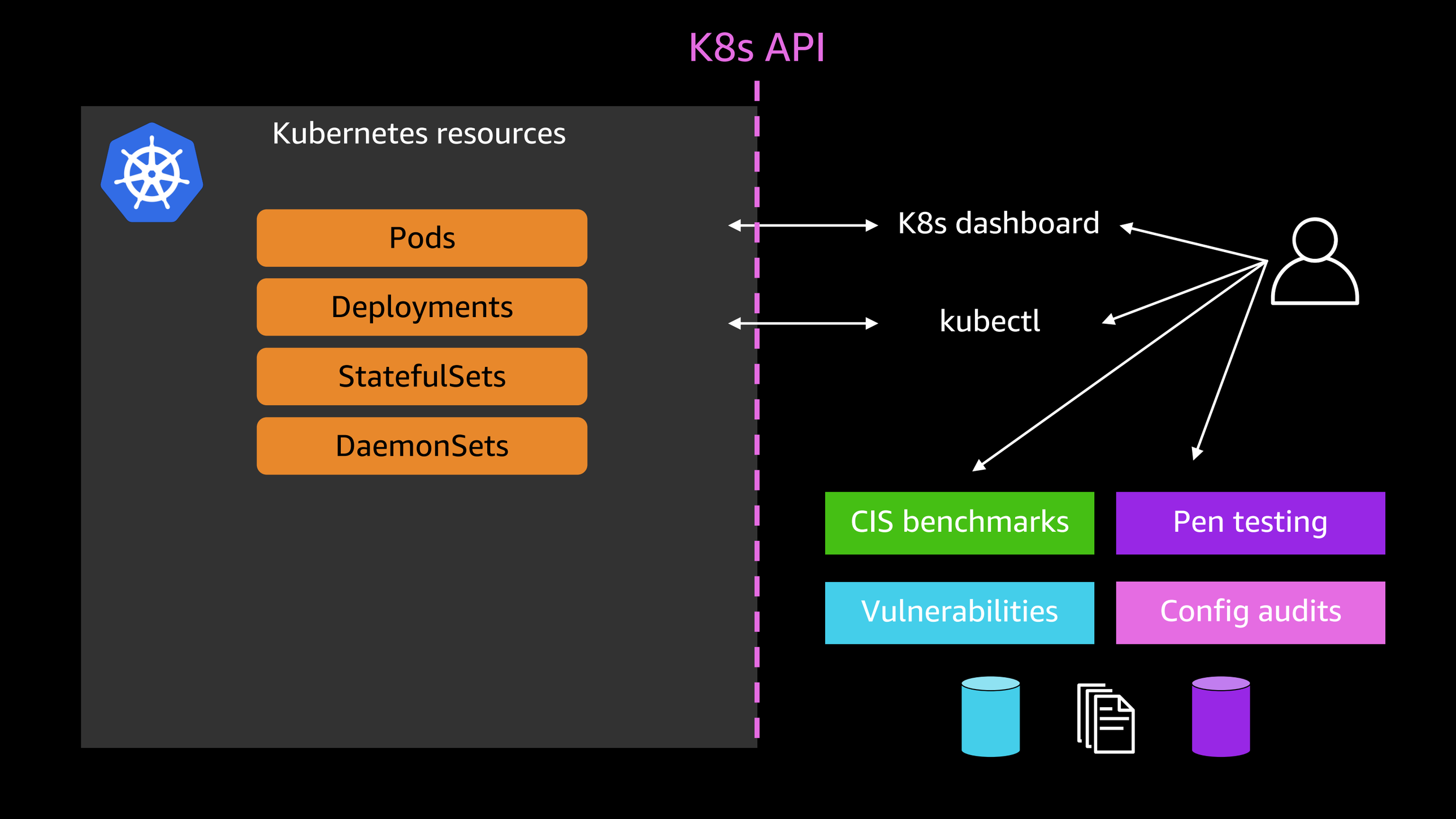
Vulnerabilities in running Kubernetes workloads

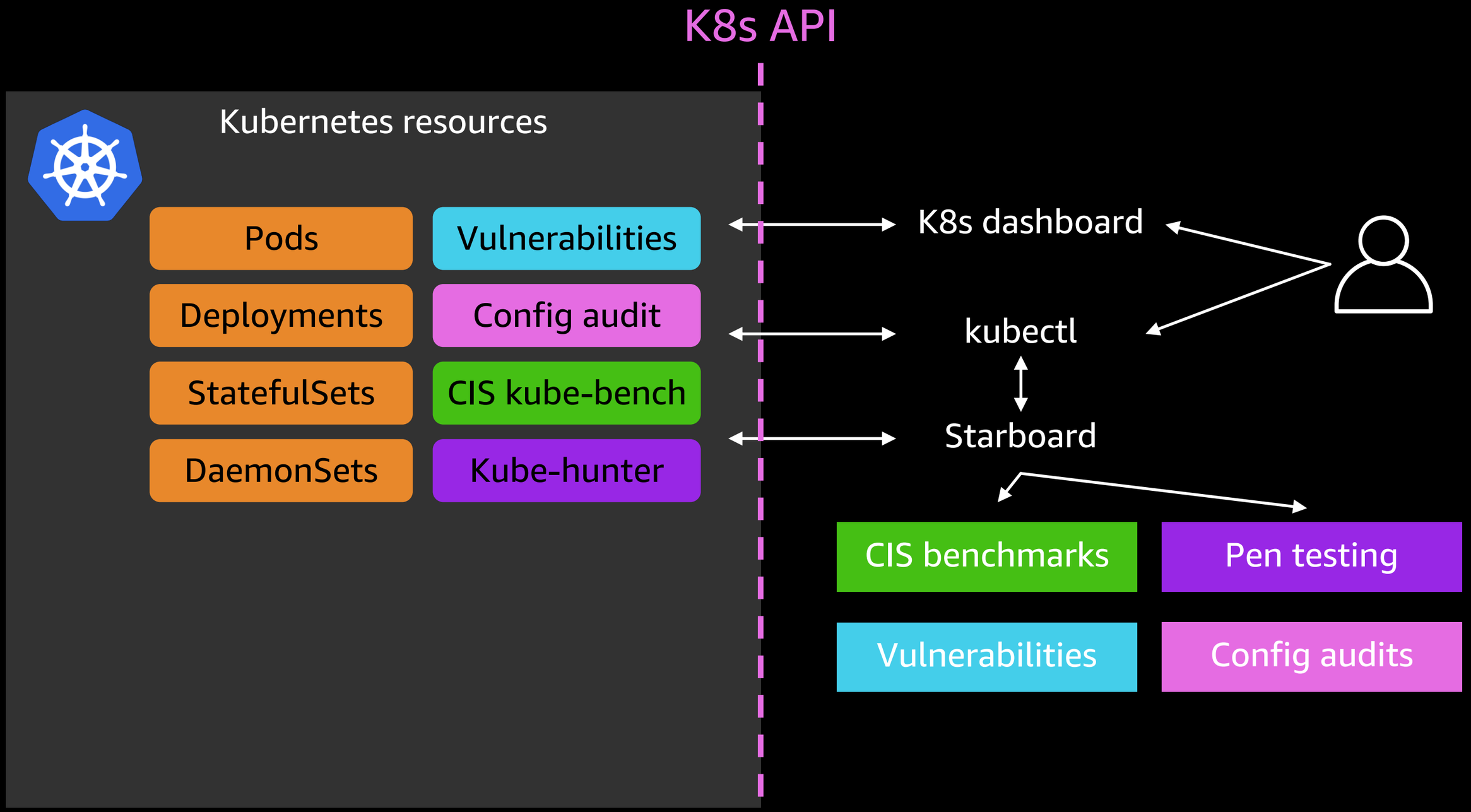


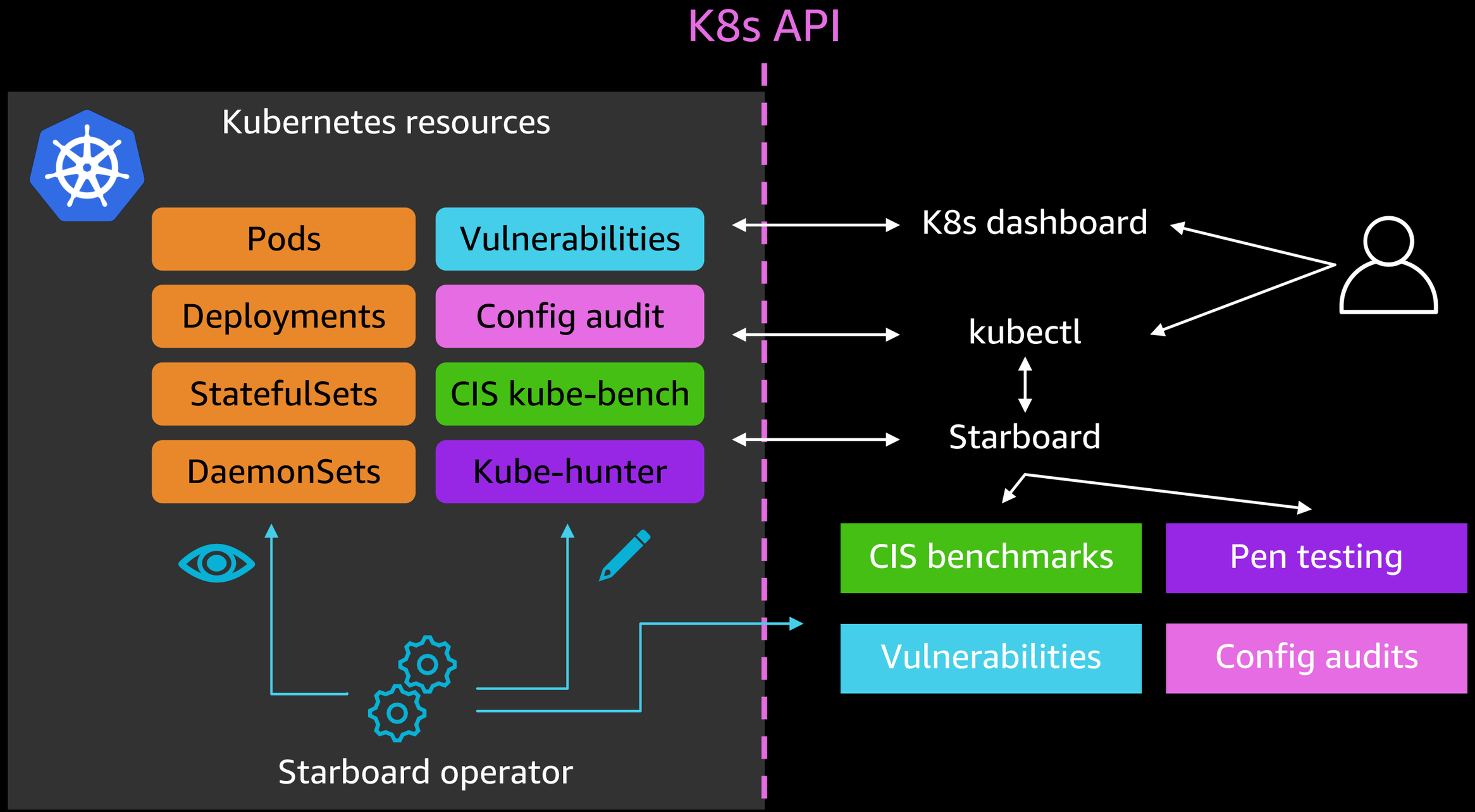
AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.

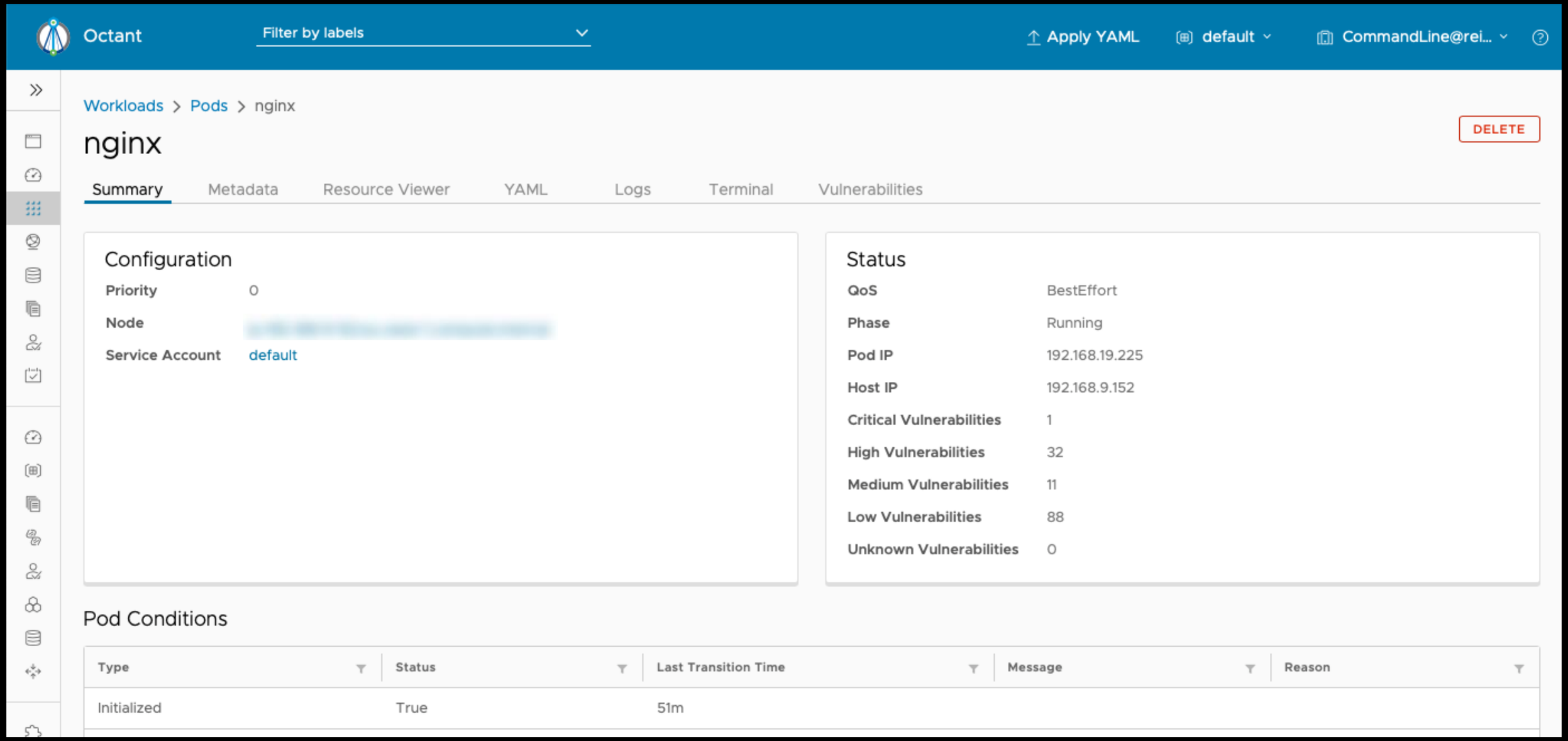

K8s API
Kubernetes resources
Pods
Deployments
StatefulSets
DaemonSets
K8s dashboard
kubectl


K8s API
Kubernetes resources
Pods
Deployments
StatefulSets
DaemonSets
K8s dashboard
kubectl
CIS benchmarks
Pen testing
Vulnerabilities
Config audits


K8s API
Kubernetes resources
Pods
Deployments
StatefulSets
DaemonSets
Vulnerabilities
Config audit
CIS kube-bench
Kube-hunter
K8s dashboard
kubectl
Starboard
CIS benchmarks
Pen testing
Vulnerabilities
Config audits


K8s API
Kubernetes resources
Pods
Deployments
StatefulSets
DaemonSets
Vulnerabilities
Config audit
CIS kube-bench
Kube-hunter
Starboard operator
K8s dashboard
kubectl
Starboard
CIS benchmarks
Pen testing
Vulnerabilities
Config audits

Vulnerability information in your K8s dashboard



How to pick a scanner

- **Does it support your Linux distribution?**
- **Does it support your programming language?**
- How frequently is the database updated?
- Ease of use
- Performance
- Integration with your workflow

Resources

Trivy

https://github.com/aquasecurity/trivy

Admission control webhook

https://aws.amazon.com/blogs/containers/building-serverless-admission-webhooks-for-kubernetes-with-aws-sam/

Starboard

https://operatorhub.io/operator/starboard-operator

https://artifacthub.io/packages/olm/community-operators/starboard-operator

Thank you!

Liz Rice

VP Open Source Engineering
Aqua Security
@lizrice

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Please complete the session survey

AWS re:Invent

© 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved.