



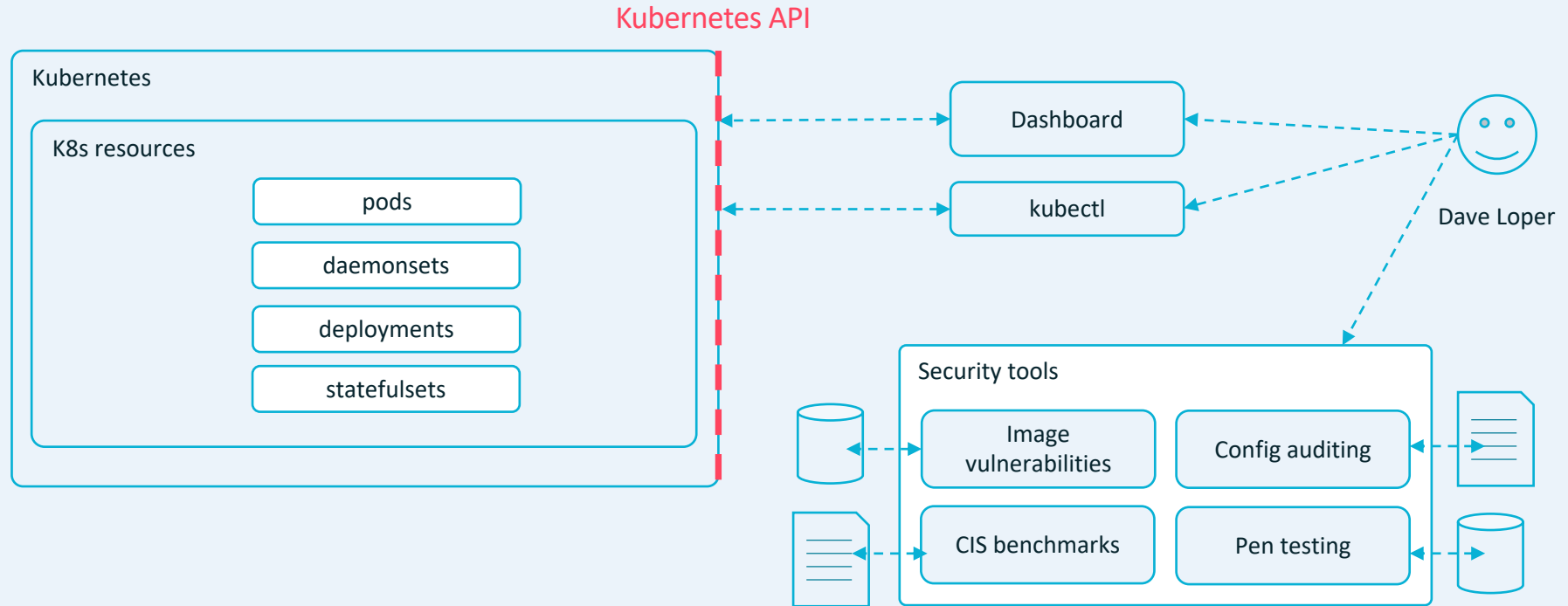
Kubernetes-native security with Starboard

Liz Rice & Daniel Pacak

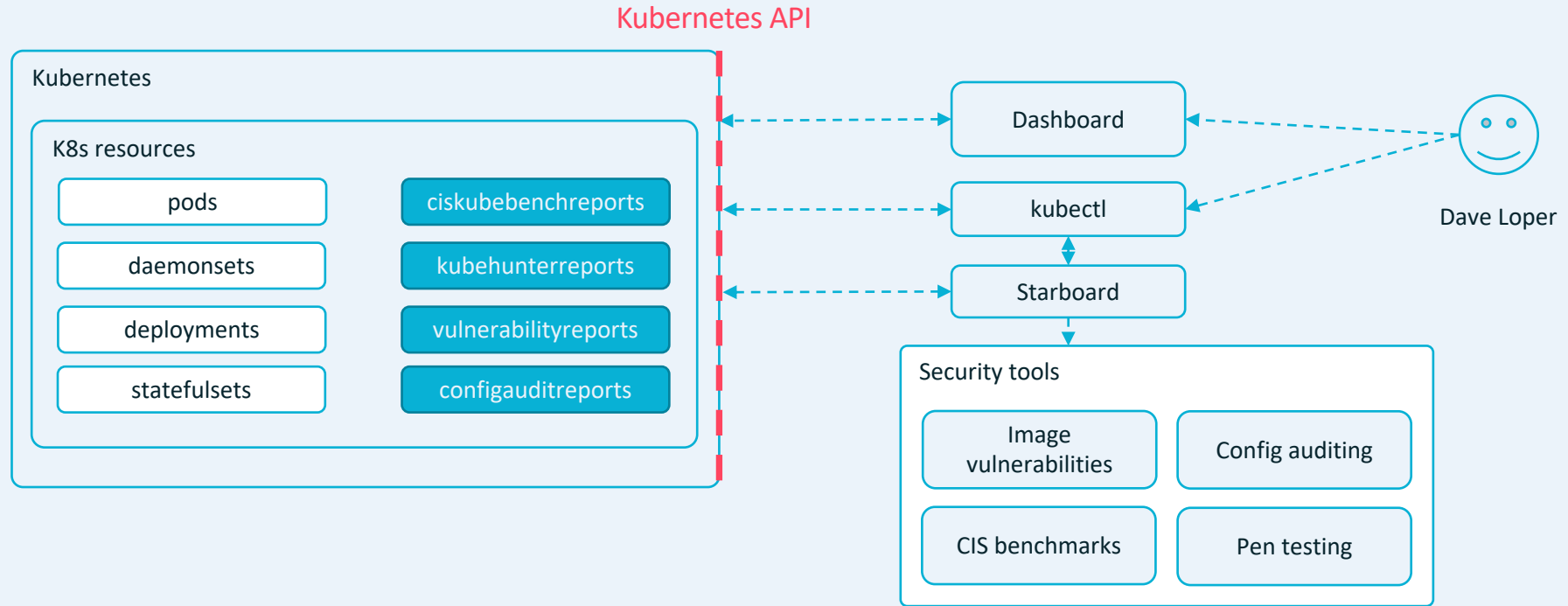
Open Source Engineering, Aqua Security

@lizrice @d_pacak

Starboard – motivation

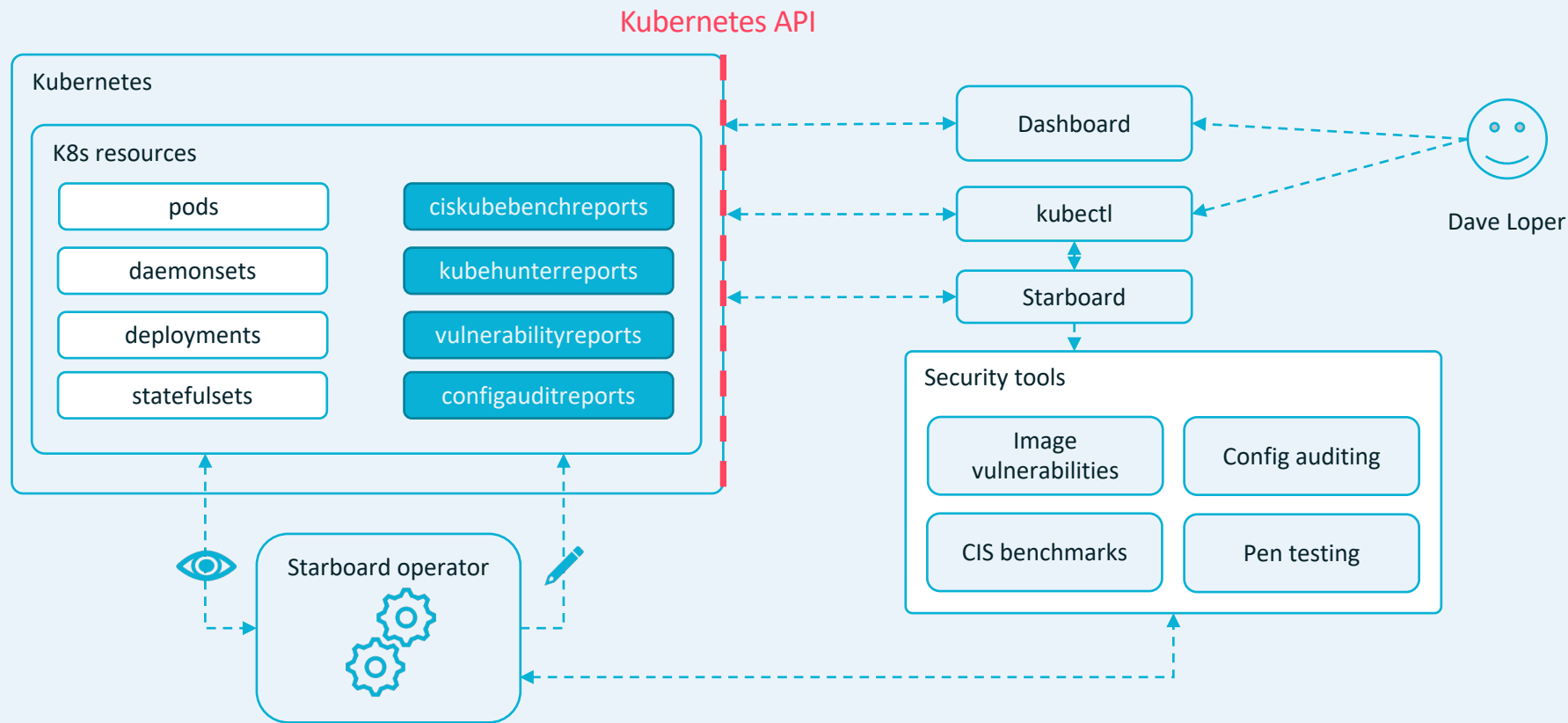


Starboard – brings security reports into Kubernetes



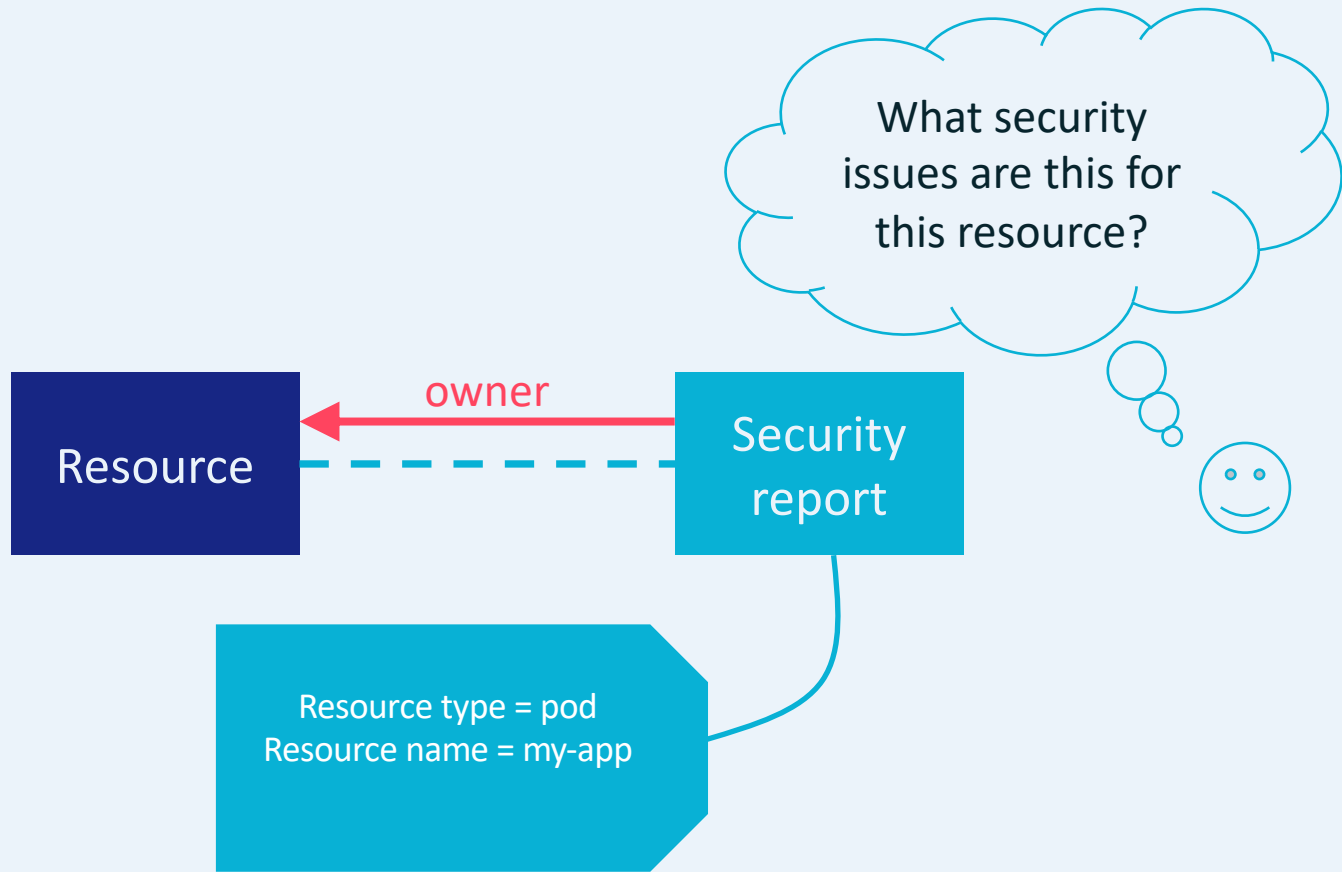
Starboard CLI demo

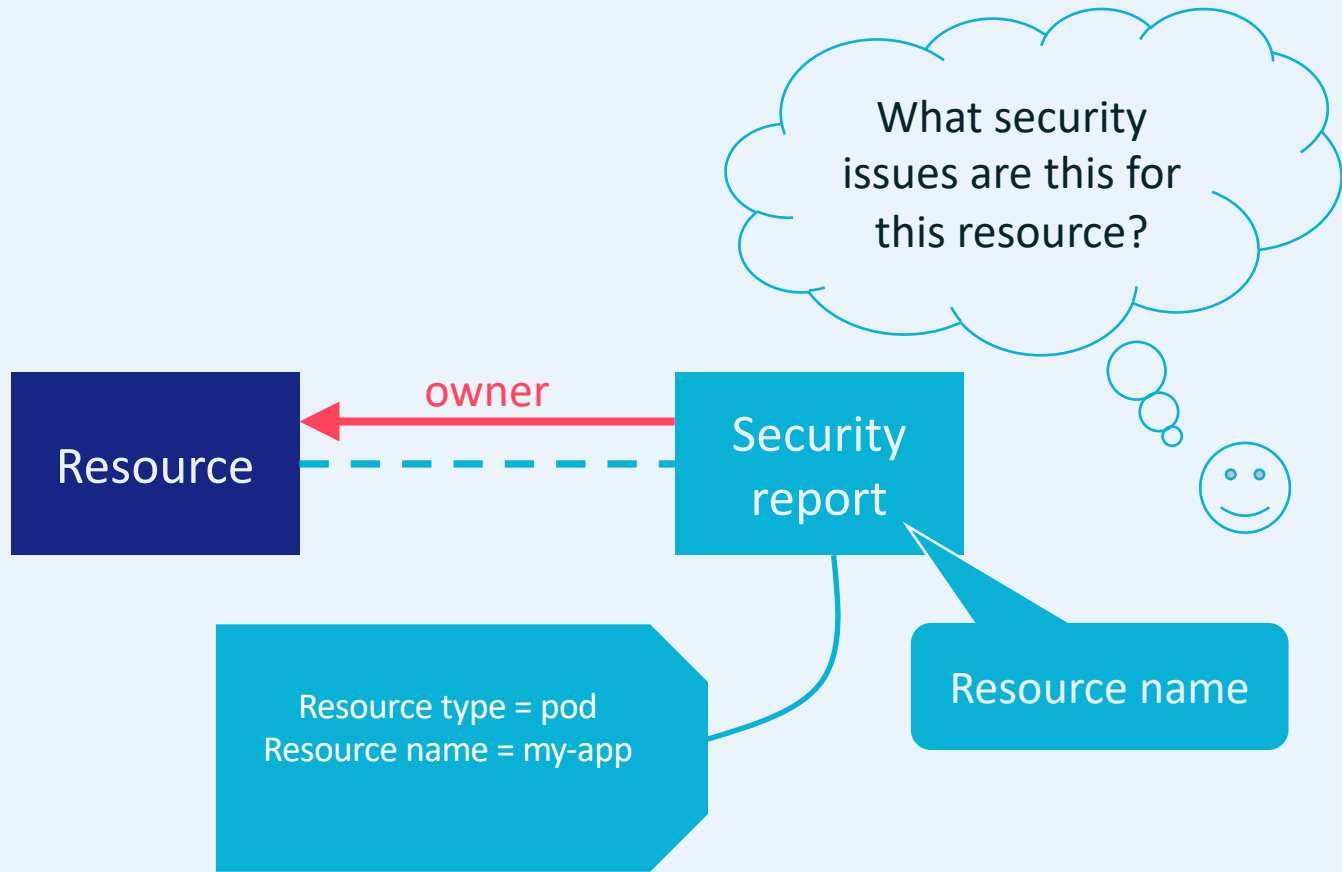
Starboard operator – automation



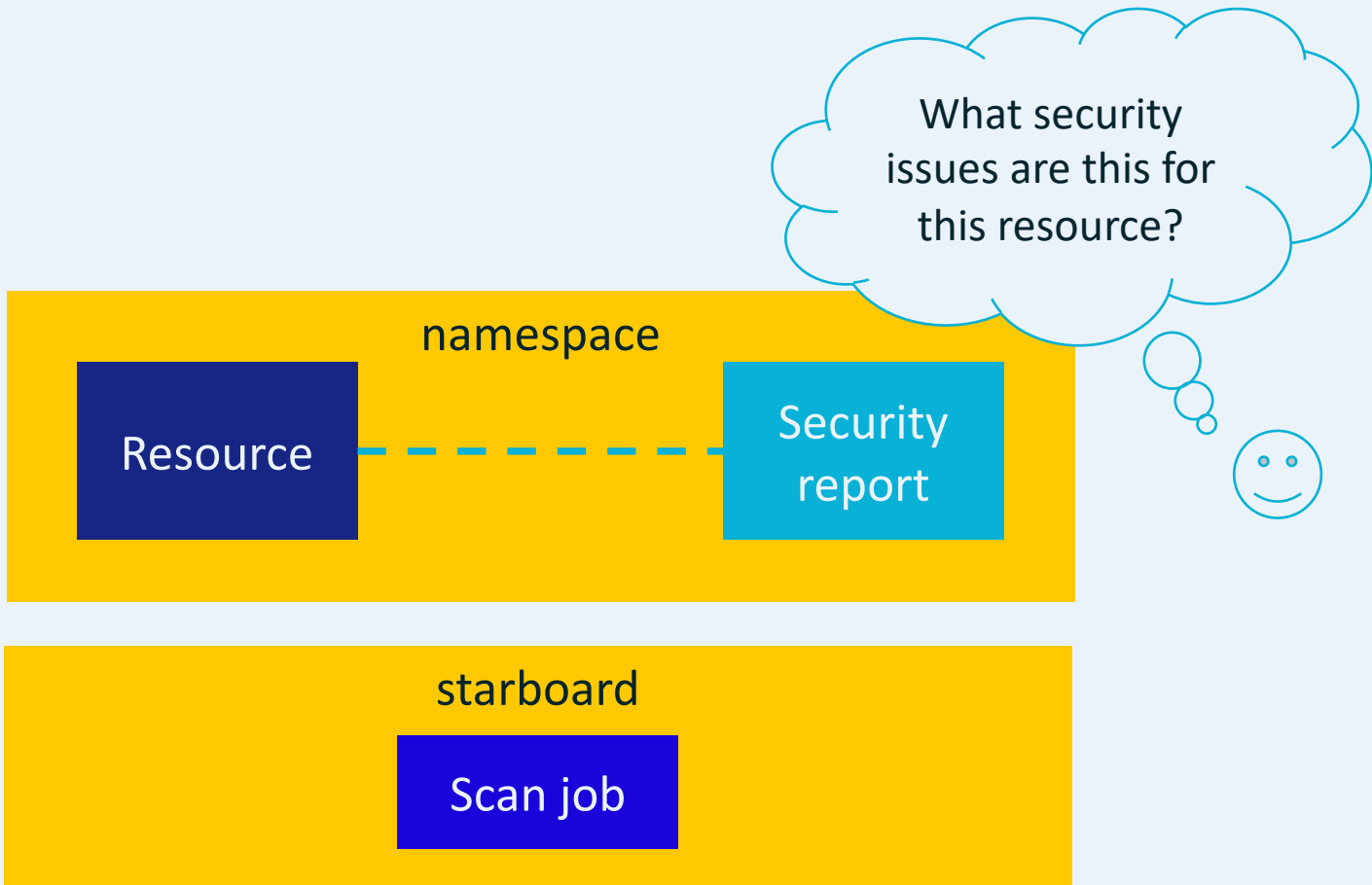
Starboard operator demo

Starboard design decisions









Unmanaged pod
other-image:2.0

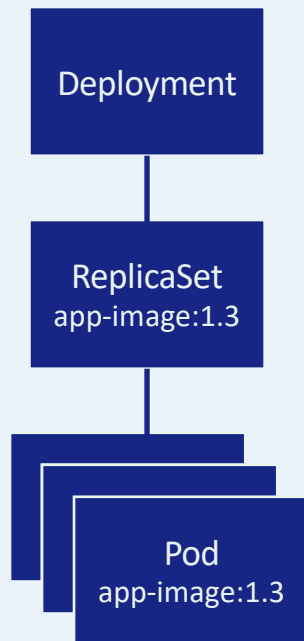
Deployment

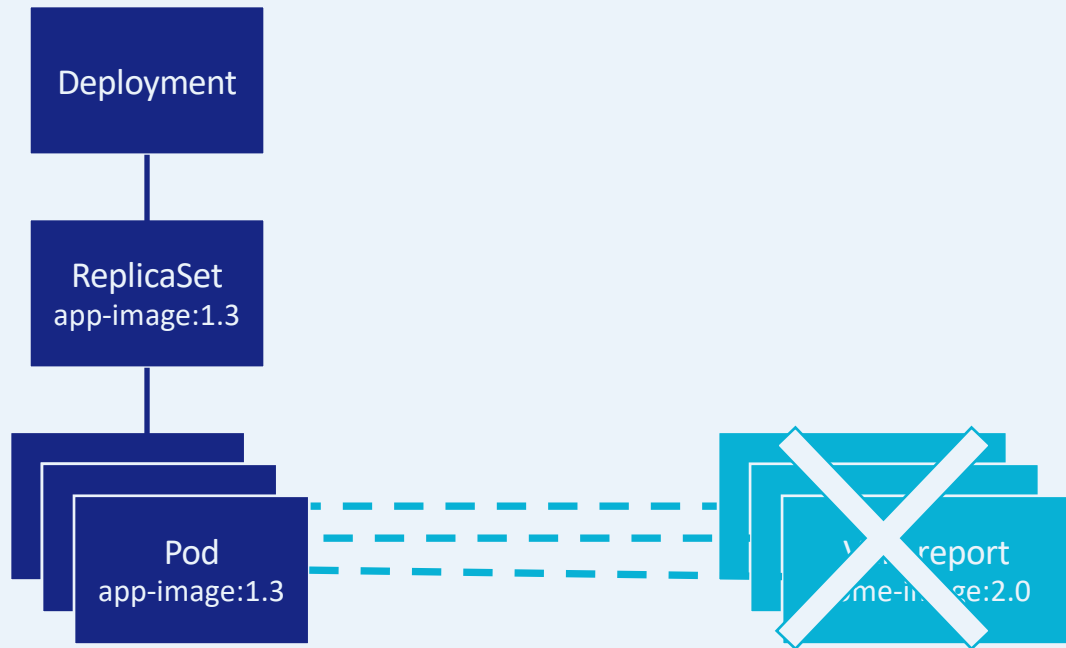
ReplicaSet
app-image:1.3

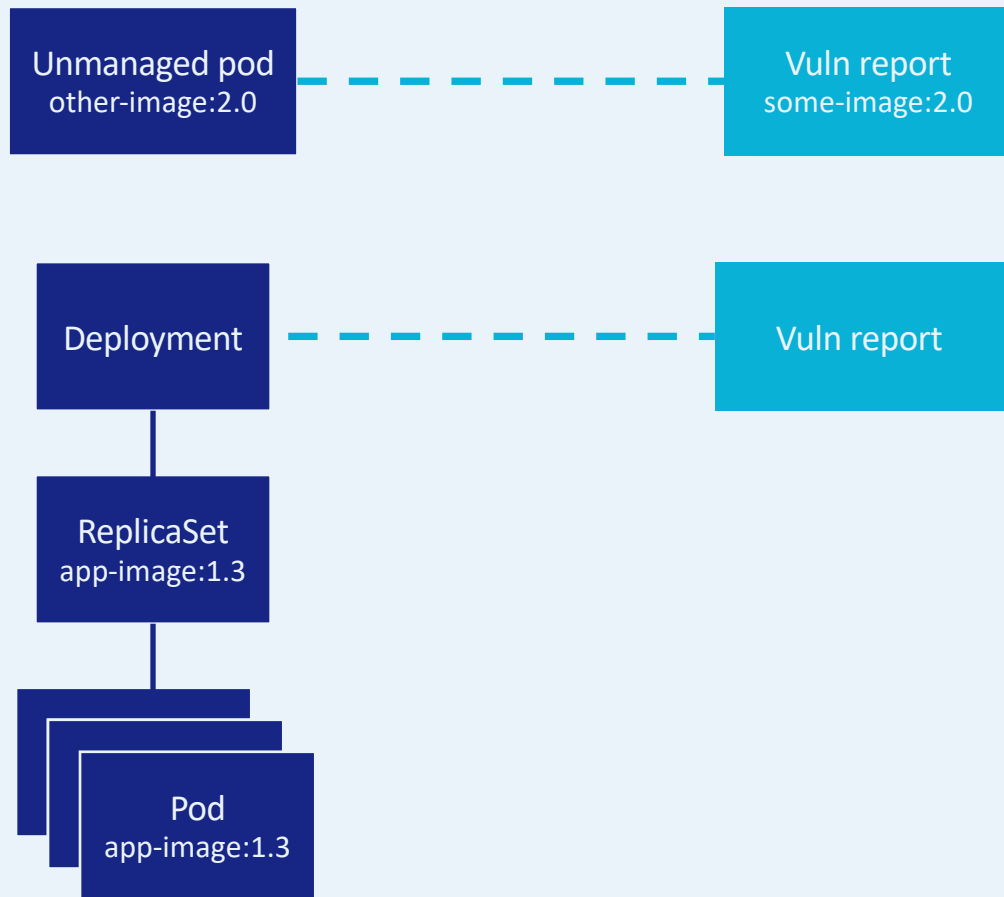
Pod
app-image:1.3

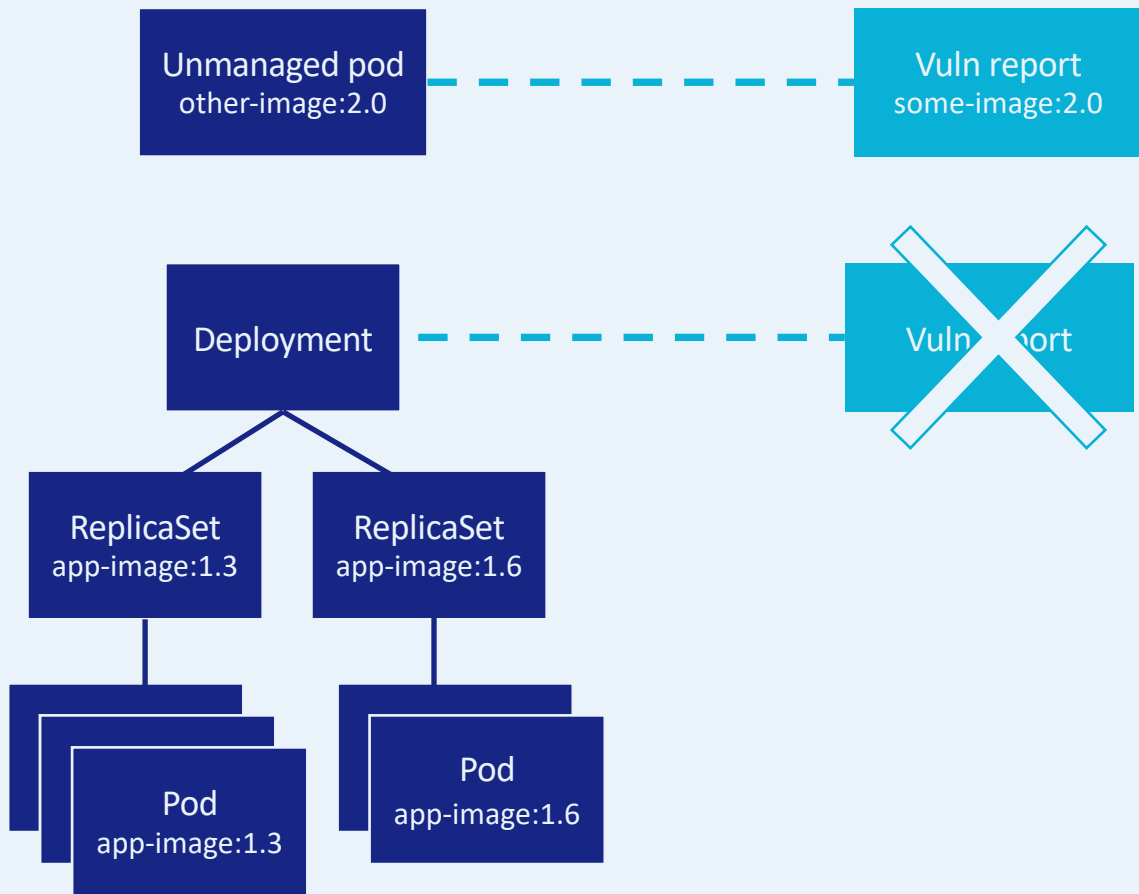
What security
issues are there
for my workloads?

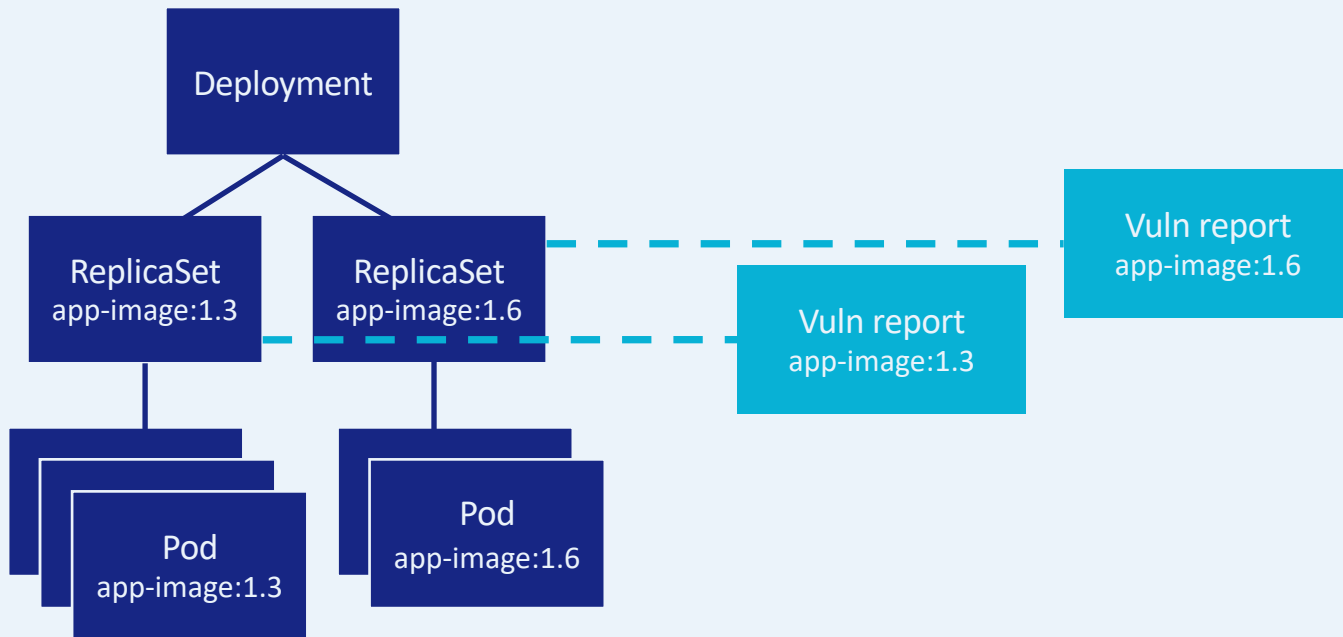


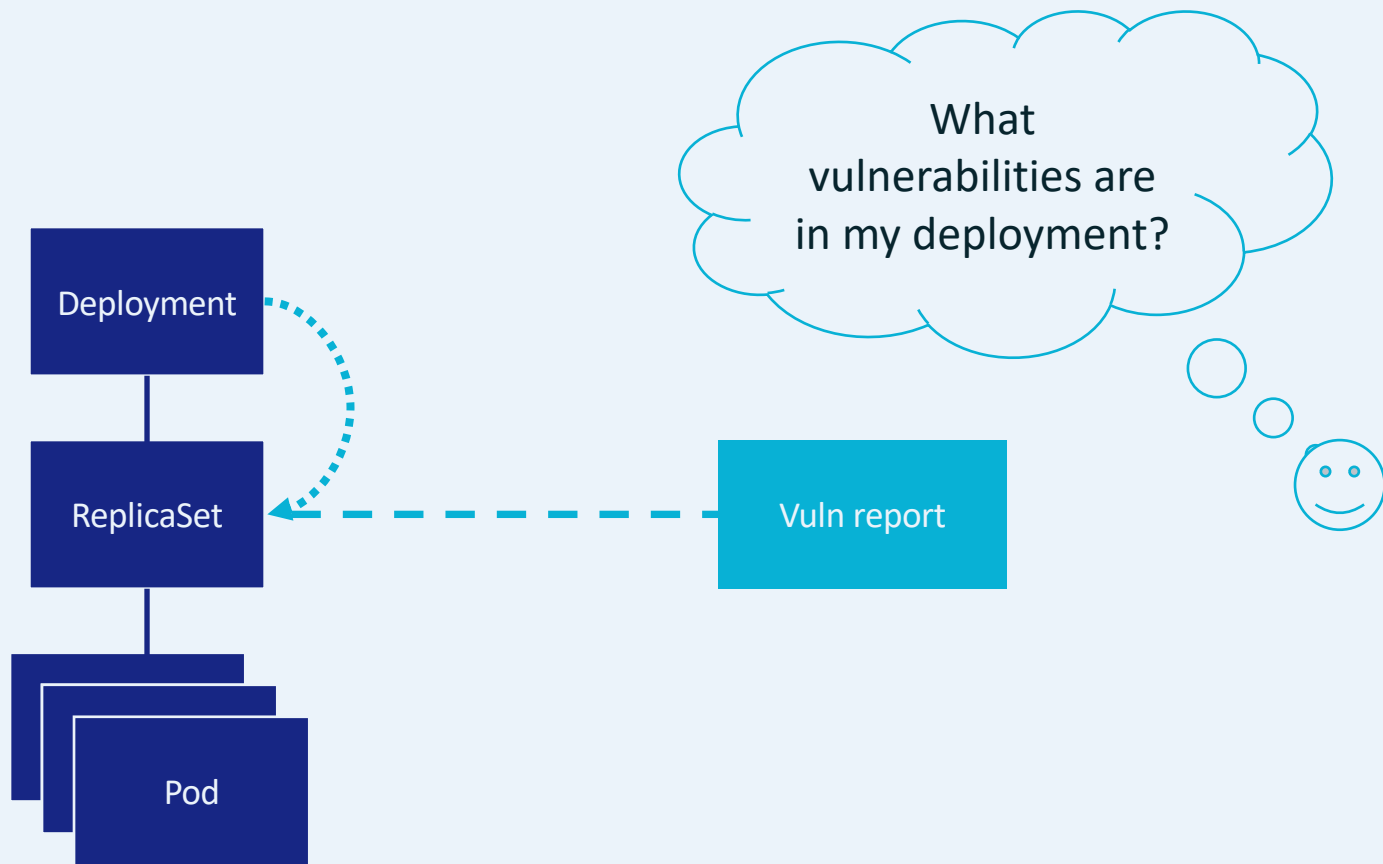








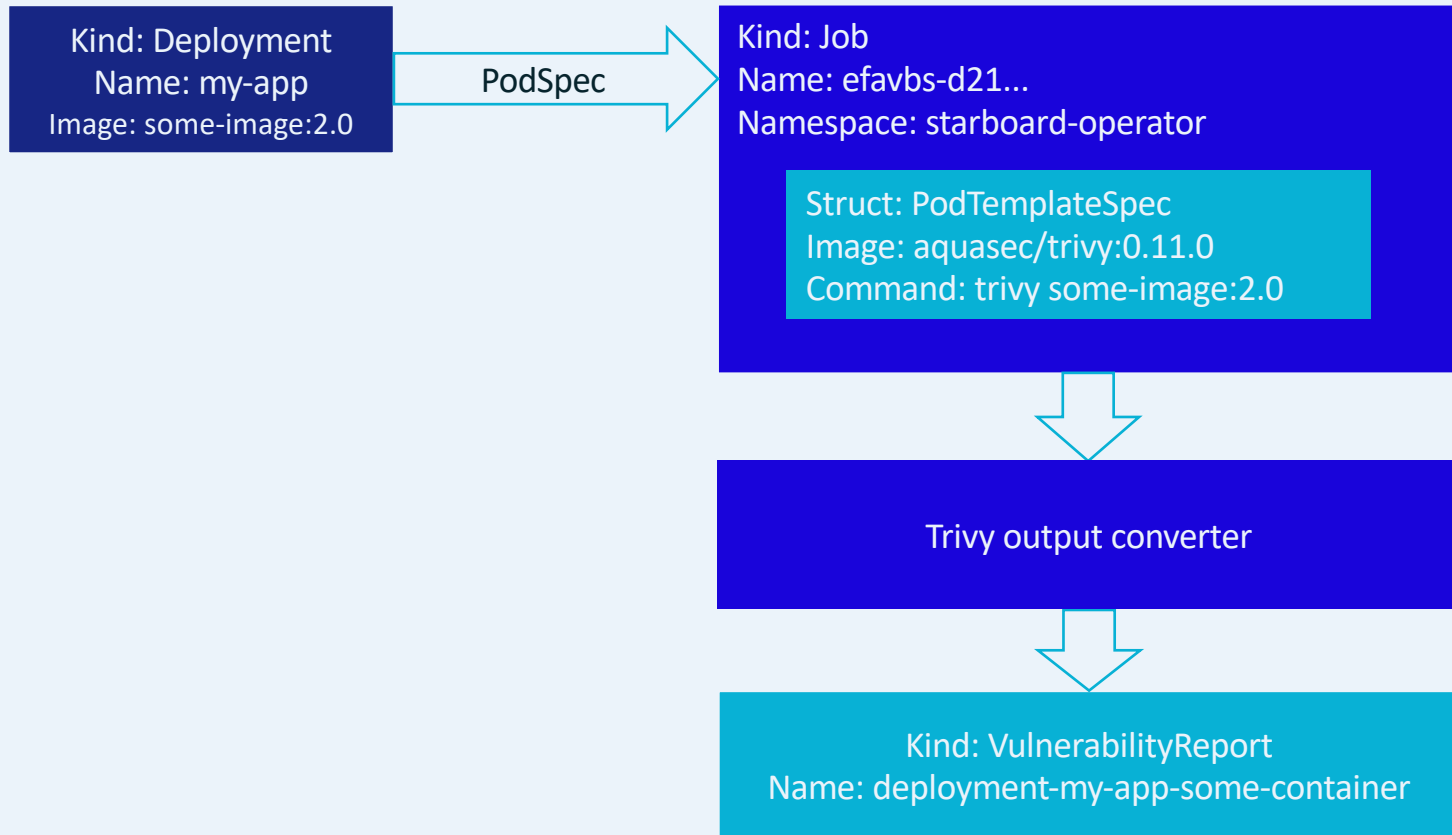




Starboard hierarchy demo

Extending Starboard

● Pluggable vulnerability scanners



VulnerabilityScanner interface

```
1 package scanner
2
3 import ...
4
11
12 type JobMeta struct {...}
13
17
18 // Options are arguments passed to the VulnerabilityScanner.GetPodTemplateSpec method.
19 type Options struct {
20     // Namespace the namespace to run the scan Job in.
21     Namespace string
22     // ServiceAccountName the name of the Service Account to run the Pod controlled by the scan Job.
23     ServiceAccountName string
24     // ScanJobTimeout scan job timeout.
25     ScanJobTimeout time.Duration
26 }
27
28 // VulnerabilityScanner defines methods implemented by vulnerability scanner vendors.
29 type VulnerabilityScanner interface {
30
31     // GetPodTemplateSpec describes the pod that will be created when executing a scan job
32     // for the specified pod descriptor.
33     GetPodTemplateSpec(spec corev1.PodSpec, options Options) (corev1.PodTemplateSpec, error)
34
35     // ParseVulnerabilityScanResult is a callback to parse and convert logs of the pod controlled
36     // by a scan job to the Starboard model.
37     ParseVulnerabilityScanResult(imageRef string, logsReader io.ReadCloser) (
38         v1alpha1.VulnerabilityScanResult, error)
39 }
```

Octant

Filter by labels

dev minikube

Items per page 10 1 - 2 of 2 items

Config Audit Reports

Report Metadata

Generated At 4h

Scanner

Name Polaris
Vendor Fairwinds
Version latest

Summary

error 30
warning 10

Pod Template

Success	ID	Severity	Category
true	hostIPCSet	error	Security
true	hostNetworkSet	warning	Networking
true	hostPIDSet	error	Security

Items per page 10 1 - 3 of 3 items

Container nginx

Success	ID	Severity	Category
false	cpuRequestsMissing	warning	Resources
true	dangerousCapabilities	error	Security
false	livenessProbeMissing	warning	Health Checks
false	runAsRootAllowed	warning	Security
false	cpuLimitsMissing	warning	Resources
true	hostPortSet	warning	Networking
true	insecureCapabilities	warning	Security
false	memoryRequestsMissing	warning	Resources
false	readinessProbeMissing	warning	Health Checks
true	runAsPrivileged	error	Security

Items per page 10 1 - 10 of 14 items 1 / 2

Pod Template app/nginx

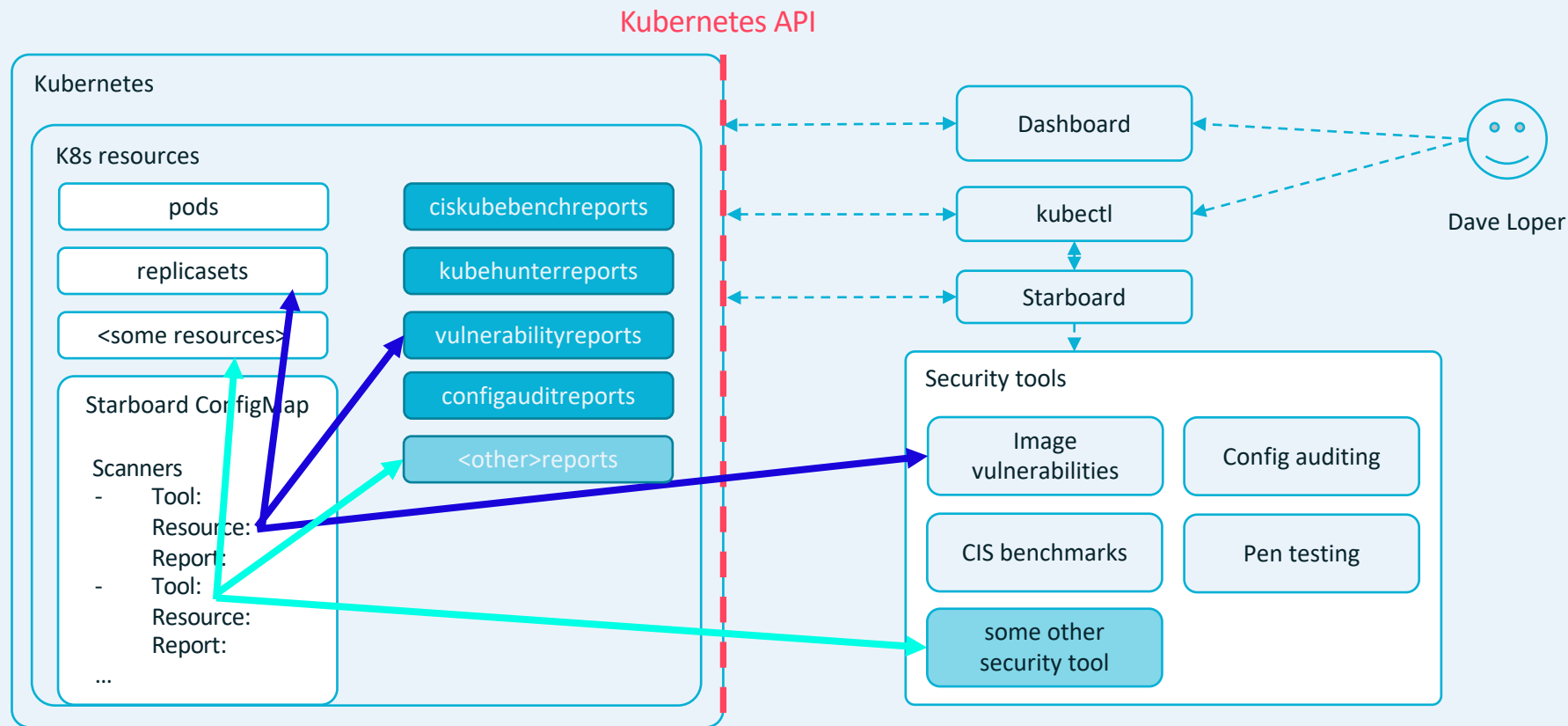
DARK


The screenshot shows the Lens Kubernetes dashboard interface. On the left is a sidebar with navigation icons for Cluster, Nodes, Workloads, Configuration, Network, Storage, Namespaces, Events, Apps, Access Control, and Custom Resources. The 'Custom Resources' menu is expanded, showing a list of definitions including aquasecurity.gi..., CISKubeBenchRe..., ConfigAuditReport, KubeHunterReport, and VulnerabilityReport. The main panel displays a table of 'Vulnerabilityreports' with one item: 'replicaset-wordpress...' in the 'default' namespace, from the 'library/wo' repository. A right-hand pane provides detailed information for this report.

VulnerabilityReport: replicaset-wordpress-6ff85b49b8-wordpress	
Created	1m ago (2020-10-21T10:10:39Z)
Name	replicaset-wordpress-6ff85b49b8-wordpress
Namespace	default
Labels	pod-spec-hash=68bf865d7d starboard.container.name=wordpress starboard.resource.kind=ReplicaSet starboard.resource.name=wordpress-6ff85b49b8 starboard.resource.namespace=default
Controlled By	ReplicaSet wordpress-6ff85b49b8
Repository	library/wordpress
Tag	4.9
Scanner	Trivy
Critical	91
High	294
Medium	290
Low	417
Unknown	0

Starboard future

Fully pluggable security reporting





What are the
most important
security issues in
my cluster?

`kubectl starboard summary <namespace>`

github.com/aquasecurity/starboard

@lizrice @d_pacak

