
KubeCon
CloudNativeCon
Europe 2023
TiKV

Canals and Bridges:
Using Amsterdam's Transit System to Secure K8s Networks

Cailyn Edwards
shopify

Who am I!?

Senior Infrastructure Security Engineer, CNCF Ambassador, SIG-Security and SIG-CLI Contributor
Farmer, Dog-mom, Squash Player, Sewist, (reluctant) Runner

Why this talk?

Agenda

01

The Metaphor

Quick history lesson and does the metaphor stick?

02

Get to Know the Network

What are we working with?!

03

Threat Model

Use the information to assess threats

04

Security Strategy

How should we tackle the issues discovered?

05

Key Takeaways

Basic steps when approaching a k8s network

Kubernetes Components

Cluster

A collection of nodes
This is what you get when you run k8s

Node

A worker machine (can be virtual or physical)

Pods

Smallest deployable execution units in k8s
Group of one or more containers

Control Plane

Made up of: api-server, etcd, kube-scheduler, controller-managers

CNI Plugin

Configures the network
Different options with different plugins

Ingress/Egress

What traffic moves in and out of the cluster.

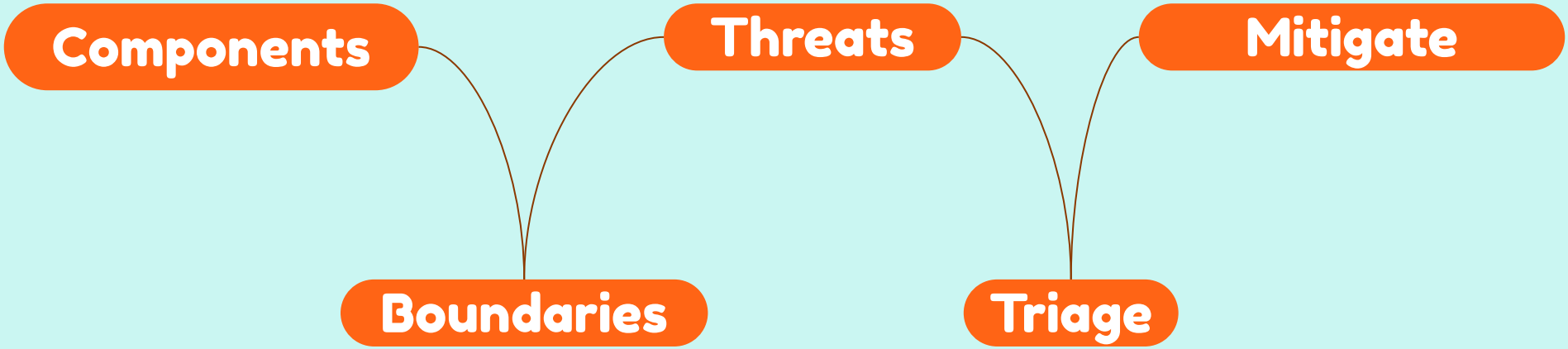
Kubernetes Network Model

Pods can communicate with all other pods on any other node without network address translation

Agents on a node can communicate with all pods on that node

Barring intentional segmentation via network policies

Evaluating the Security of a Kubernetes Network



01

Canals and Bridges

>100 km

Total Length of Canals

1,753

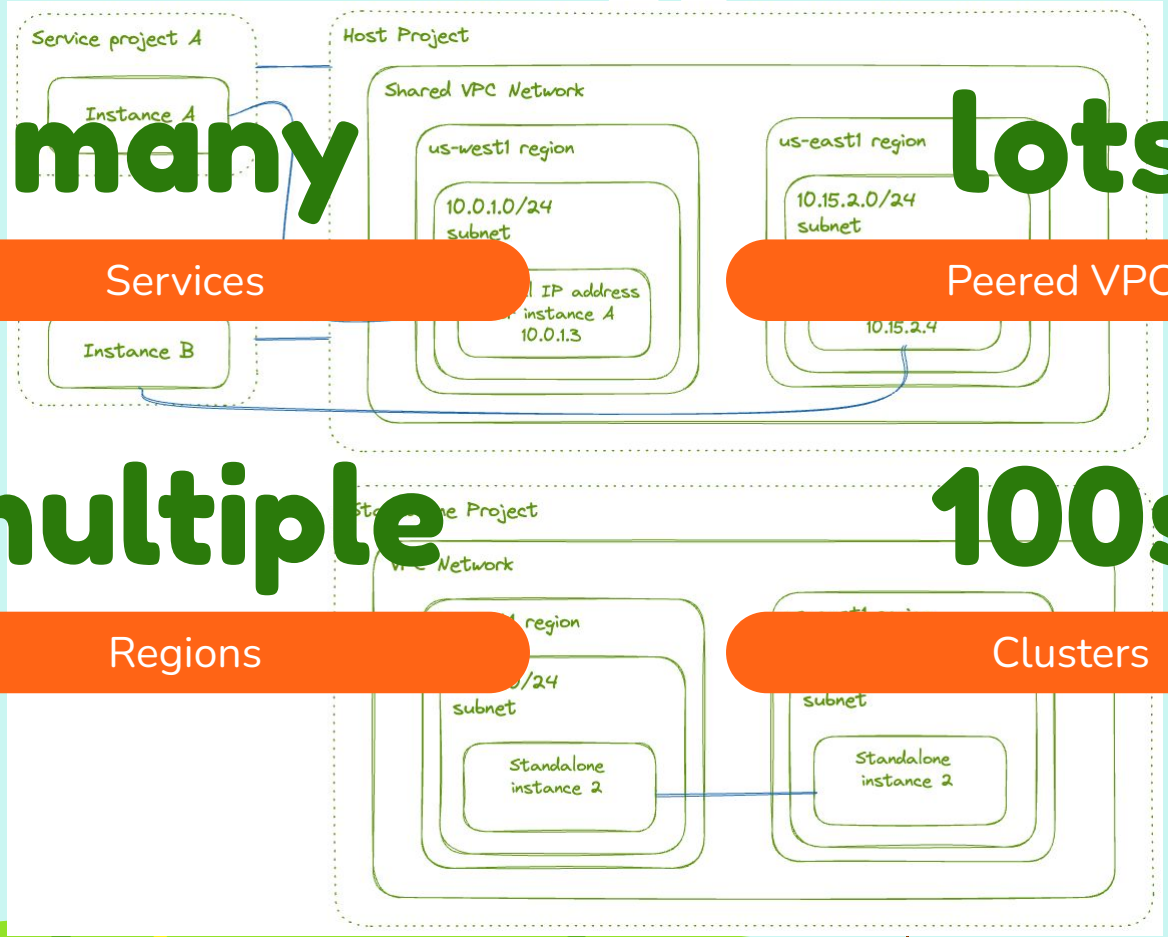
Bridges

>160

Canals

90

“Islands” Within the City



many

Services

lots

Peered VPCs

multiple

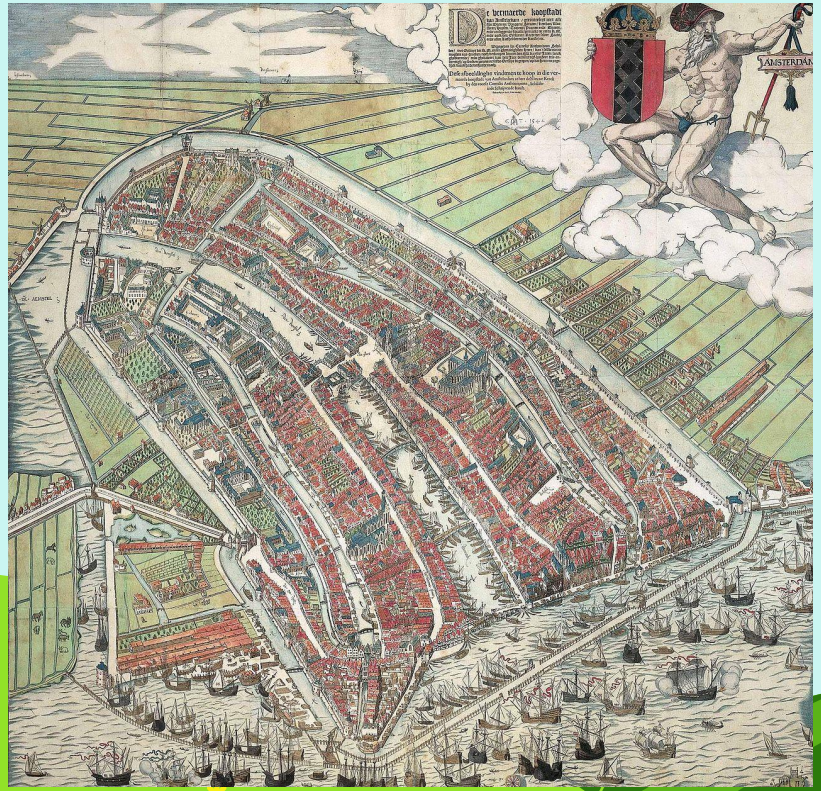
Regions

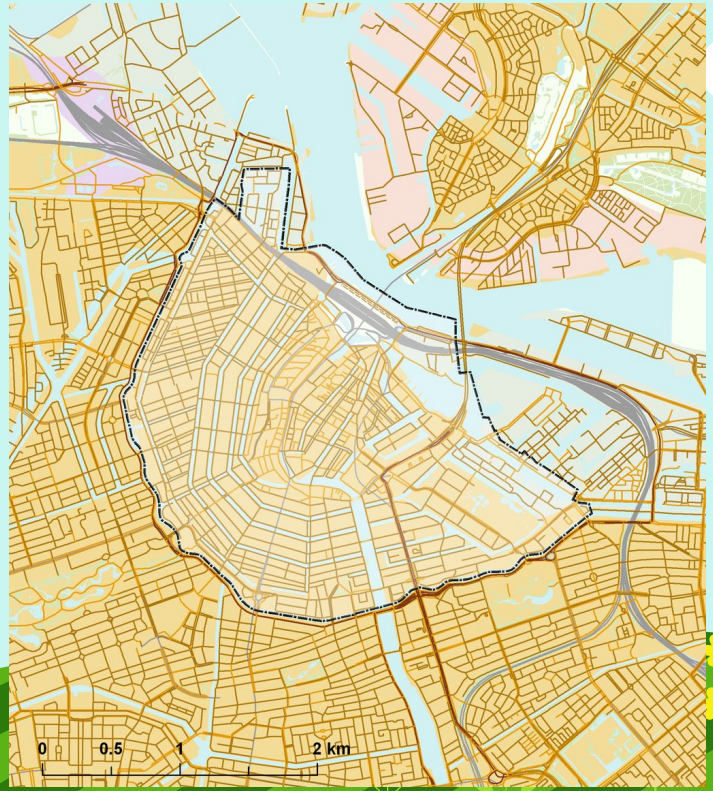
100s

Clusters

Singel and Singelgracht Canals

Canals used for perimeter defence





Firewalls and Observability

We must stand guard against unwanted traffic entering or exiting our infrastructure

It is also important to take time to understand the necessary and expected traffic

Grachtengordel

Canal Belt

Defence in Depth

Zero Trust Network

Layers of Protection

- IAM/RBAC
- Just in Time Access
- NetworkPolicy
- Observability
- Data Encryption
- Secret Management
- Patched/Supported Software

Bridges!

Amsterdam has many bridges that connect the city and control access to various sections

Access Control and Load Balancing!

There are many ways to ensure access is limited to those who need it, for only as long as they need it

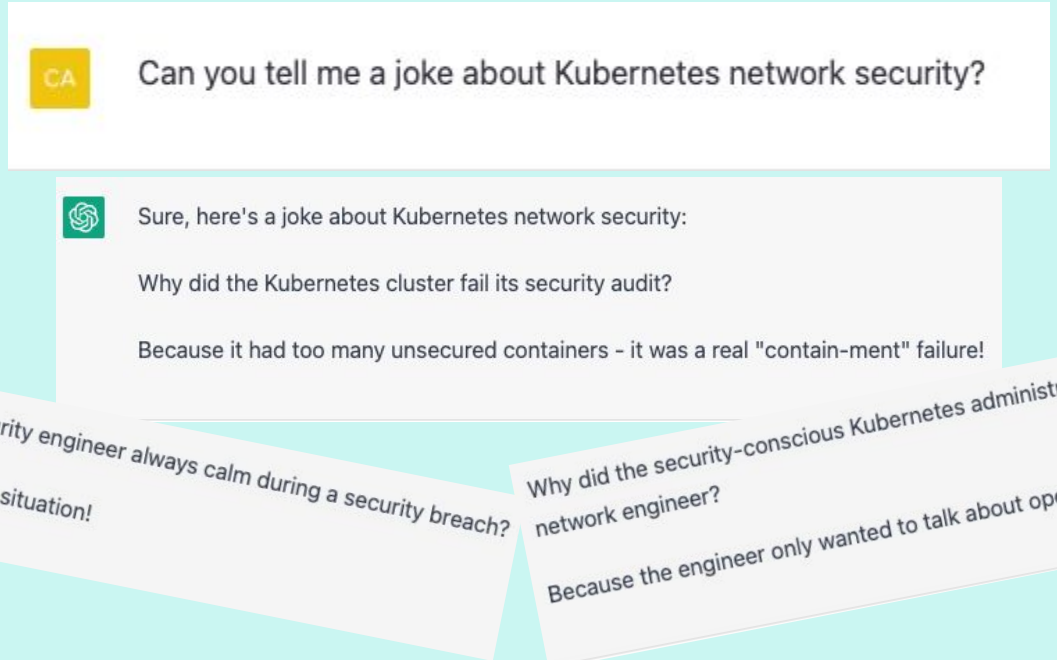
OK Cailyn - we get it the metaphor is awesome

Can we move on?

Amsterdam	Kubernetes
Different Licence Classes for Canal Use	Network Policies, more Access Control
Flooding the Waterline	Default Deny Network Policy
Canal/Bridge Maintenance	Up to Date Software, Regular Security Assessments

02

Getting to Know a Network



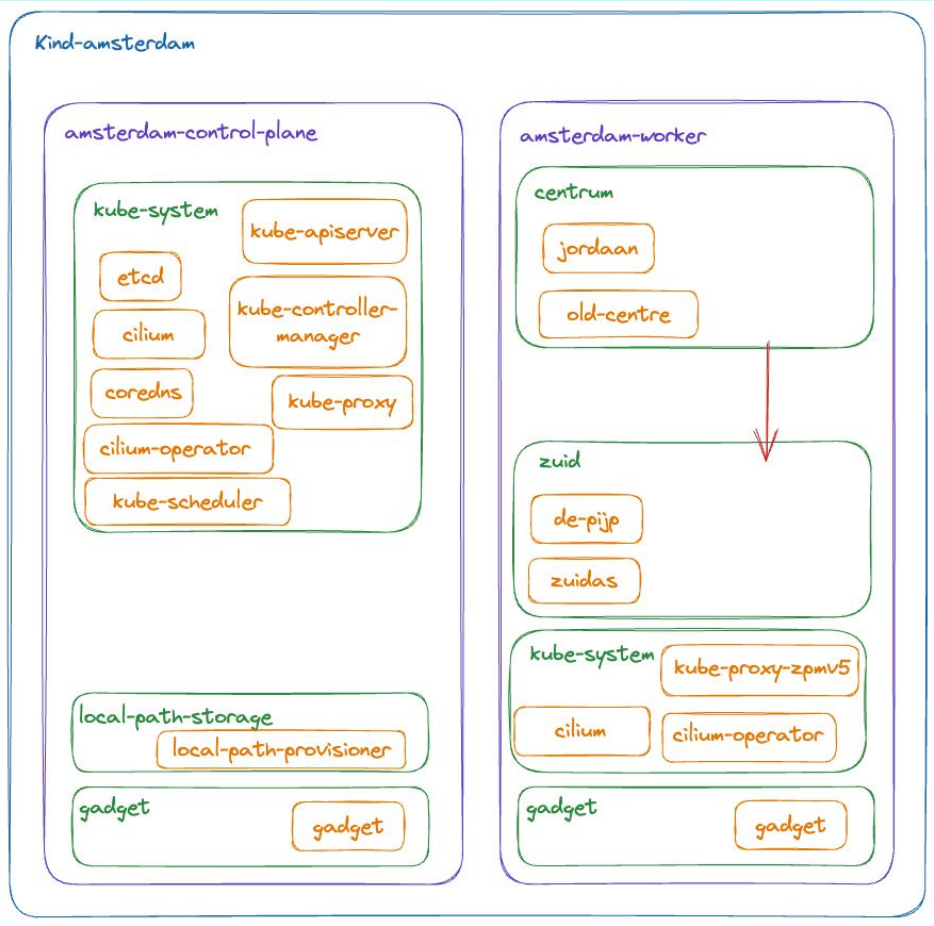
DEMOS

```
$ kubectl config view
- context:
    cluster: kind-amsterdam
    namespace: kube-public
    user: kind-amsterdam
  name: kind-amsterdam
```

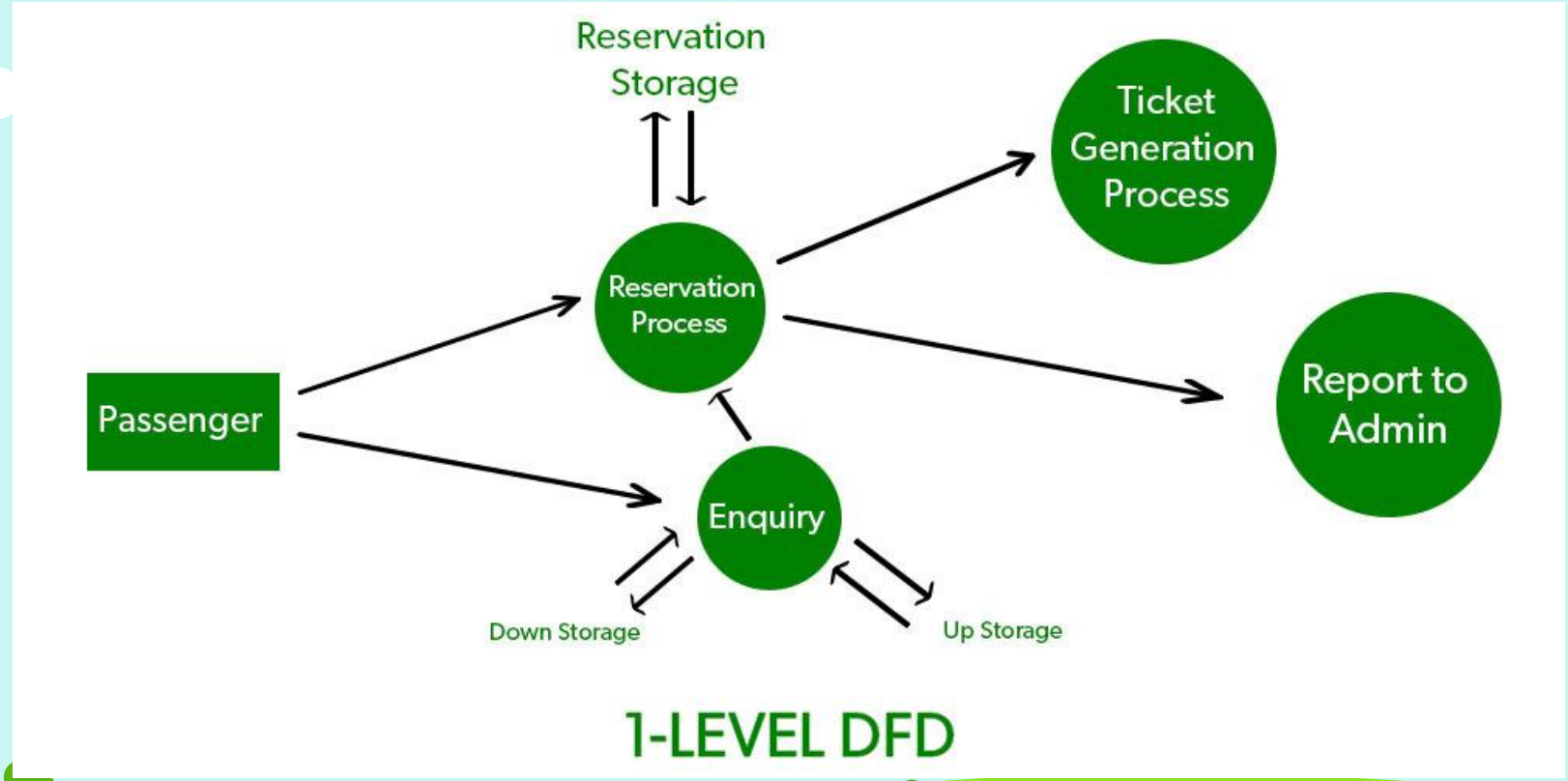

```
$ kubectl get all --all-namespaces
```

- Node
- Namespace
- Pod
- NetworkPolicy
- Service
- Deployments
- Ingress

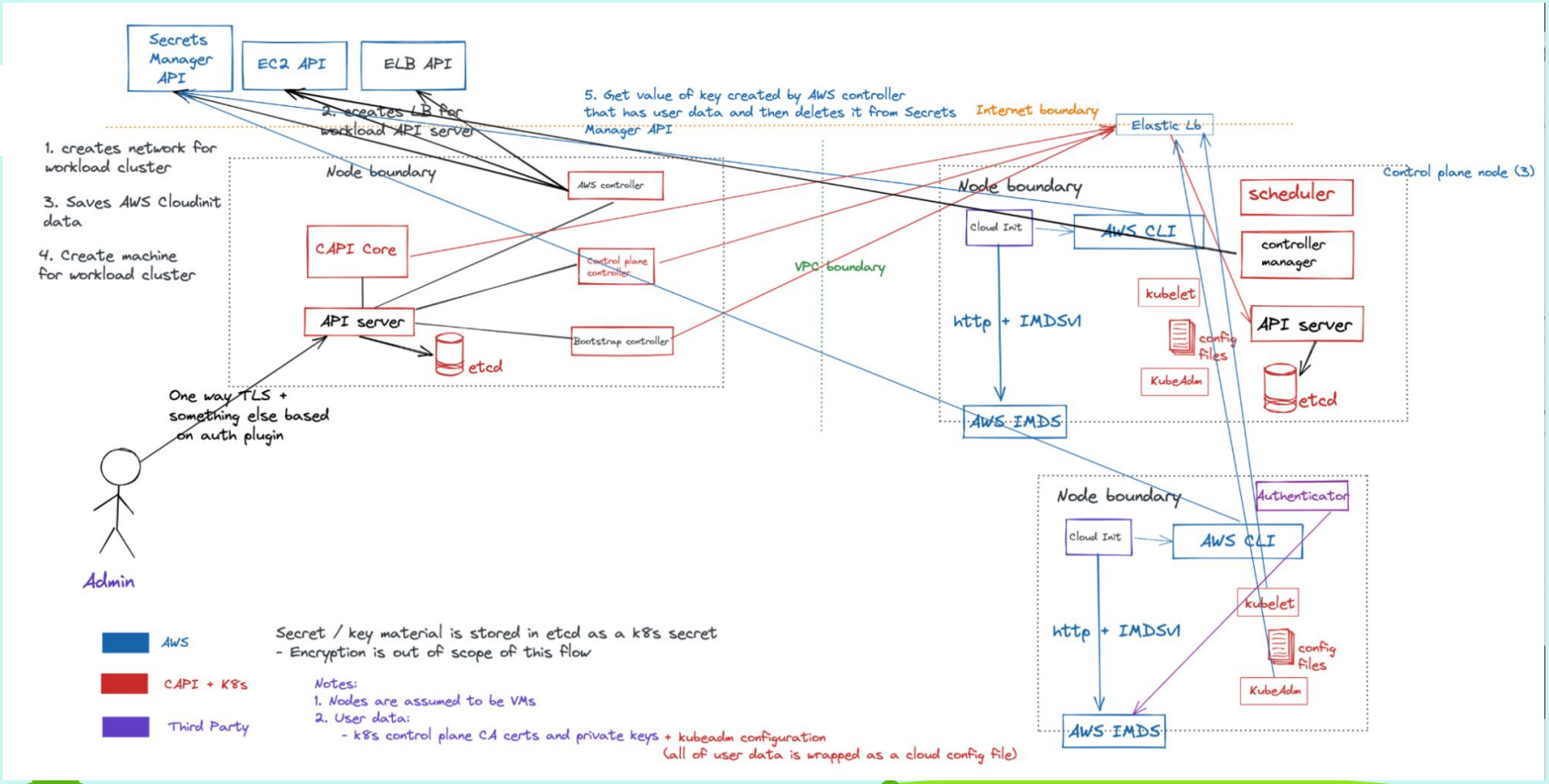

cailynedwards at Cailyns-MBP-2 in ~/amsterdam
kind-amsterdam/zuid


Kind-amsterdam
amsterdam-control-plane
kube-system
kube-apiserver
etcd
kube-controller-manager
cilium
coredns
kube-proxy
cilium-operator
kube-scheduler
local-path-storage
local-path-provisioner
gadget
gadget
amsterdam-worker
centrum
jordaan
old-centre
zuid
de-pijp
zuidas
kube-system
kube-proxy-zpmv5
cilium
cilium-operator
gadget
gadget

Data-flow Diagram



Data-flow Diagram



03

Threat Model

STRIDE

A useful threat modelling framework

s **Spoofing**
compromised tokens

t **Tampering**
over privileged, api-server access

r **Repudiation**
making dangerous or malicious changes without a trace

i **Information Disclosure**
compromised secrets, lack of encryption, unisolated workloads

d **Denial of Service**
overload the api-server, flood cluster network with traffic

e **Elevation of Privilege**
root users in containers, over privileged roles

04

Security Strategy

OK, we have a bunch of issues - now what?

We need to be able justify our priorities

Triage for best business case

Personnel

How complex is the problem?

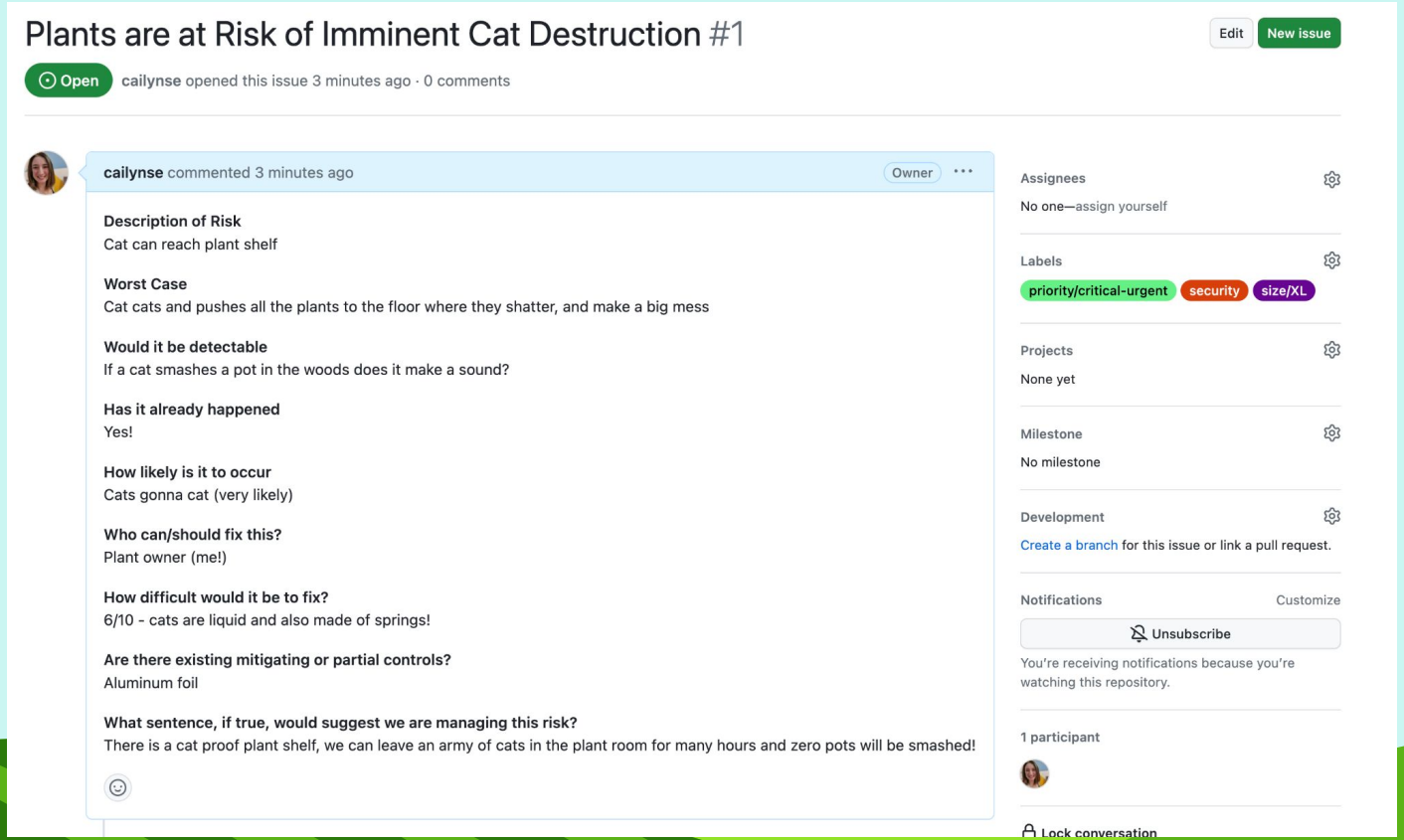
Threat Level

What is the likelihood it will be exploited?

Impact

If it is exploited will the impact be critical?

Risk Tracking



Plants are at Risk of Imminent Cat Destruction #1

Edit | New issue

Open | cailynse opened this issue 3 minutes ago · 0 comments

cailynse commented 3 minutes ago — Owner

Description of Risk
Cat can reach plant shelf

Worst Case
Cat cats and pushes all the plants to the floor where they shatter, and make a big mess

Would it be detectable
If a cat smashes a pot in the woods does it make a sound?

Has it already happened
Yes!

How likely is it to occur
Cats gonna cat (very likely)

Who can/should fix this?
Plant owner (me!)

How difficult would it be to fix?
6/10 - cats are liquid and also made of springs!

Are there existing mitigating or partial controls?
Aluminum foil

What sentence, if true, would suggest we are managing this risk?
There is a cat proof plant shelf, we can leave an army of cats in the plant room for many hours and zero pots will be smashed!

Assignees
No one—assign yourself

Labels
priority/critical-urgent | security | size/XL

Projects
None yet

Milestone
No milestone

Development
Create a branch for this issue or link a pull request.

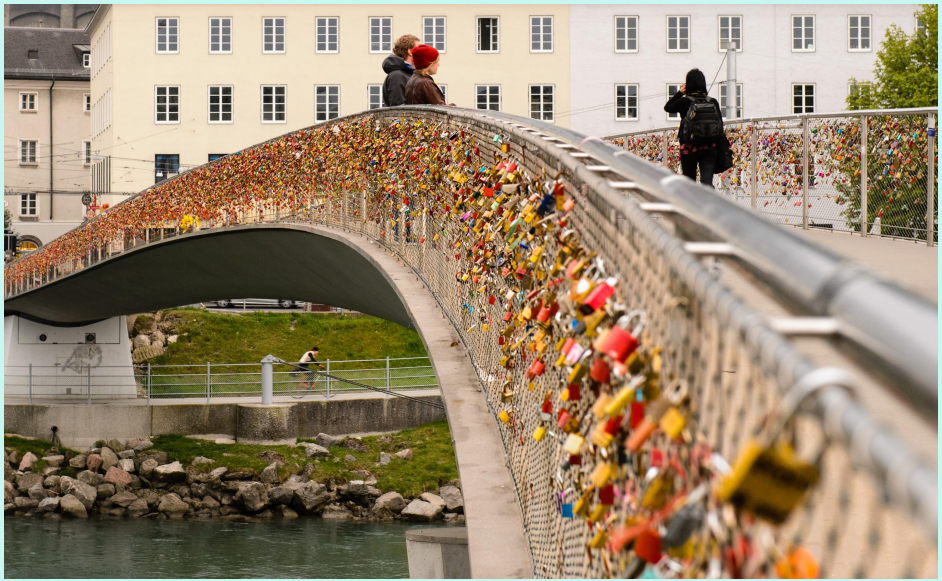
Notifications — Customize
Unsubscribe
You're receiving notifications because you're watching this repository.

1 participant

Lock conversation

05

Key Takeaways



Evaluating the Security of a Kubernetes Network

Components

What is the network made up of (we did this!!)

Boundaries

What's the edge? What egress/ingress is required?

Threats

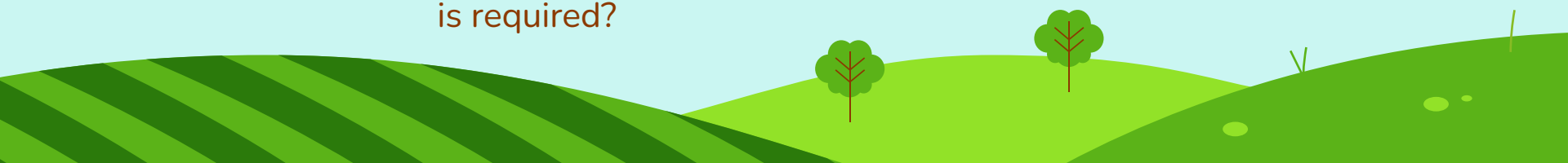
What are the risks? How are others getting exploited?

Triage

Where should we focus our efforts?

Mitigate

Create a security roadmap and start crushin' issues

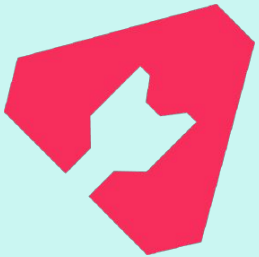


Useful Tools

eBPF

cilium

Open Policy Agent



and *SO* many more!

Resources

Basics

- https://kubernetes.io/docs/concepts/services-networking/
- https://kubernetes.io/docs/concepts/overview/components/

Getting to know the network

- https://kubernetes.io/docs/reference/kubectl/cheatsheet/
- https://www.inspektor-gadget.io/docs/latest/gadgets/advise/
- https://github.com/kubernetes/sig-security/tree/main/sig-security-assessments

Threat Modeling

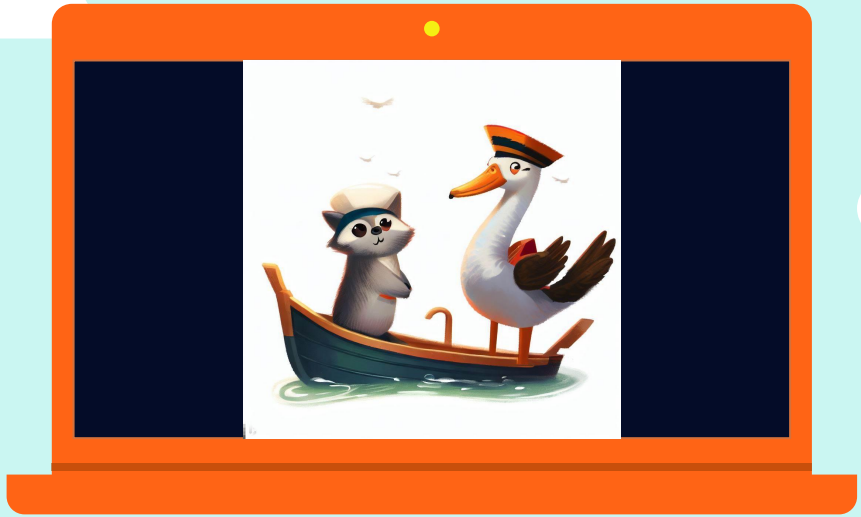
- https://owasp.org/www-community/Threat_Modeling_Process
- https://github.com/quarkslab/kdigger
- https://github.com/aquasecurity/kube-hunter

Security Strategy

- https://chandanbn.github.io/cvss/

Interested in contributing?

Come chat with us - if you want to help or learn more! We will be at the SIG meet and greet on Friday April 21 12:30-2:30!



Join us on slack!

Thank you!

KubeCon | CloudNativeCon
Europe 2023

FEEDBACK