BITS & BYTES

Lars Lefebvre

Kapers op de K8s kust

11:45 – 12:30

ANNACON 0X7E8

#whoami

BE België

🦁 Product Security@ING

🎸 Bassist

🎾 Padel- en tennis speler

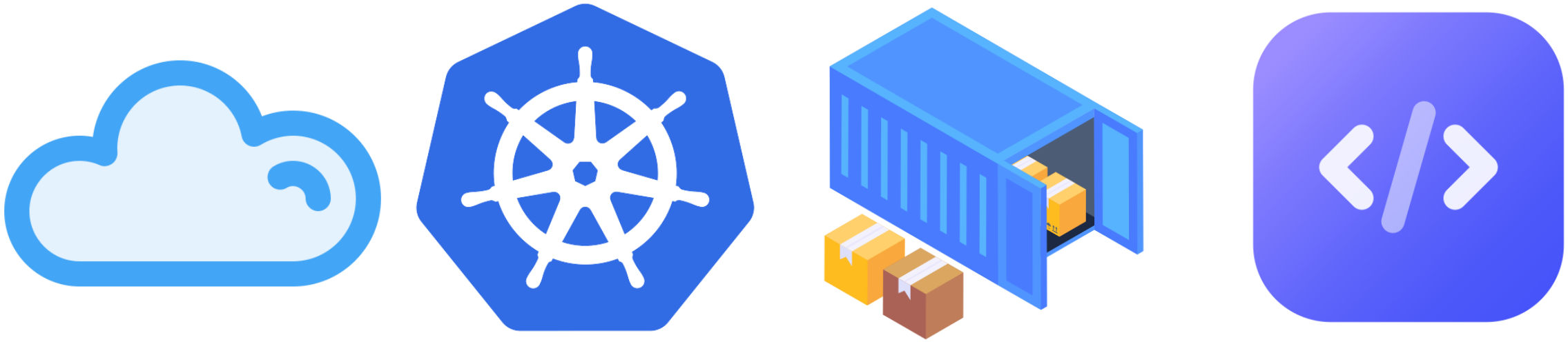
🏀 NBA fan

🍔 Smashed burgers

Google

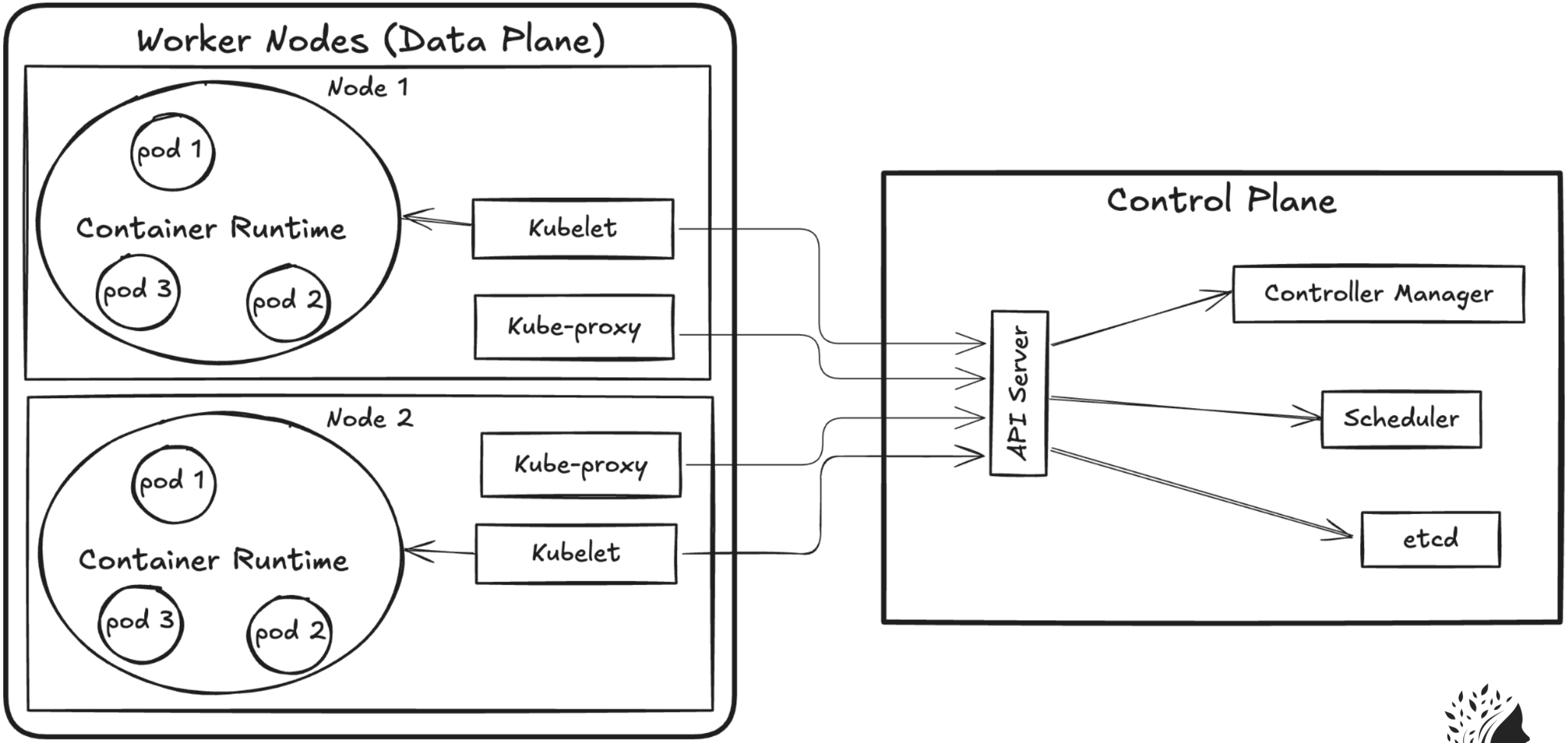
ANNACON
0X7E8

4 C’s of Cloud-Native Security

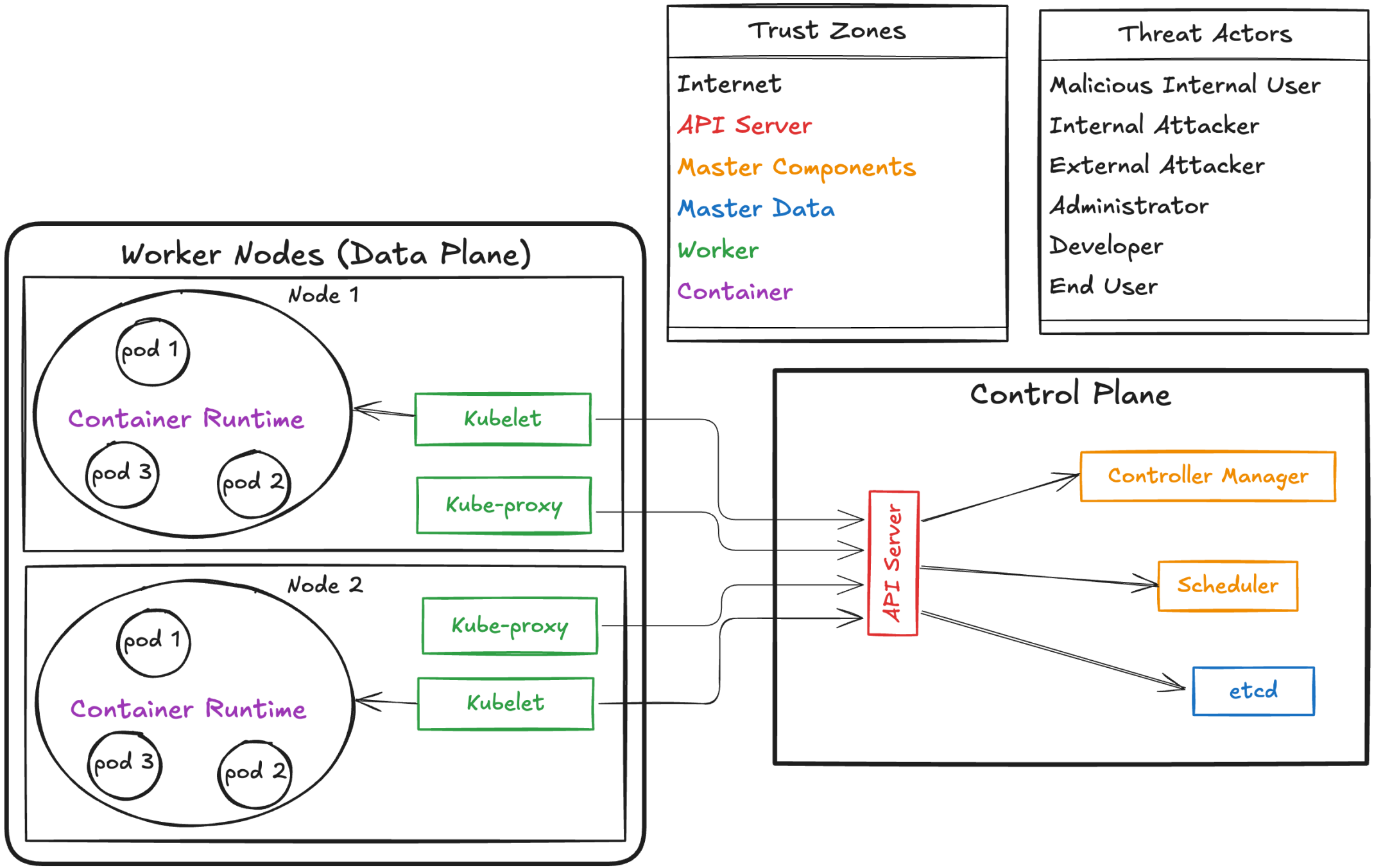


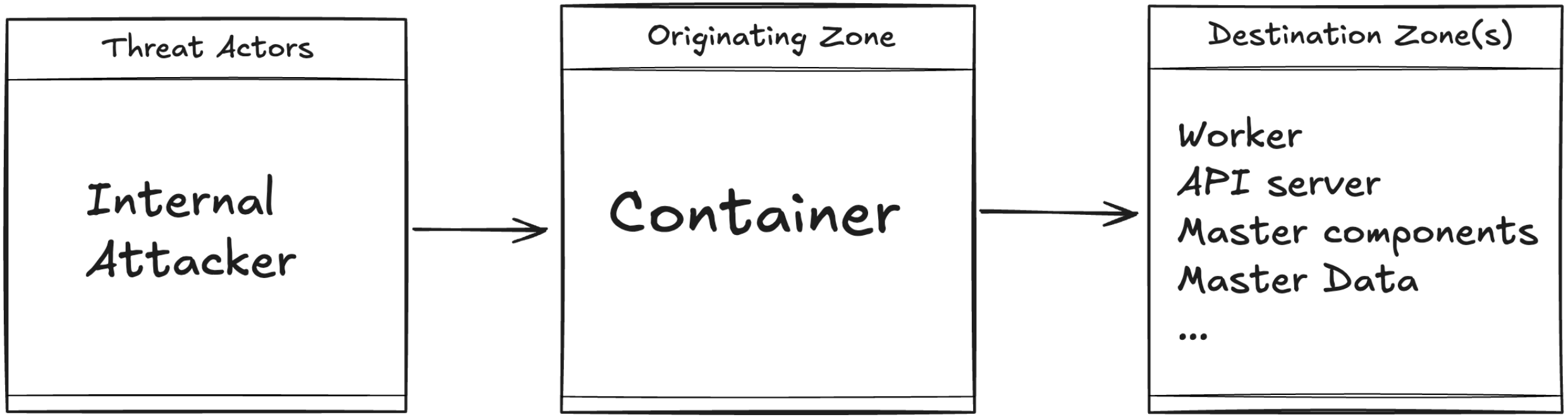
Kubernetes (Security) Concepts

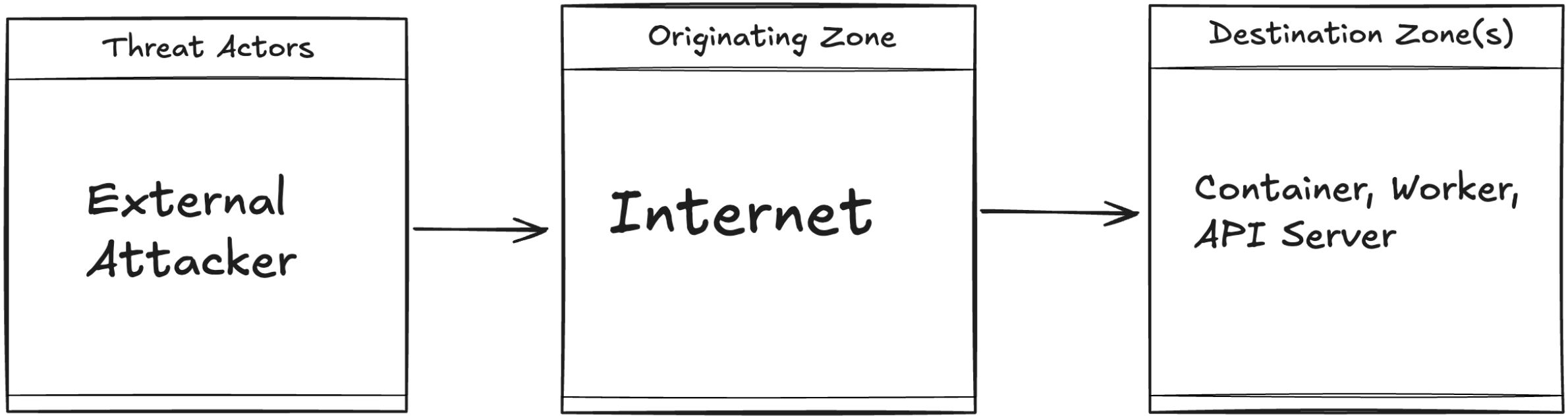
ANNACON
0X7E8

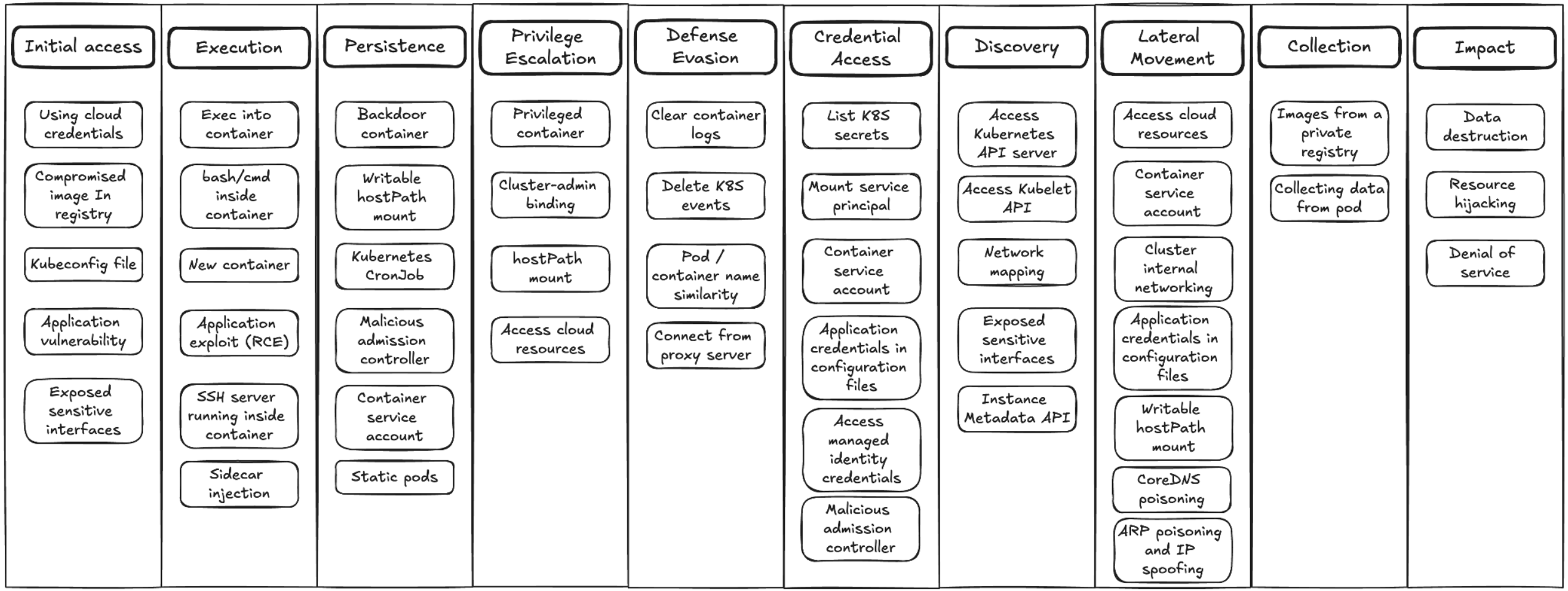


ANNACON
0X7E8



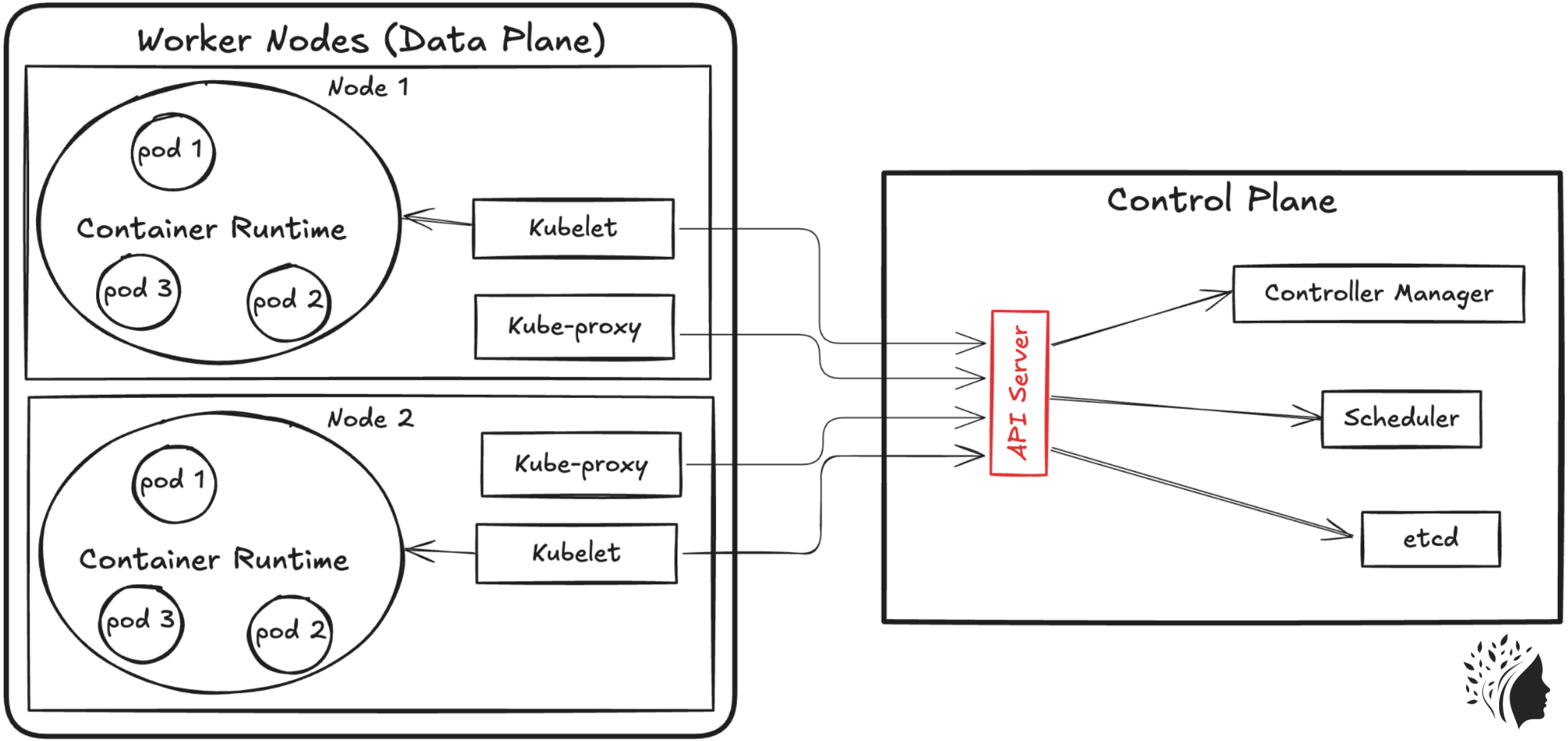


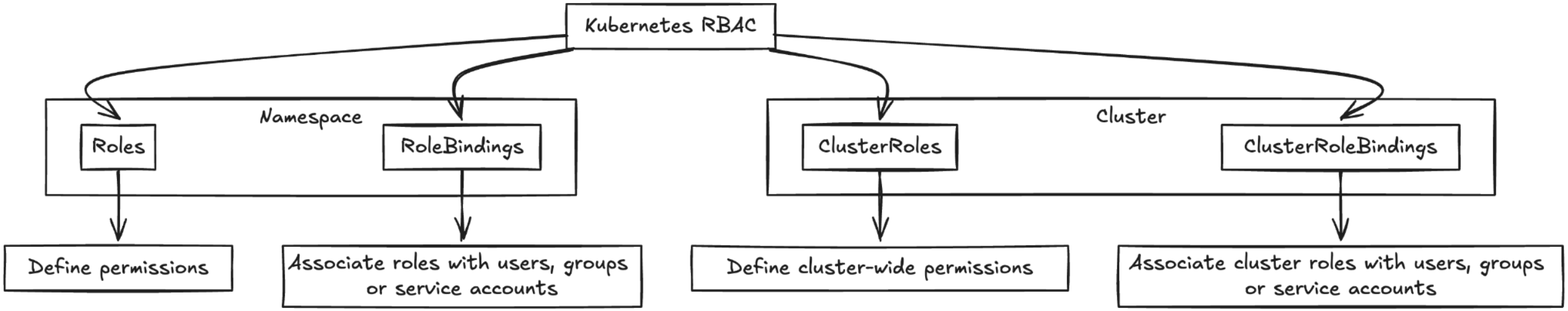

Threat Actors
External Attacker
Originating Zone
Internet
Destination Zone(s)
Container, Worker, API Server



ANNACON
0X7E8

Overly Permissive RBAC





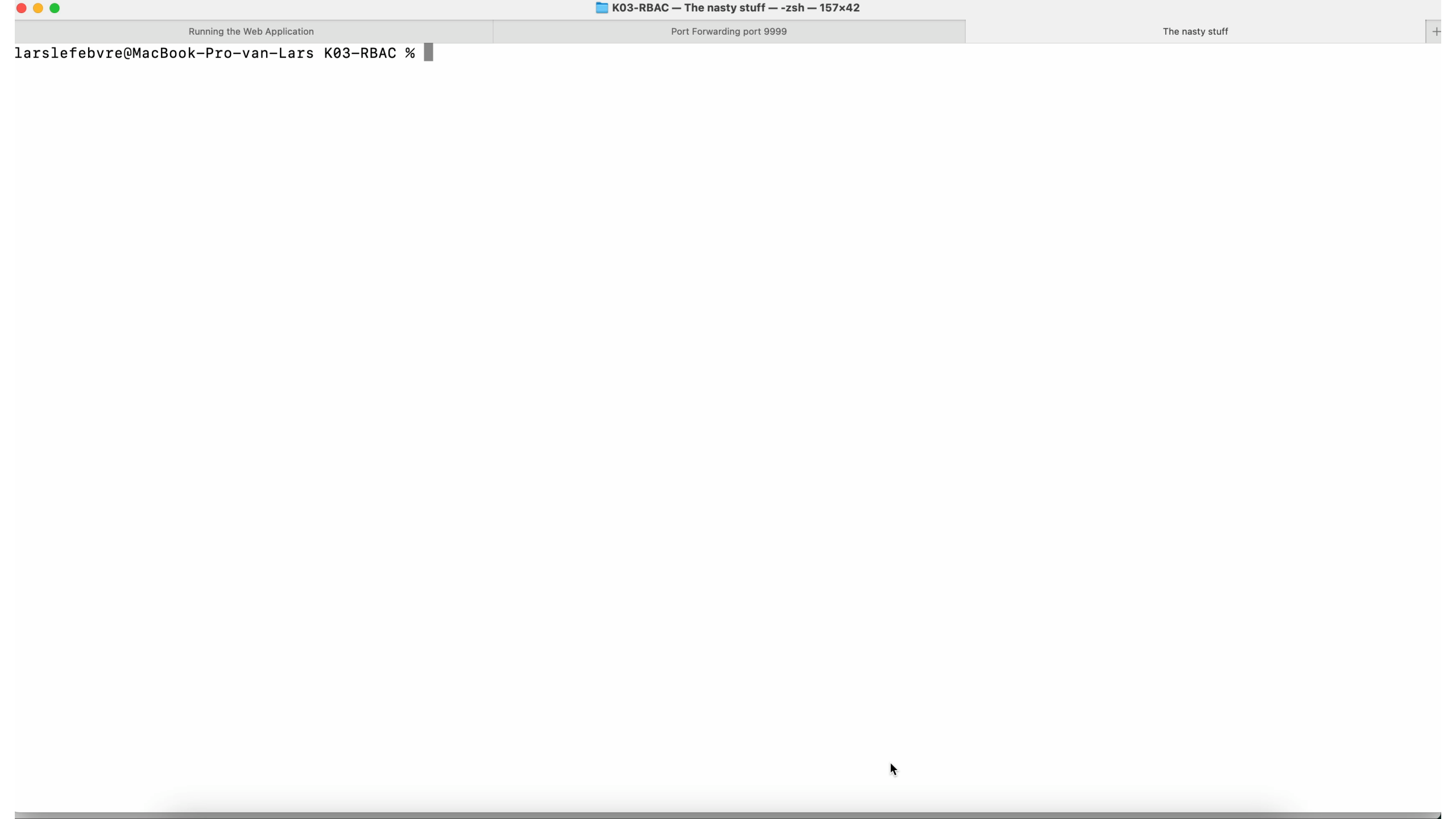
```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: demo-ns
  name: demo-role
rules:
- apiGroups: [""]
  resources: ["pods"]
  verbs: ["create", "get", "watch", "list", "exec","patch"]
- apiGroups: [""]
  resources: ["pods/exec"]
  verbs: ["create"]
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: demo-role-binding
  namespace: demo-ns
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: demo-role
subjects:
- kind: ServiceAccount
  name: demo-sa
  namespace: demo-ns
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: demo-cluster-role
rules:
- apiGroups: [""]
  resources: ["nodes","pods",pods/exec"]
  verbs: ["get", "watch", "list","exec","create"]
```

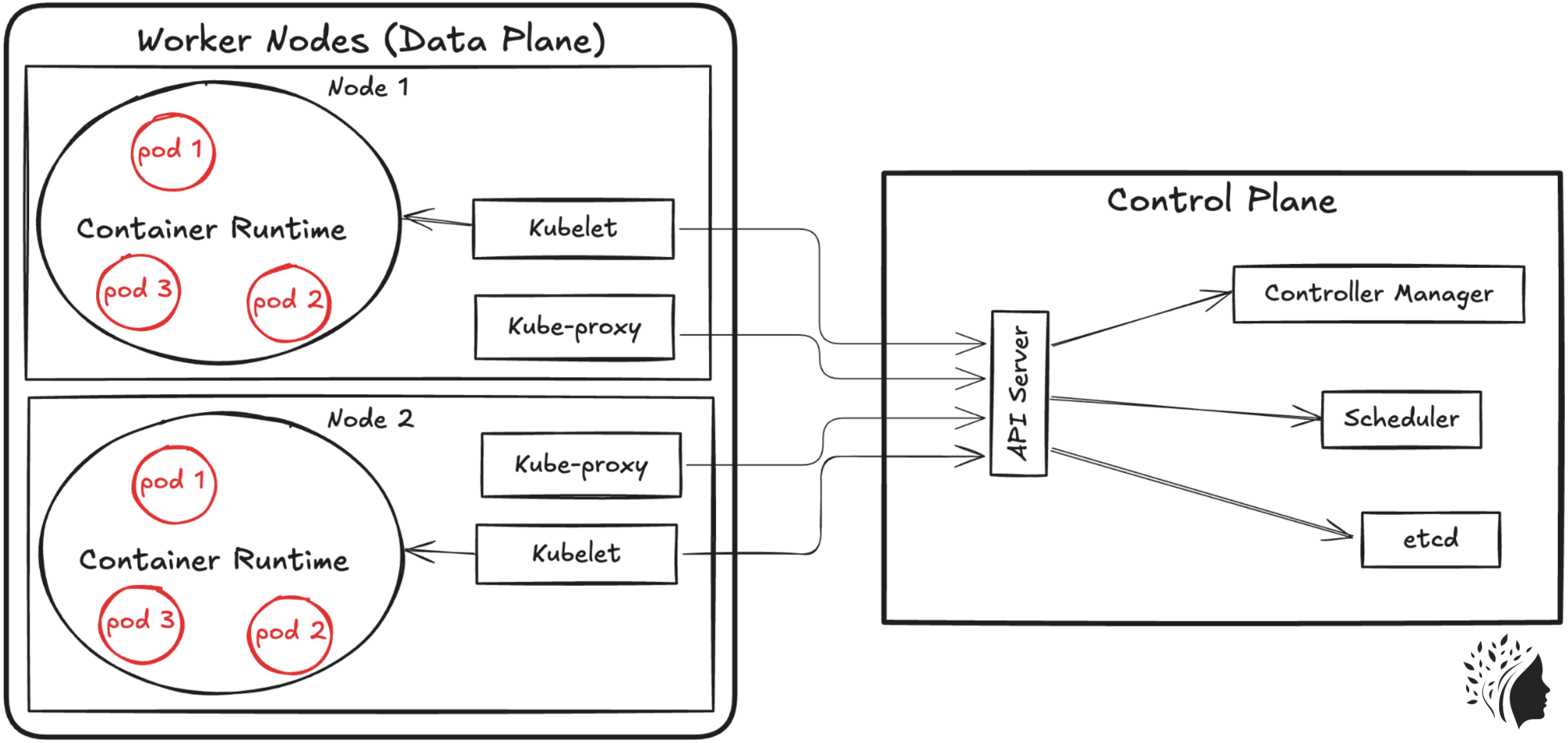
```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: demo-cluster-role-binding
subjects:
- kind: ServiceAccount
  name: demo-sa
  namespace: demo-ns
roleRef:
  kind: ClusterRole
  name: demo-cluster-role
  apiGroup: rbac.authorization.k8s.io
```

cluster-admin
binding


K03-RBAC — The nasty stuff — -zsh — 157×42
Running the Web Application
Port Forwarding port 9999
The nasty stuff
larslefebvre@MacBook-Pro-van-Lars K03-RBAC %

Avoiding Overly Permissive RBAC Configurations

Insecure Workload Configurations



```yaml
apiVersion: v1
kind: Pod
metadata:
 name: demo-app-insecure-config
spec:
 securityContext:
   runAsNonRoot: false
   runAsUser: 0
```

```
apiVersion: v1
kind: Pod
....
  spec:
    containers:
    - name: demo-app-insecure-config
      image: larslefebvre/h4cking-workshop-demo-app:867361
      imagePullPolicy: IfNotPresent
      securityContext:
        privileged: true
      ...
    serviceAccountName: demo-app-insecure-config
    ...
```

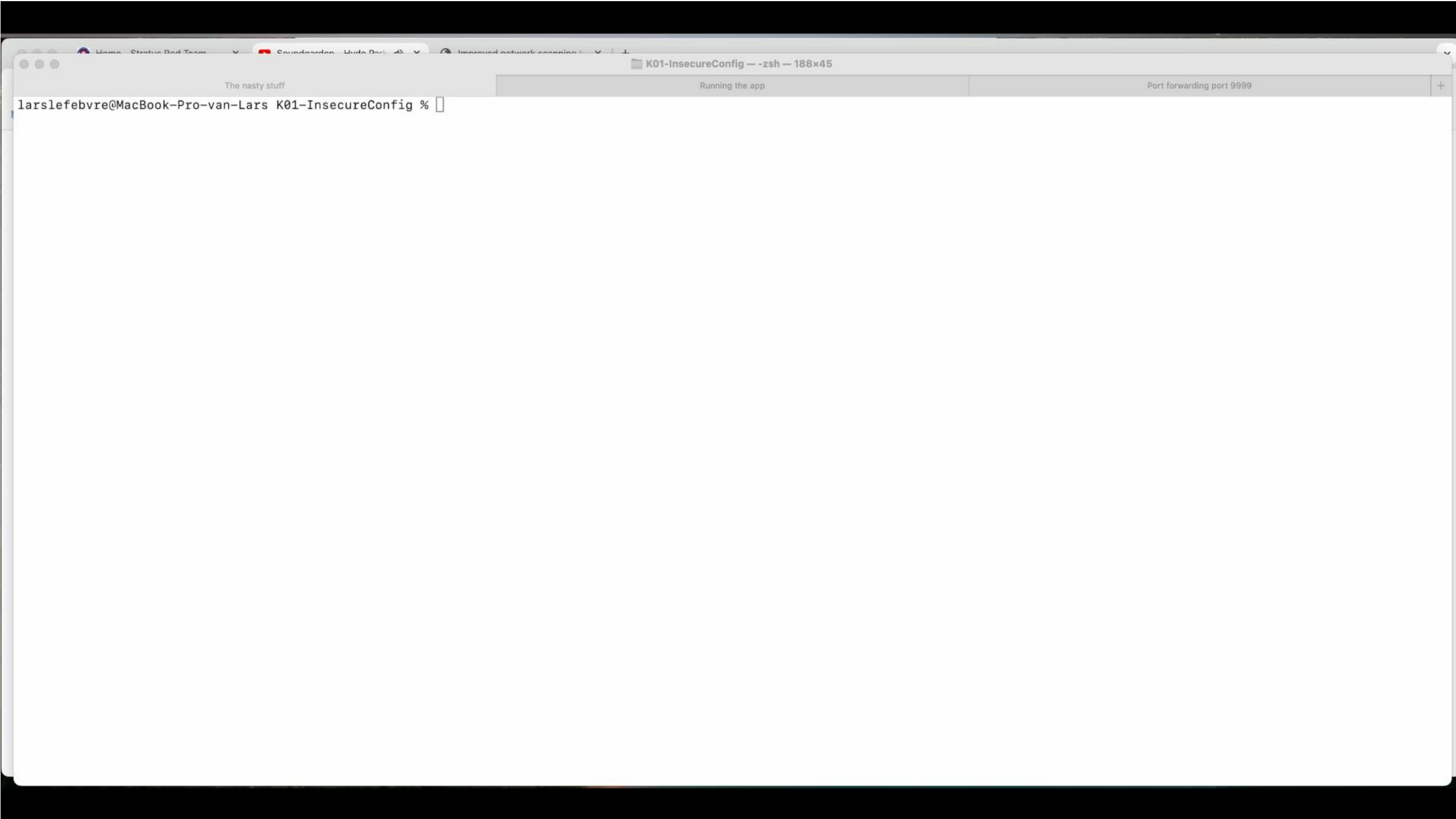
```
apiVersion: v1
kind: Pod
....
  spec:
    hostNetwork: true
    hostPID: true
    hostIPC: true
    containers:
    - name: demo-app-insecure-config
      ...
      volumeMounts:
      - mountPath: /host
        name: noderoot
    serviceAccountName: demo-app-insecure-config
    volumes:
    - name: noderoot
      hostPath:
        path: /
```

```
apiVersion: v1
kind: Pod
....
  spec:
    hostNetwork: true
    hostPID: true
    hostIPC: true
    containers:
    - name: demo-app-insecure-config
      ...
      volumeMounts:
      - mountPath: /host
        name: noderoot
    serviceAccountName: demo-app-insecure-config
    volumes:
    - name: noderoot
      hostPath:
        path: /
```

```yaml
apiVersion: v1
kind: Pod
....
  spec:
    containers:
    - name: demo-app-insecure-config
      ...
      securityContext:
        capabilities:
          drop:
            - ALL
          add: ["NET_ADMIN","SYS_TIME","SYS_ADMIN"]
      ...
```

privileged
container

hostPath mount


K01-InsecureConfig — -zsh — 188×45
The nasty stuff
Running the app
Port forwarding port 9999
larslefebvre@MacBook-Pro-van-Lars K01-InsecureConfig %

Remedies for Insecure Workload Configuration

Deze partners hebben een ❤️ voor ANNACON 0x7E8.

ANNACON
0X7E8

easi
NEUVIK
astrea
UPRIGHT
INFOSENTRY
TSF
pwc
Business
exabeam
REFRACTED
JARVISS
FOX IT
SentinelOne
sweepatic
Beltug
ISACA
Belgium Chapter
SAI