KubeCon + CloudNativeCon North America 2026

Securing Rural Colorado with Open Source

Running a Student-Led SOC on Kubernetes

Maciej Wal
Cybersecurity Platform Architect, the Cybersecurity Center, Metropolitan State University of Denver

About the Cybersecurity Center

- Hands-on cybersecurity clinic at MSU Denver
- Bridge education and industry through real-world experience
- Prepare students to enter the cybersecurity workforce with confidence, competence, and credibility

MSU DENVER

The Cybersecurity Center

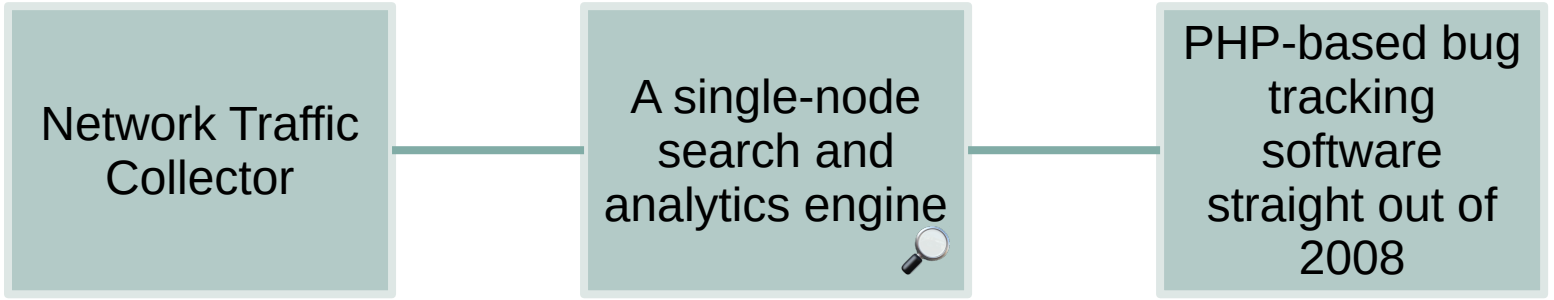
Cybersecurity Multi-Use Training Environment

About Centurion SECURED

- Cybersecurity students are trained to monitor and protect public-sector entities that represent more than 500,000 Coloradans
- Our mission is to strengthen cybersecurity for Colorado’s small governments and businesses through a student-staffed, professionally led monitoring service that gives students real SOC experience for the cybersecurity workforce

Centurion SECURED

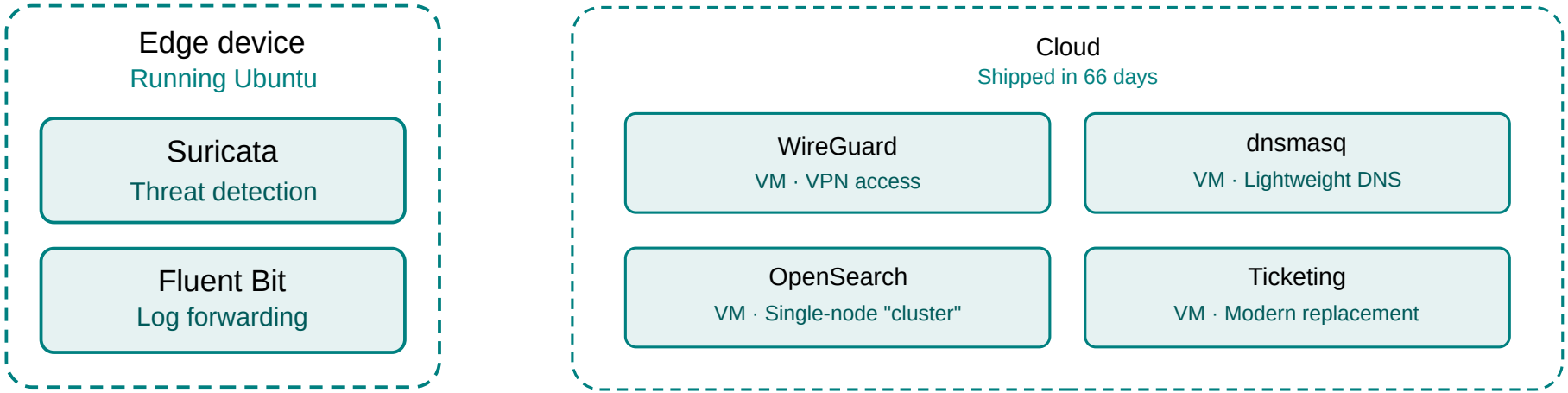
Original Student Workflow



ET EXPLOIT Possible OpenSSL HeartBleed Large HeartBeat Response from Common S
ET EXPLOIT Possible CVE-2014-6271 malicious DNS response
ET EXPLOIT MVPower DVR Shell UCE
ET EXPLOIT TP-Link Archer AX21 Unauthenticated Command Injection Inbound (CVE-2
ET EXPLOIT_KIT SUSPICIOUS JAR Download by Java UA with non JAR EXT matches va
ET EXPLOIT Possible Apache log4j RCE Attempt - 2021/12/12 Obfuscation Observed I
ET EXPLOIT Malformed HeartBeat Request
ET EXPLOIT Possible TLS HeartBleed Unencrypted Request Method 3 (Inbound to Com
ET EXPLOIT D-Link - RCE Attempt Inbound (CVE-2021-45382)
ET EXPLOIT Netgear DGN Remote Command Execution

Late March 2024...

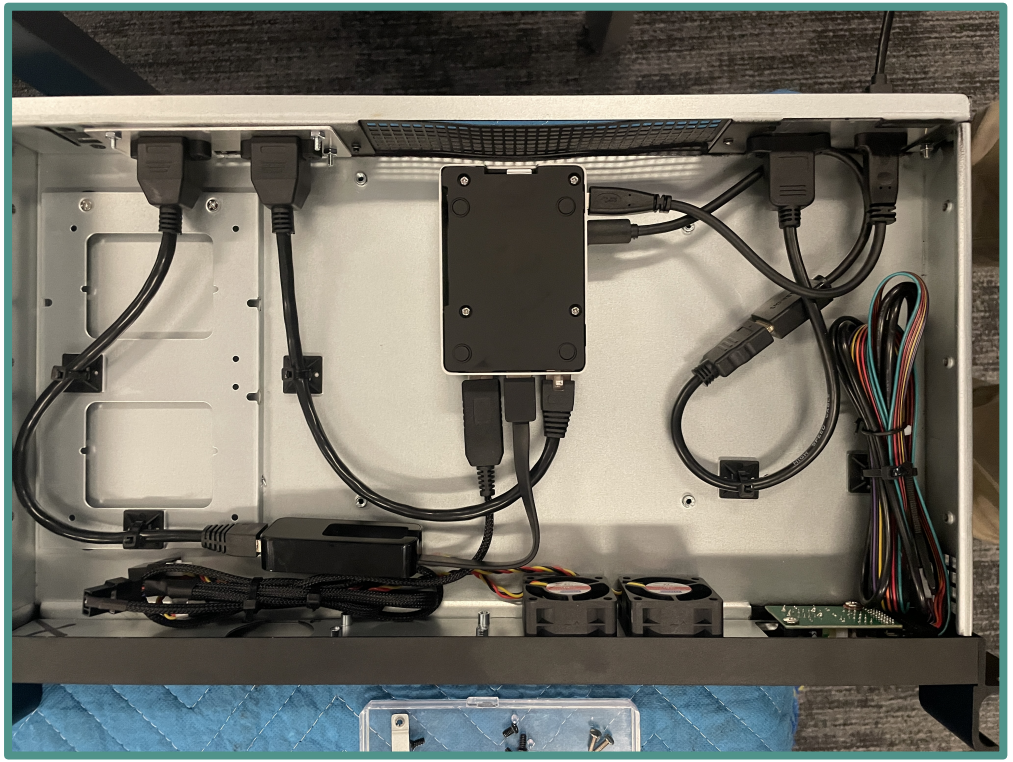
Time to rebuild



Time to rebuild (edge device)

Raspberry Pi 5 running:

- Ubuntu
- Wireguard
- FluentBit
- Suricata



Hooray! Everything is working. All deployed in 66 days...

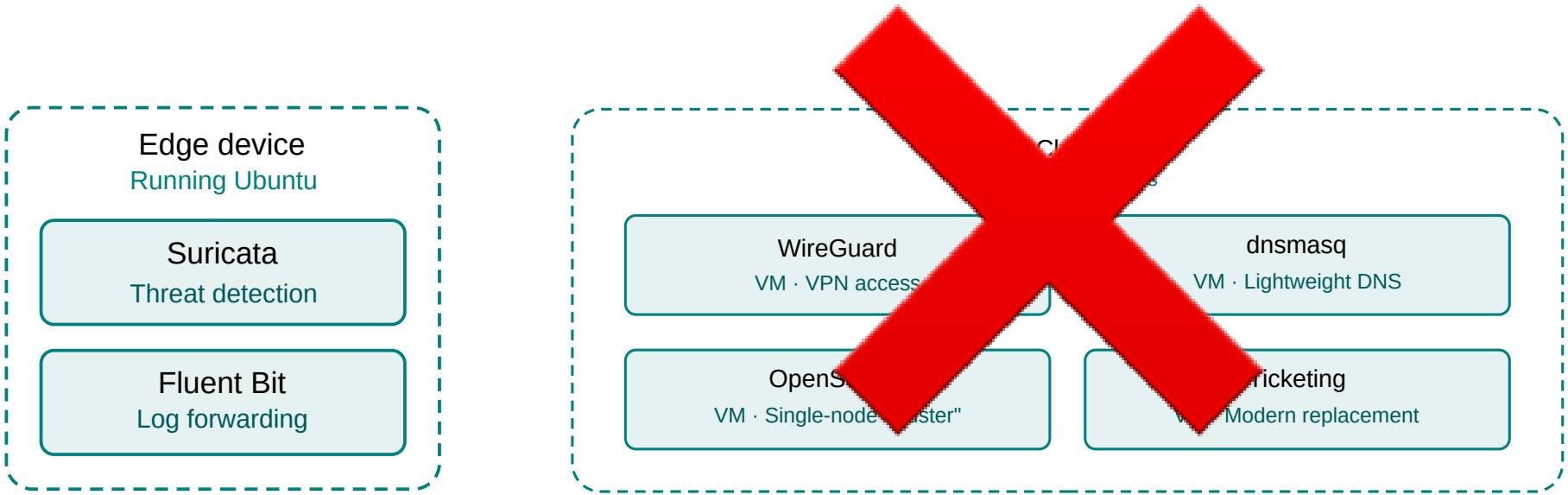


Then my director started talking about offering this as a statewide service, and I was a team of one...



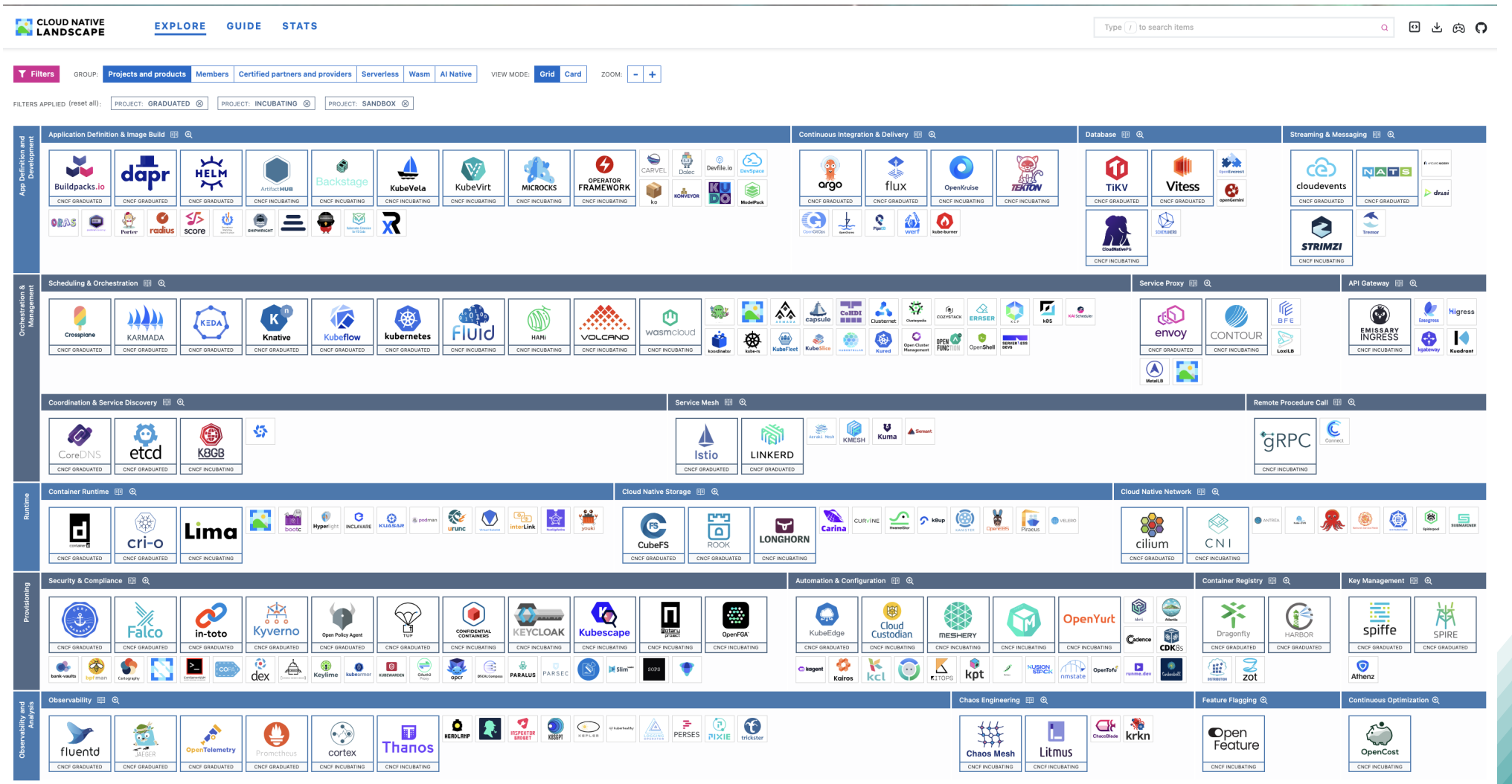
Issues with the 4 VMs

- A single-node OpenSearch “cluster” couldn’t scale
- Every app managed its own users
- Every change and new partner meant hand-configuring servers


Edge device
Running Ubuntu
Suricata
Threat detection
Fluent Bit
Log forwarding
WireGuard
VM · VPN access
dnsmasq
VM · Lightweight DNS
VM · Modern replacement

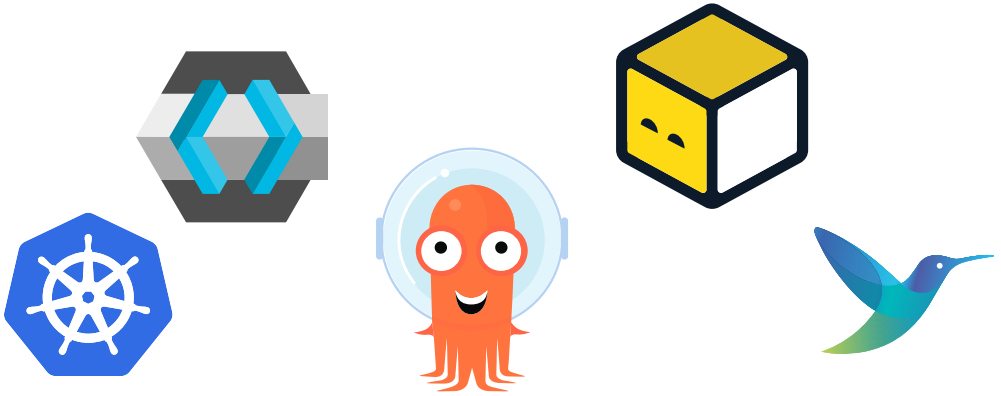
What is everyone else doing?




CLOUD NATIVE LANDSCAPE
EXPLORE
GUIDE
STATS
Type / to search items
Filters
GROUP: Projects and products | Members | Certified partners and providers | Serverless | Wasm | AI Native
VIEW MODE: Grid | Card
ZOOM: - +
FILTERS APPLIED (reset all): PROJECT: GRADUATED | PROJECT: INCUBATING | PROJECT: SANDBOX
App Definition and Development
Application Definition & Image Build
Buildpacks.io
dapr
HELM
ArtifactHUB
Backstage
KubeVela
KubeVirt
MICROCKS
OPERATOR FRAMEWORK
CARVEL
Dalec
Devfile.io
DevSpace
ko
KONVEYOR
KUDO
ModePack
ORAS
Porter
radius
score
SHIPWRIGHT
XR
Continuous Integration & Delivery
argo
flux
OpenKruise
TEKTON
OpenGitOps
PipeCD
werf
kube-burner
Database
TiKV
Vitess
OpenEverest
openGemini
CloudNativePG
SCHEMAHERO
Streaming & Messaging
cloudevents
NATS
drasi
STRIMZI
Tremor
Orchestration & Management
Scheduling & Orchestration
Crossplane
KARMADA
KEDA
Knative
Kubeflow
kubernetes
Fluid
HAMi
VOLCANO
wasmcloud
koordinator
kube-rs
KubeFleet
KubeSlice
Kured
Open Cluster Management
OPEN FUNCTION
OpenShell
SERVERLESS DEVS
COZYSTACK
ERASER
KCP
k8s
KAI Scheduler
Service Proxy
envoy
CONTOUR
BFE
LoxiLB
MetalLB
API Gateway
EMISSARY INGRESS
Easegress
Higress
kgateway
Kuadrant
Coordination & Service Discovery
CoreDNS
etcd
KBGB
Service Mesh
Istio
LINKERD
KMESH
Kuma
Remote Procedure Call
gRPC
Connect
Runtime
Container Runtime
cri-o
Lima
bootc
Hyperlight
INCLAVARE
KUASAR
podman
runc
inter Link
youki
Cloud Native Storage
CubeFS
ROOK
LONGHORN
Carina
CURVINE
HwameiStor
kBup
KANISTER
OpenEBS
Piraeus
VELERO
Cloud Native Network
cilium
CNI
ANTREA
Spiderpool
SUBMARINER
Provisioning
Security & Compliance
Falco
in-toto
Kyverno
Open Policy Agent
TUF
CONFIDENTIAL CONTAINERS
KEYCLOAK
Kubescape
Notary project
OpenFGA
bank-vaults
bpfman
Cartography
container2wasm
cosign
dex
Keylime
kubearmor
KUBEWARDEN
OAuth2 Proxy
OPCR
OSCAL Compass
PARALUS
PARSEC
SLIM
SOPS
Automation & Configuration
KubeEdge
Cloud Custodian
MESHERY
OpenYurt
Akri
Atlantis
Cadence
CDK8s
kagent
Kairos
kcl
KITOPS
kpt
kusion stack
nmstate
OpenTofu
rainbond
Sealos
Container Registry
Dragonfly
HARBOR
DISTRIBUTION
zot
Key Management
spiffe
SPIRE
Athenz
Observability and Analysis
Observability
fluentd
JAEGER
OpenTelemetry
Prometheus
cortex
Thanos
HERDLRNR
INSPEKTOR GRIDGET
KRR
KUBEPULSE
PERSES
PIXIE
trickster
Chaos Engineering
Chaos Mesh
Litmus
ChaosBlade
krkn
Feature Flagging
Open Feature
Continuous Optimization
OpenCost

Ordering off the CNCF Landscape

- **Kubernetes:** Container orchestration
- **Keycloak:** Identity and access management
- **ArgoCD:** GitOps done right
- **OpenTofu:** Cloud resources declared like the big players
- **Fluent Bit:** Shipping logs from the edge to OpenSearch



Why Kubernetes?

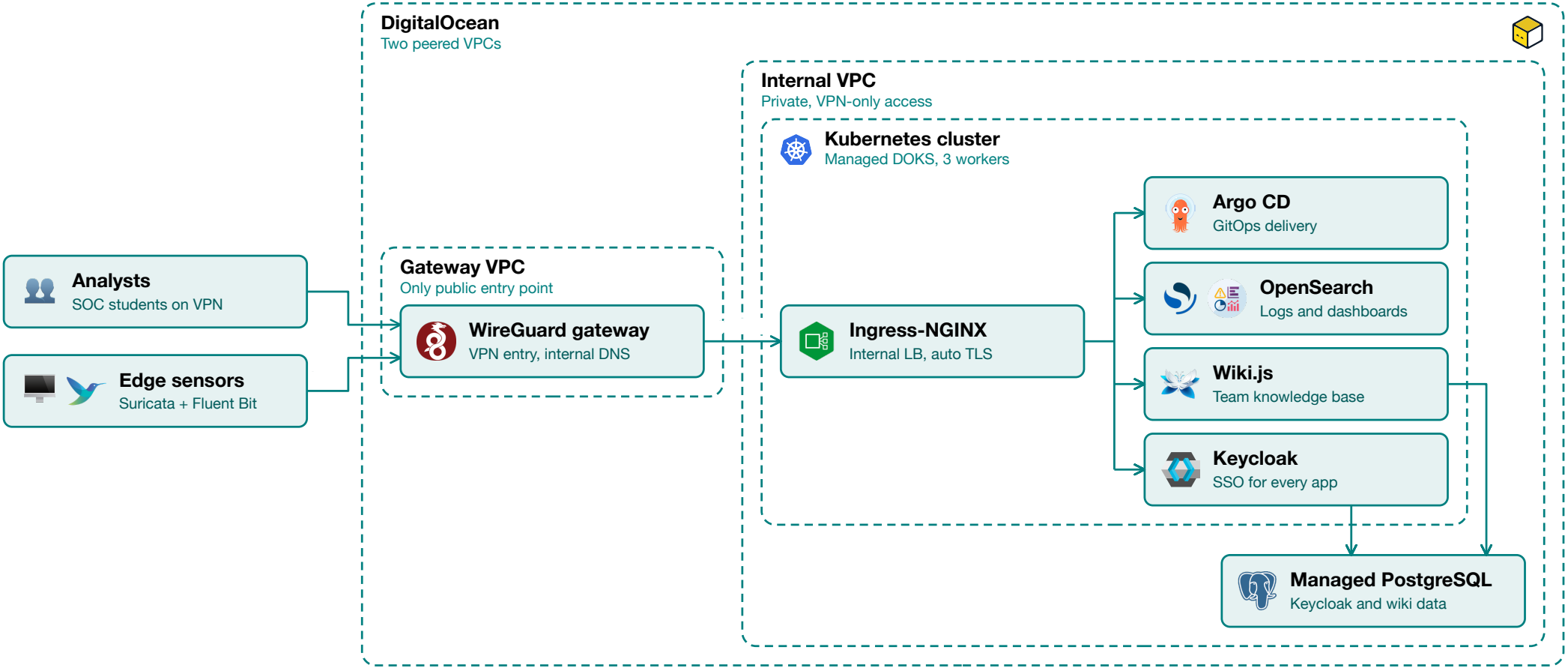
- Everything declared in Git
- No more building servers!
- Students could get hands-on experience with the same GitOps and Cloud Native tools used in industry



So long, four VMs...



Centurion SECURED on Kubernetes!



How much does this cost?

- Around ~$1,000

Billing History

DATE	DESCRIPTION	AMOUNT	
December, 31 2025		-$912.73	•••
December, 31 2025	Invoice for December 2025	$912.73	•••
November, 30 2025		-$912.88	•••
November, 30 2025	Invoice for November 2025	$912.88	•••
October, 31 2025		-$821.57	•••
October, 31 2025	Invoice for October 2025	$821.57	•••

Sweet, all done! Right?



Well...



Shard Explosions

- 14+ community partners, each creating their own indices within OpenSearch
- A misconfigured printer flooded a network with mDNS requests
- Poof. The cluster couldn’t keep up and went down



Shard Explosions: The Fix

- Drop mDNS alerts before they ever hit the index
- Restart the pod every day at 2:00 AM. Why not?
- The actual fix: A dedicated cluster just for OpenSearch

Observability

- Students on a Discord server should be fine



Observability: The Fix

- Students on a Discord server is not fine
- Real alerting with Prometheus and Grafana in a management cluster

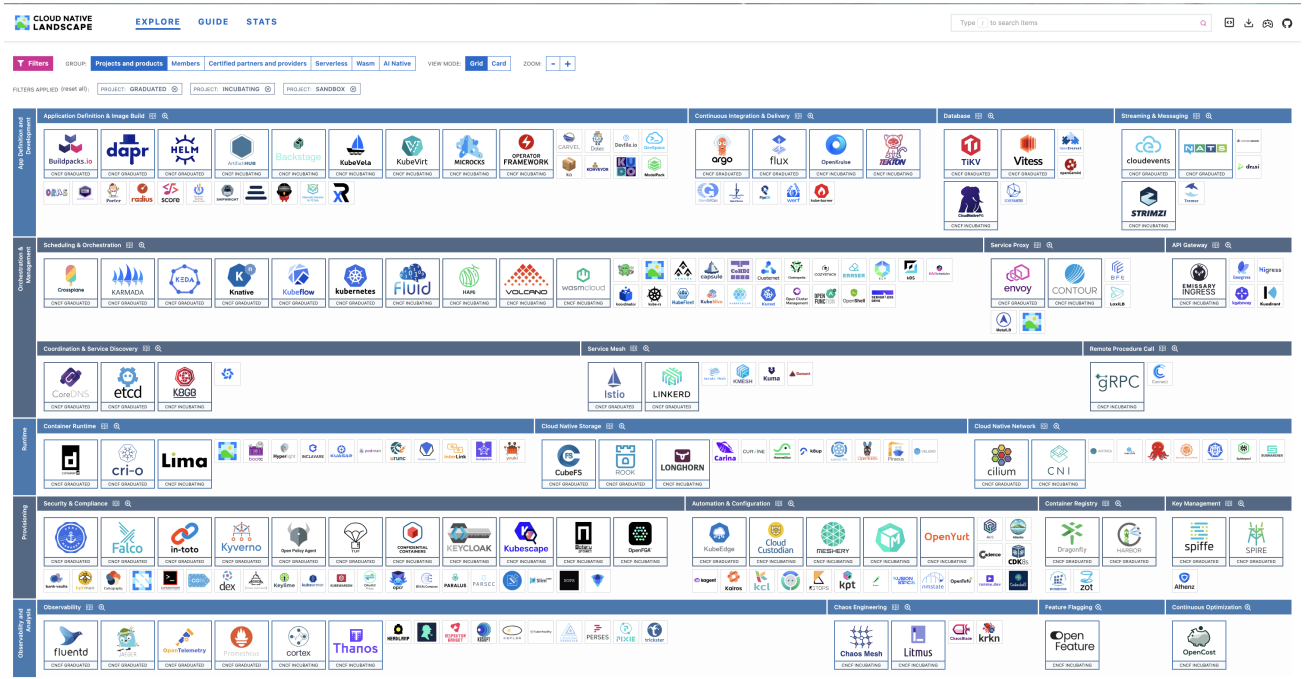




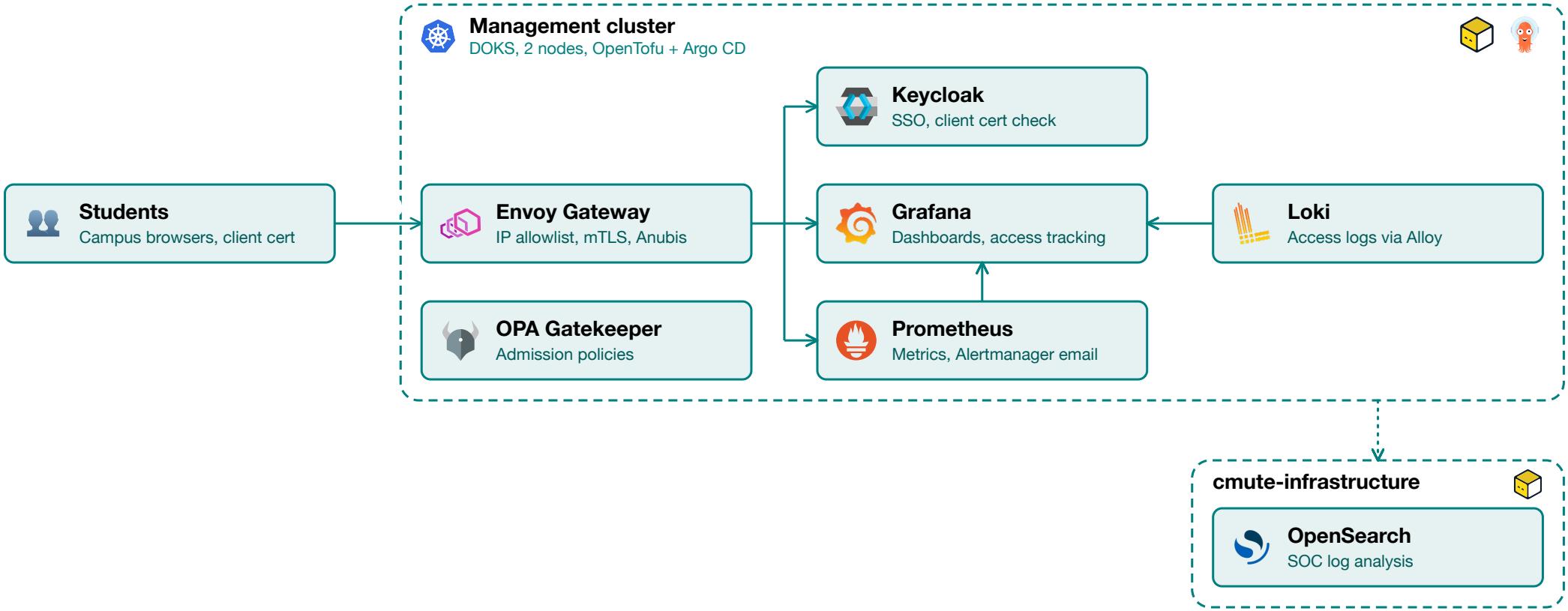
Zero Trust Nobody Used

- Every new cohort of 30 students meant SSHing in to generate WireGuard configs by hand
- Move to Envoy Gateway, pair it with Keycloak, and give students browser certificates instead
- A separate management cluster
- Make this whole thing meet some sort of benchmark

Back to the CNCF Landscape...



Zero-Trust Management Cluster!



Remember: Zero Trust nobody used?



Zero Trust Nobody Used

- The WireGuard certificates worked. That was enough for everyone but me
- None of it mattered without buy-in
- The dedicated OpenSearch cluster stayed and finally ended the shard explosions
- The zero-trust access got turned off

One of the hardest problems in platform engineering is closing the gap between self-service and people actually using the service

Students are at the core of all of this



Two kinds of students

- Student analysts: Learn log analysis and how a real SOC works, with live data
- Student developers: Maintain the platform itself through GitOps and Kubernetes



They always end up leaving me... for real jobs



The Kubernetes Workshop

- Each cluster provisioned on DigitalOcean with OpenTofu
- Learn about tools like ArgoCD, Envoy Gateway, cert-manager, and GitHub Actions
- See GitOps in action



The Colorado Sustainability Hub

- An NSF-funded platform built by undergraduate students that makes Colorado's environmental, economic, and social sustainability data usable by people who are not analysts
- Developed a chatbot named Bili
- Used OpenTelemetry, Jaeger, and Prometheus to instrument their application



https://github.com/msu-denver/bili-core

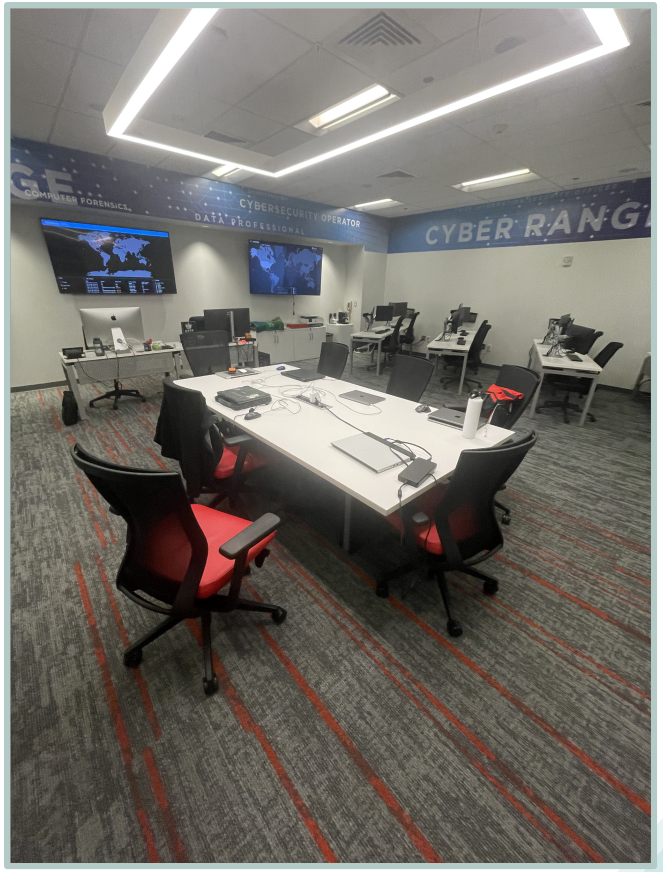
Roadrunner Connect Club

- A group of students that develop a mobile application for MSU Denver to empower students to engage with campus
- Implemented OpenFeature to standardize feature flags across the app

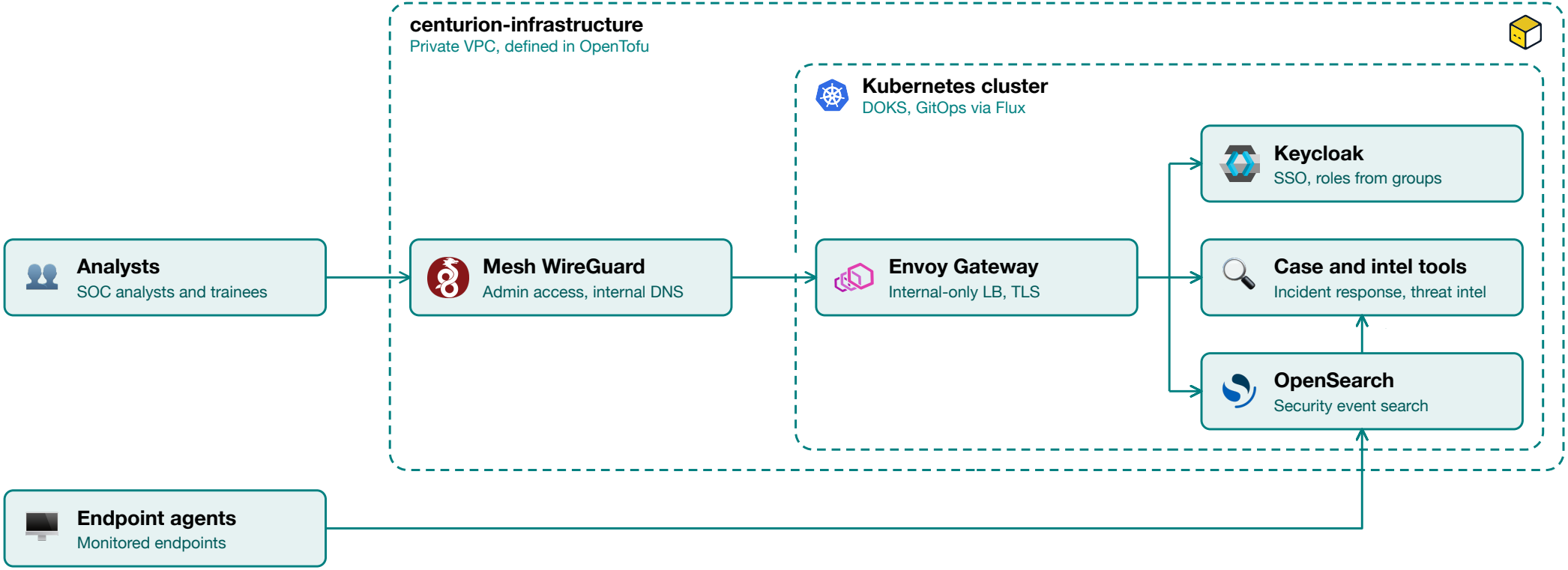


Technology brings everyone together

- Students interacting with real data
- Rural Colorado getting security it couldn’t otherwise afford
- Counties with 1-3 IT people who just need day-to-day operations to stay stable



Centurion 2.0: Lessons Applied



None of this would have been possible with bespoke bash scripts

Thank You.

Any questions?

Connect with me on LinkedIn:

https://www.linkedin.com/in/maciejwal/

Maciej Wal
Cybersecurity Platform Architect, the Cybersecurity Center, Metropolitan State University of Denver