
K8s Adversary Emulation
Adopting an Attacker's Mindset for Kubernetes Security

# Whoami

## Markus Gierlinger

Product Manager @ Cast AI

Former security researcher @ Dynatrace

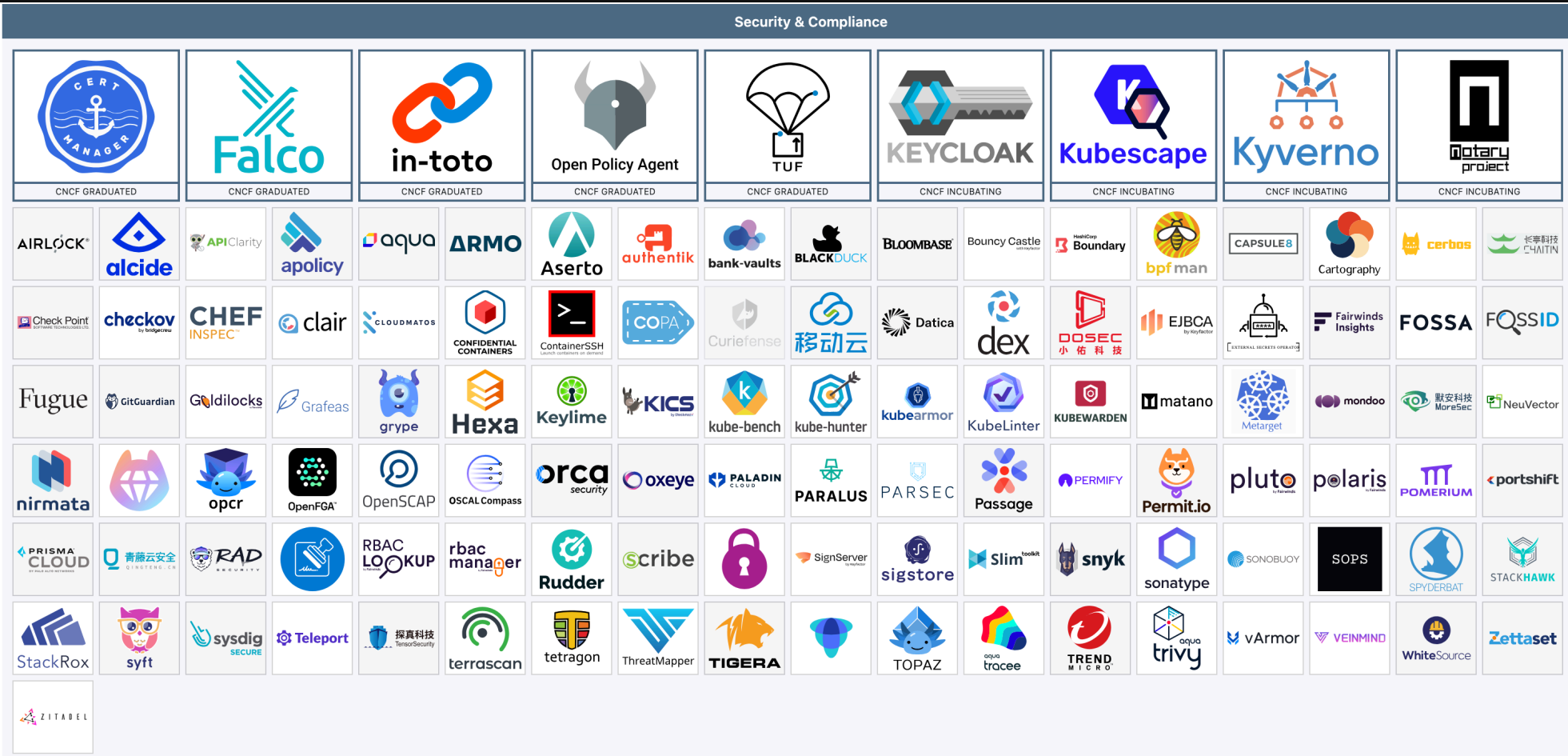
Enjoys exploring cybersecurity and AI

Magier Markus

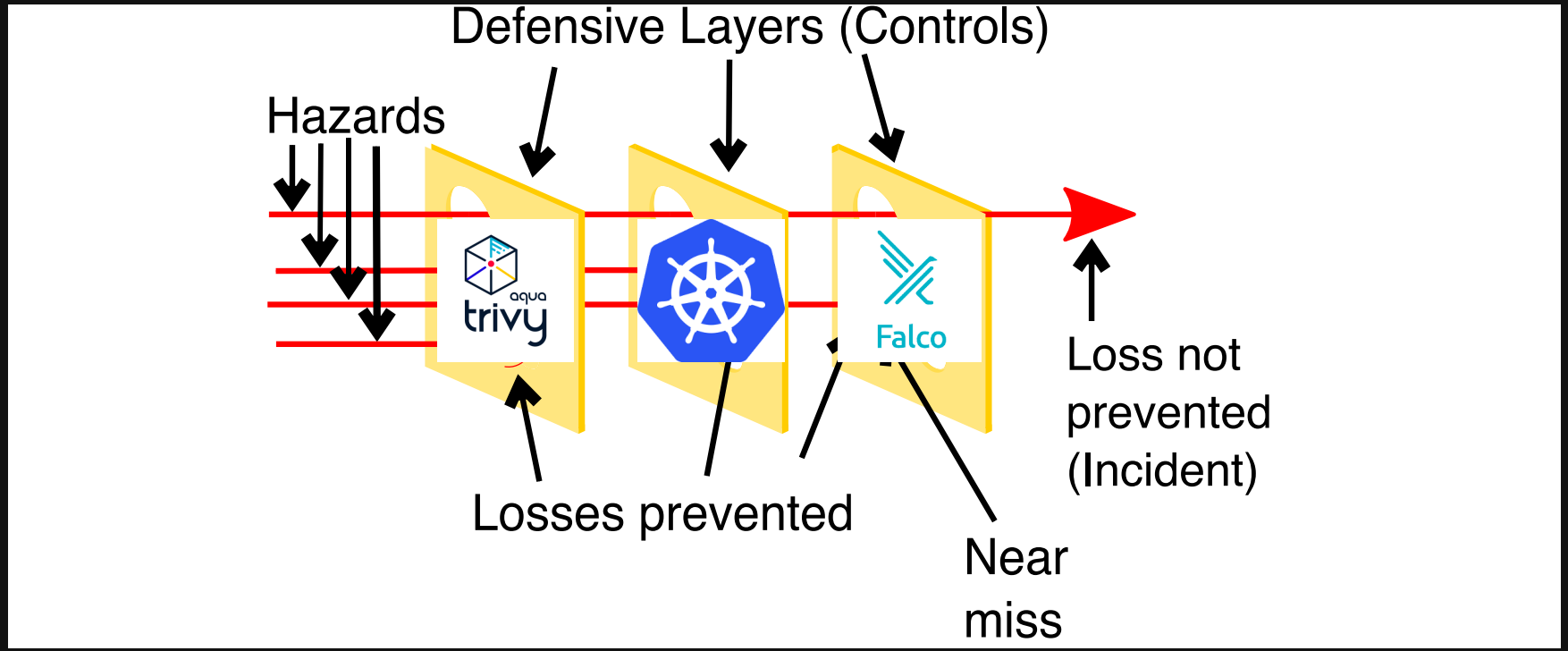
# Whois Molly?

- New and only **SecOps Engineer** at Wish Ltd.
  - Wish Ltd. has ~300 employees
  - Heavy use of Kubernetes
- Previously ~3 years experience as SRE
- Responsible for “securing” the product

# What does "secure" mean?

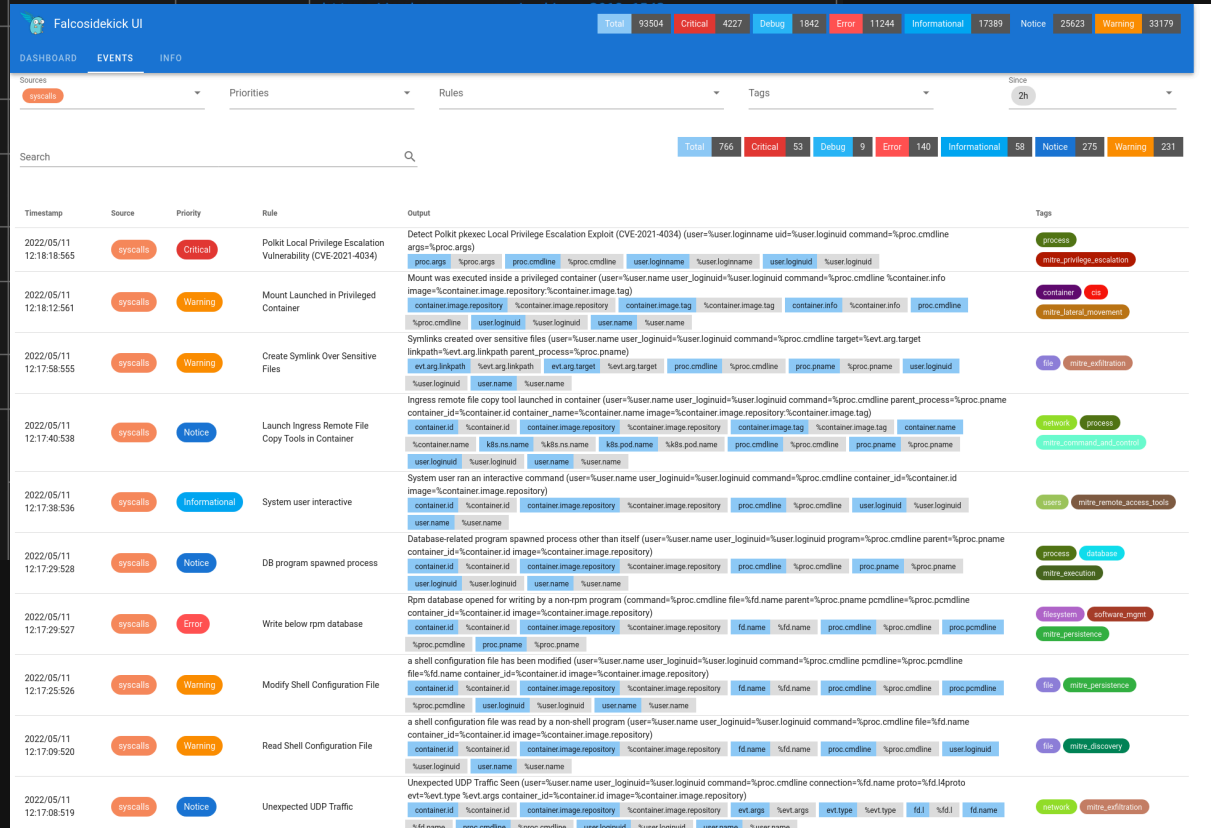

Security & Compliance
CNCF GRADUATED
CNCF GRADUATED
CNCF GRADUATED
CNCF GRADUATED
CNCF GRADUATED
CNCF INCUBATING
CNCF INCUBATING
CNCF INCUBATING
CNCF INCUBATING
AIRLOCK
alcide
APIClarity
apolicy
aqua
ARMO
Aserto
authentik
bank-vaults
BLACKDUCK
BLOOMBASE
Bouncy Castle
Boundary
bpf man
CAPSULE8
Cartography
cerbos
CHAITIN
Check Point
checkov
CHEF INSPEC
clair
CLOUDMATOS
CONFIDENTIAL CONTAINERS
ContainerSSH
COPA
Curiefense
移动云
Datica
dex
DOSEC
EJBCA
Fairwinds Insights
FOSSA
FOSSID
Fugue
GitGuardian
Goldilocks
Grafeas
grype
Hexa
Keylime
KICS
kube-bench
kube-hunter
kubearmor
KubeLinter
KUBEWARDEN
matano
Metarget
mondoo
NeuVector
nirmata
opcr
OpenFGA
OpenSCAP
OSCAL Compass
orca security
oxeye
PALADIN CLOUD
PARALUS
PARSEC
Passage
PERMIFY
Permit.io
pluto
polaris
POMERIUM
portshift
PRISMA CLOUD
青藤云安全
RAD SECURITY
RBAC LOOKUP
rbac manager
Rudder
scribe
SignServer
sigstore
Slim
snyk
sonatype
SONOBUOY
SOPS
SPYDERBAT
STACKHAWK
StackRox
syft
sysdig SECURE
Teleport
terrascan
tetragon
ThreatMapper
TIGERA
TOPAZ
tracee
TREND MICRO
trivy
vArmor
VEINMIND
WhiteSource
Zettaset
ZITADEL

# Defense in Depth



# Endless list of findings

| | | | | | |
|---|---|---|---|---|---|
| expat | CVE-2019-15903 | HIGH | 2.2.6-r0 | 2.2.7-r1 | expat: heap-based buffer over-read via crafted XML input https://avd.aquasec.com/nvd/cve-2019-15903 |
| libcrypto1.1 | CVE-2019-1543 | | 1.1.1a-r1 | 1.1.1b-r1 | openssl: ChaCha20-Poly1305 with long nonces |
| libcrypto1.1 | CVE-2020-1967 | HIGH | | | |
| libcrypto1.1 | CVE-2021-23840 | HIGH | | | |
| libcrypto1.1 | CVE-2021-3450 | HIGH | | | |
| libssl1.1 | CVE-2019-1543 | HIGH | | | |
| libssl1.1 | CVE-2020-1967 | HIGH | | | |
| libssl1.1 | CVE-2021-23840 | HIGH | | | |
| libssl1.1 | CVE-2021-3450 | HIGH | | | |
| sqlite-libs | CVE-2019-19244 | | | | |

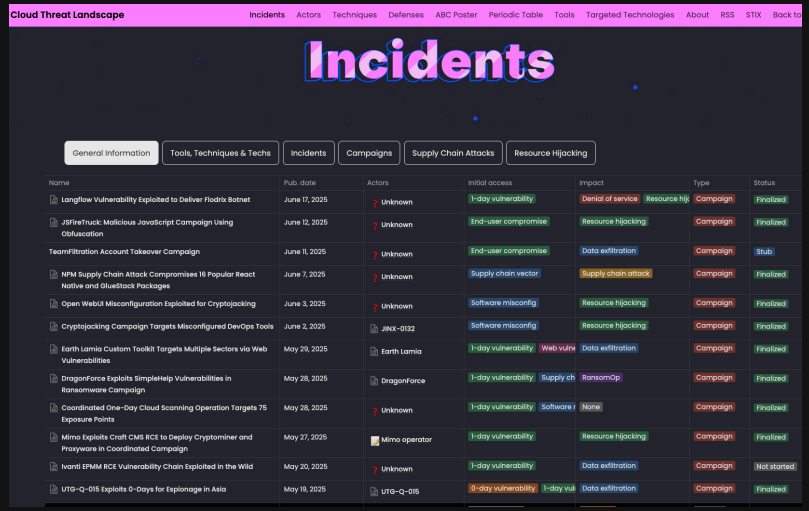


# Does *this* make our environments secure?

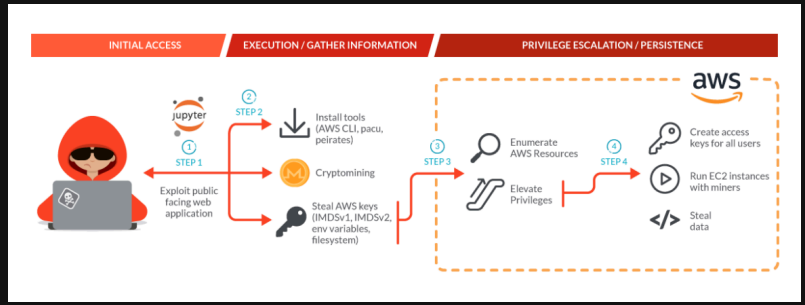
"Defenders think in lists.
Attackers think in graphs.
As long as this is true, attackers win"

John Lambert, VP Security @ Microsoft, 2015

# Threat Intelligence

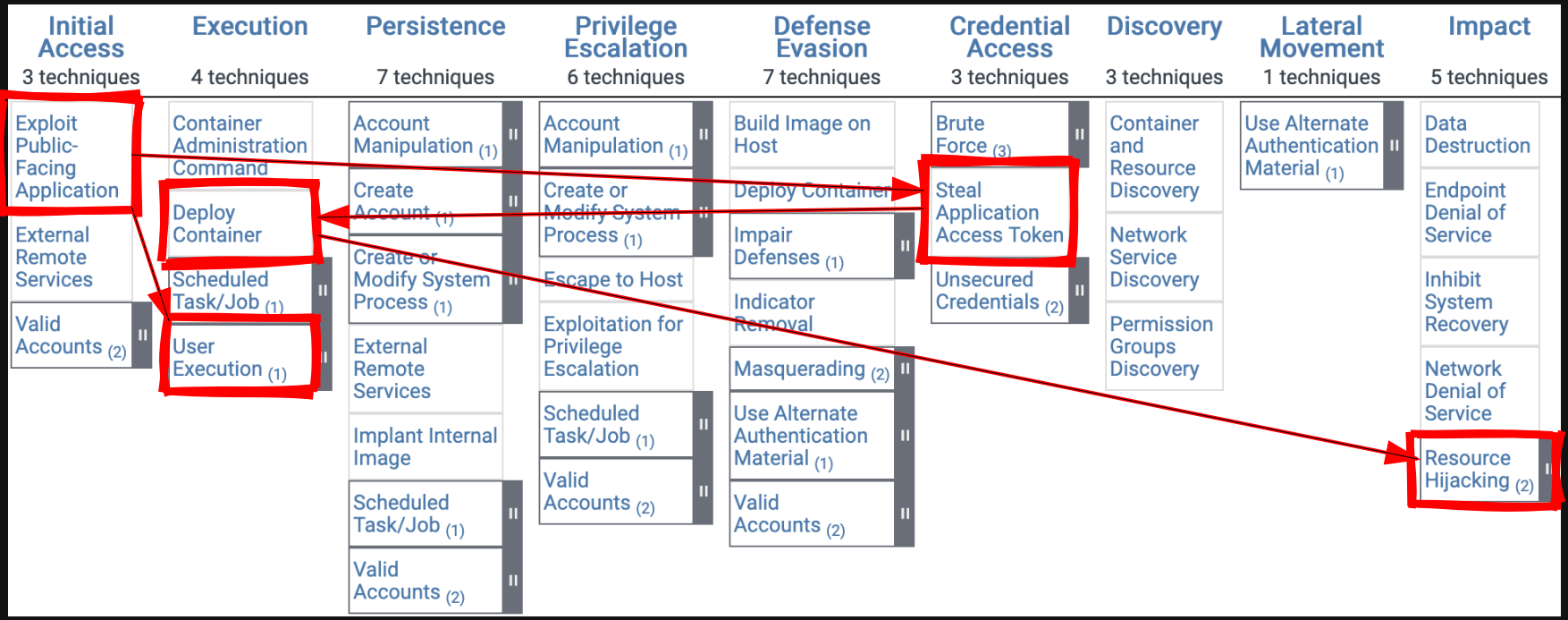



Wiz' Cloud Threat Landscape




Sysdig: Scarleteel 2.0

# MITRE ATT&CK

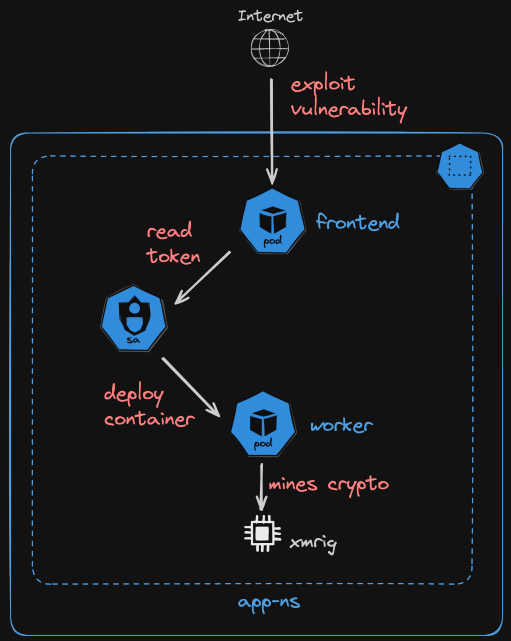



MITRE ATT&CK - Containers Matrix

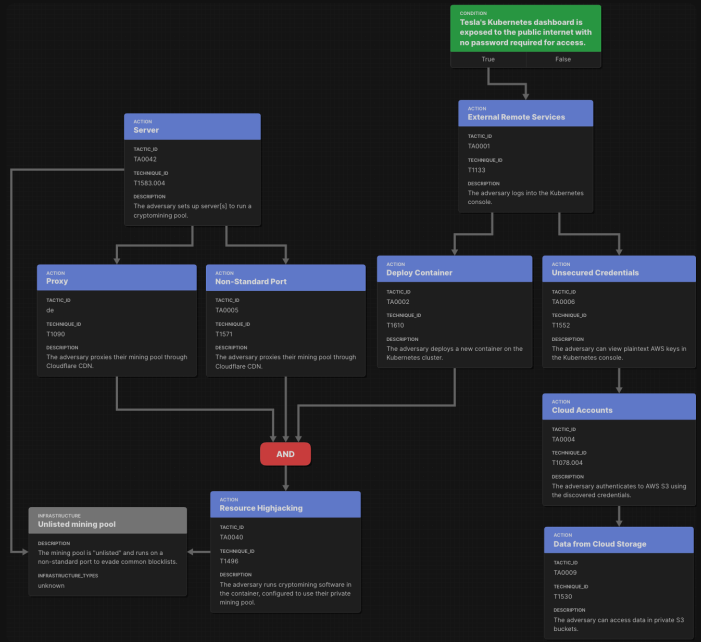
# Attack Graph

= combination of TTPs

## Resource-centric

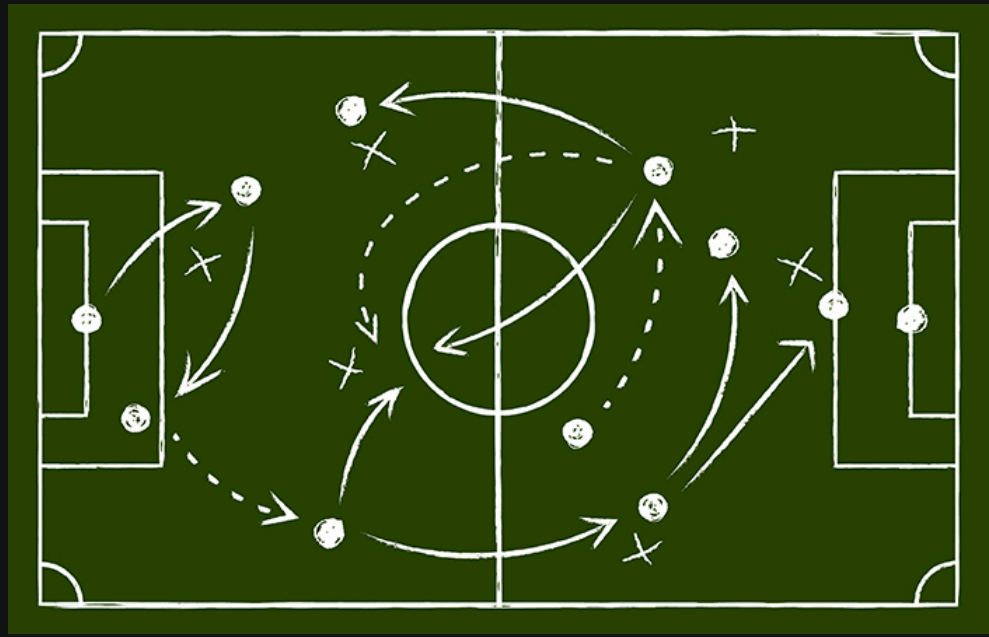



## Attack-centric



# Attack Path Analysis

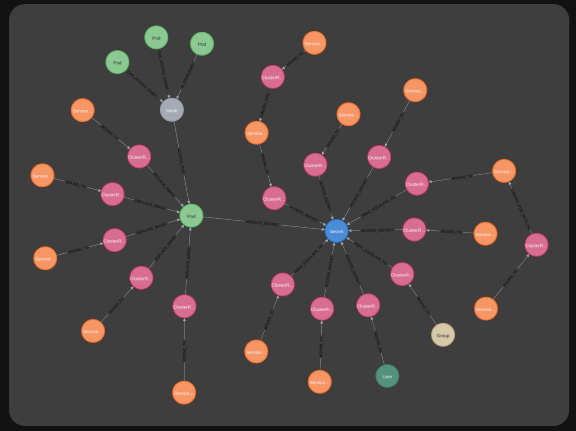
- *Models* all possible attack paths
- Full visiblity of environment
- Contextualizes findings
- Enables advanced analysis



# Attack Path Analysis Tools

## IceKube


- 25 TTPs
- uses Neo4J
- Query using Cypher

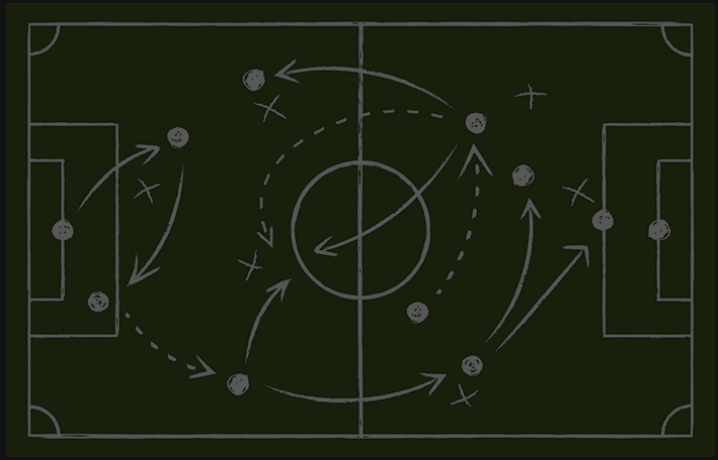


## KubeHound


- 25 TTPs
- uses JanusGraph
- Jupyter Notebook for analysis
- experimental automation features

# Getting real

## Attack Path Analysis



## Adversary Emulation

# Adversary Emulation

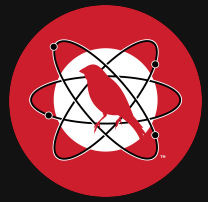
- Perform attack on real environments
- Evalates the effectiveness of security controls
- Varying degree of realism:

# Atomic Emulation

- detonate single TTPs
- primarily use-case:
  - test processing pipeline
  - manage detections

## Tools

### Atomic Red Team



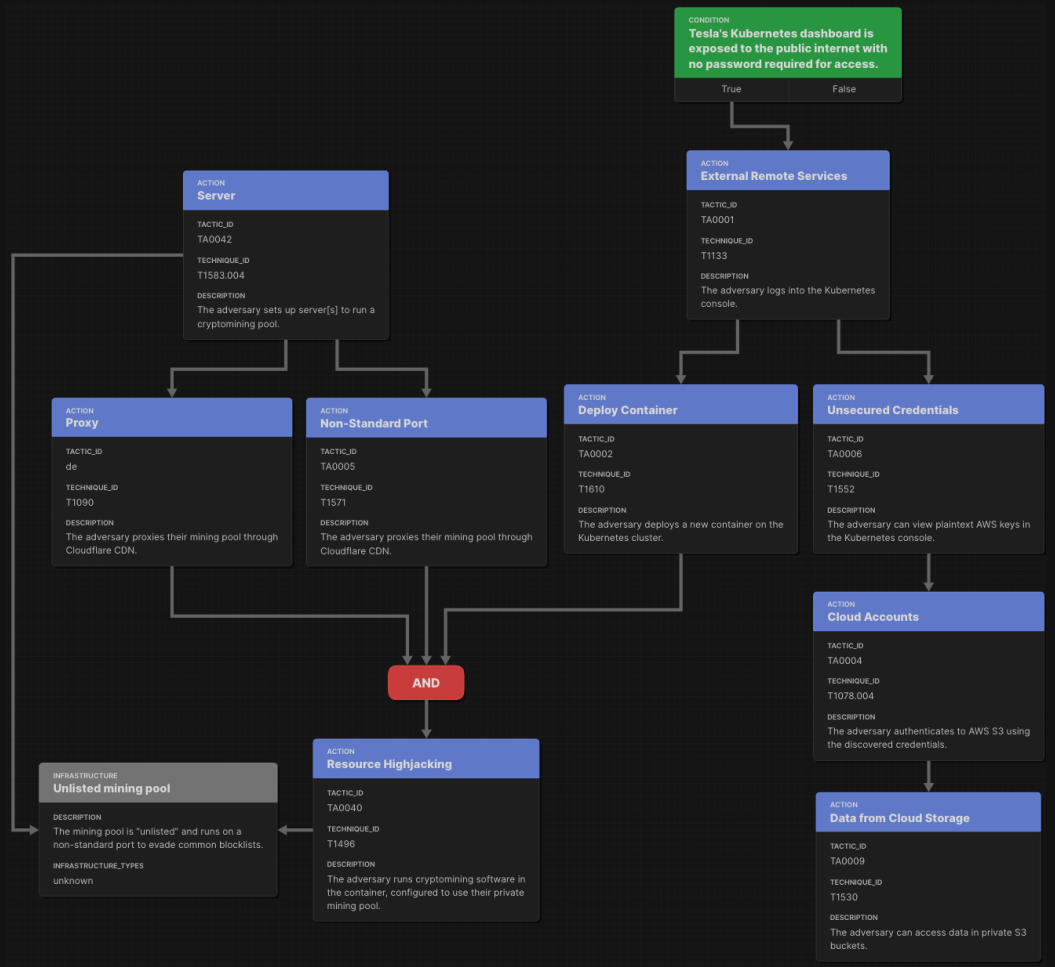
- 1700+ TTPs
- focus on OS-based TTPs
- ~10 TTPs for Docker + K8s

### Stratus Red Team


- 50+
- focuses on AWS, Azure, GCP
- ~8 TTPs for K8s

# Planned Emulation

- aka "Micro emulations"
- easy to automate
- Validate atomic + chain analytics
- good for reproducing scenarios



# Planned Emulation: Tools

## Mitre Caldera

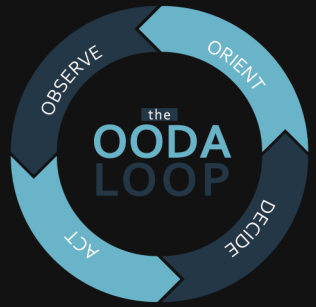

- oldest and most mature emulation tool (2015)
- primary for enterprise environments
- no special K8s support
- big plugin ecosystem
- supports automated planning

## Leonidas

- similar to Stratus Red Team
- allows chaining of TTPs
- runs as workload inside K8s cluster
- supports only `kubectl` -based TTPs for K8s

# Realistic Emulation

- "Fog of War"
- a red team engagement




## Use Cases

- Evaluate incident response plans
- testing more sophisticated defenses
  - Moving Target Defense
  - Deception

## Tools

CALDERA

Ran

# Demo

# Take-aways

Adopt an attacker's mindset to assess your effective security.

## Attack Path Analysis

- Contextualize security findings
- Uncover dangerous combinations
- Plan for improvements

## Adversary Emulation

- Validate security controls
- Improve detection & response
- Show value of more advanced defenses