

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



Open Policy Agent

CNCF GRADUATED



TUF

CNCF GRADUATED



CNCF INCUBATING



Kubescape

CNCF INCUBATING



CNCF INCUBATING



CNCF INCUBATING

AIRLOCK



alcide

API Clarity



apolicy

aqua

ARMO



Aserto

authentic

bank-vaults

BLACKDUCK

BLOOMBASE

Bouncy Castle

Boundary



bpfman

CAPSULE8

Cartography

cerbos

长亭科技 CHAITIN

Check Point

checkov

CHEF INSPEC

clair

CLOUDMATS

CONFIDENTIAL CONTAINERS

ContainerSSH

COPA

Curiefense

移动云

Datica

dex

DOSEC 小佑科技

EJBCA by Keyfactor

EXTERNAL SECRETS OPERATOR

Fairwinds Insights

FOSSA

FQSSID

Fugue

GitGuardian

Goldilocks

Grafeas

grype

Hexa

Keylime

KICS

kube-bench

kube-hunter

kubearmor

KubeLinter

KUBEWARDEN

matano

Metarget

mondoo

默安科技 MoreSec

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 QINTENG.CN

RAD SECURITY

RBAC LOOKUP

rbac manager

Rudder

scribe

SignServer by Keyfactor

sigstore

Slim toolkit

snyk

sonatype

SONOBUOY

SOPS

SPYDERBAT

STACKHAWK

StackRox

syft

sysdig SECURE

Teleport

探真科技 TensorSecurity

terrascan

tetragon

ThreatMapper

TIGERA

TOPAZ

trivy

TREND MICRO

vArmor

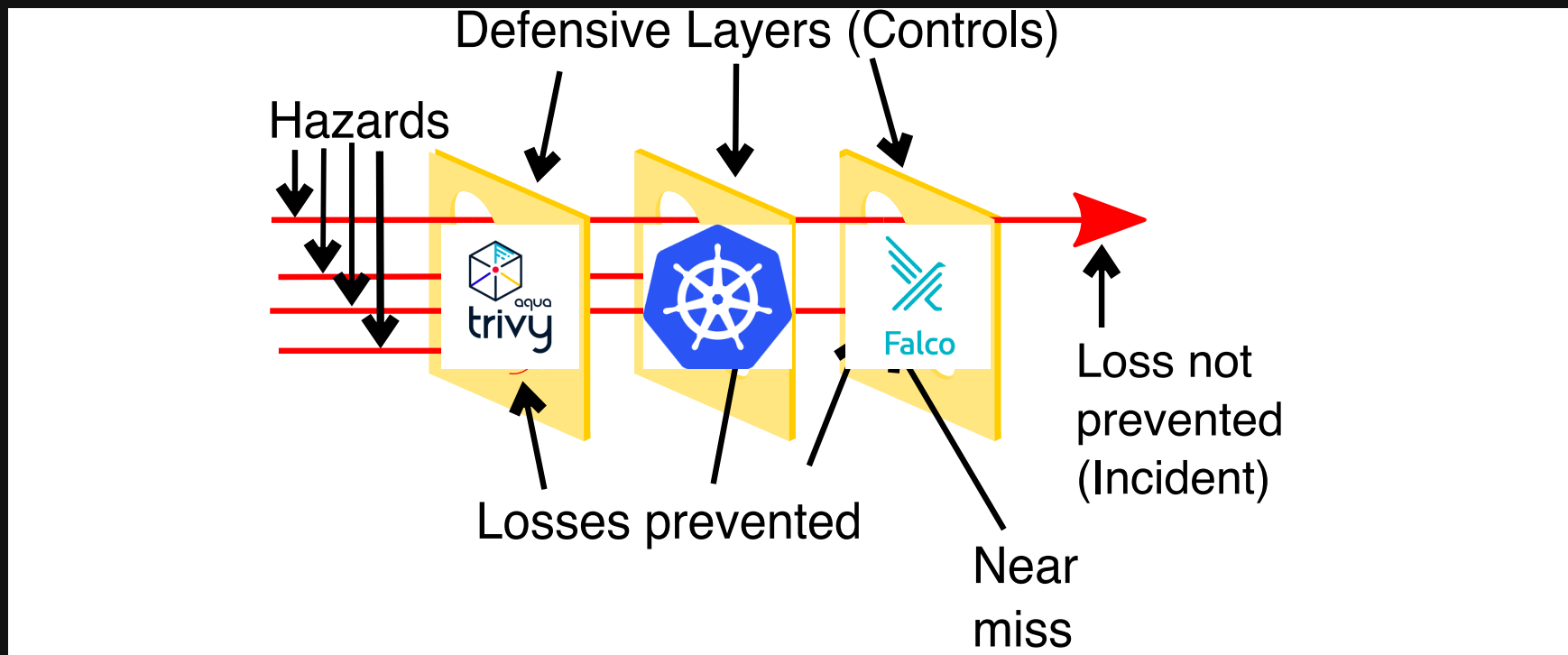
VEINMIND

WhiteSource

Zettaset

ZITABEL

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
libcrypto.1.1	CVE-2019-1543		1.1.1a-r1	1.1.1b-r1	openssl: ChaCha20-Poly1305 with long nonces
libcrypto.1.1	CVE-2020-1967	HIGH			
libcrypto.1.1	CVE-2021-23840	HIGH			
libcrypto.1.1	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

Cloud Threat Landscape

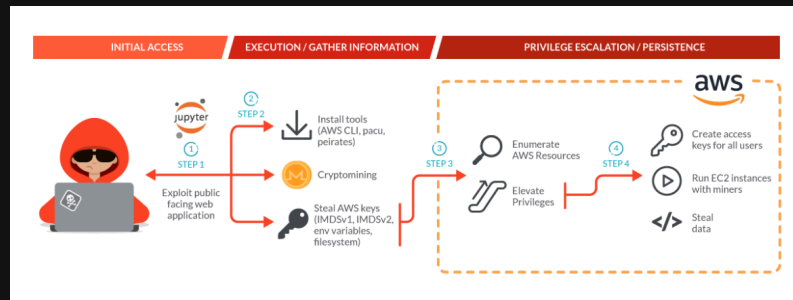
Incidents Actors Techniques Defenses ABC Poster Periodic Table Tools Targeted Technologies About RSS STX Back to

Incidents

General Information Tools, Techniques & Techs Incidents Campaigns Supply Chain Attacks Resource Hijacking

Name	Pub. date	Actors	Initial access	Impact	Type	Status
Longflow Vulnerability Exploited to Deliver Fiodia Botnet	June 17, 2025	Unknown	1-day vulnerability	Denial of service, Resource hijacking	Campaign	Finalized
J\$FireTruck: Malicious JavaScript Campaign Using Obfuscation	June 12, 2025	Unknown	End-user compromise	Resource hijacking	Campaign	Finalized
Teamfiltration Account Takeover Campaign	June 11, 2025	Unknown	End-user compromise	Data exfiltration	Campaign	Stub
NPM Supply Chain Attack Compromises 16 Popular React Native and Quackstack Packages	June 7, 2025	Unknown	Supply chain vector	Supply chain attack	Campaign	Finalized
Open WebUI Misconfiguration Exploited for Cryptojacking	June 3, 2025	Unknown	Software misconfig	Resource hijacking	Campaign	Finalized
Cryptojacking Campaign Targets Misconfigured DevOps Tools	June 2, 2025	JNX-0132	Software misconfig	Resource hijacking	Campaign	Finalized
Earth.Lamia Custom Toolkit Targets Multiple Sectors via Web Vulnerabilities	May 29, 2025	Earth.Lamia	1-day vulnerability, Web vuln	Data exfiltration	Campaign	Finalized
Dragonforce Exploits SimpleHelp Vulnerabilities in Ransomware Campaign	May 28, 2025	Dragonforce	1-day vulnerability, Supply ch	Ransomware	Campaign	Finalized
Coordinated One-Day Cloud Scanning Operation Targets 75 Exposure Points	May 28, 2025	Unknown	1-day vulnerability, Software	None	Campaign	Finalized
Mimo Exploits Craft CMS CVE to Deploy Cryptominer and Proxyware in Coordinated Campaign	May 27, 2025	Mimo operator	1-day vulnerability	Resource hijacking	Campaign	Finalized
WordPress PMM RCE Vulnerability Chain Exploited in the Wild	May 20, 2025	Unknown	1-day vulnerability	Data exfiltration	Campaign	Not started
UTO-Q-015 Exploits 0-Days for Espionage in Asia	May 19, 2025	UTO-Q-015	0-day vulnerability, 1-day vuln	Data exfiltration	Campaign	Finalized

Wiz' Cloud Threat Landscape



Sysdig: Scarleteel 2.0

MITRE ATT&CK

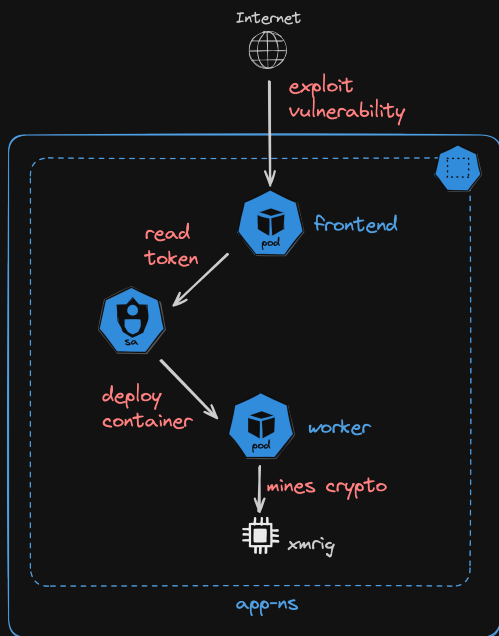
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact
3 techniques	4 techniques	7 techniques	6 techniques	7 techniques	3 techniques	3 techniques	1 techniques	5 techniques
<div>Exploit Public-Facing Application</div> <div>External Remote Services</div> <div>Valid Accounts (2)</div>	<div>Container Administration Command</div> <div>Deploy Container</div> <div>Scheduled Task/Job (1)</div> <div>User Execution (1)</div>	<div>Account Manipulation (1)</div> <div>Create Account (1)</div> <div>Create or Modify System Process (1)</div> <div>External Remote Services</div> <div>Implant Internal Image</div> <div>Scheduled Task/Job (1)</div> <div>Valid Accounts (2)</div>	<div>Account Manipulation (1)</div> <div>Create or Modify System Process (1)</div> <div>Escape to Host</div> <div>Exploitation for Privilege Escalation</div> <div>Scheduled Task/Job (1)</div> <div>Valid Accounts (2)</div>	<div>Build Image on Host</div> <div>Deploy Container</div> <div>Impair Defenses (1)</div> <div>Indicator Removal</div> <div>Masquerading (2)</div> <div>Use Alternate Authentication Material (1)</div> <div>Valid Accounts (2)</div>	<div>Brute Force (3)</div> <div>Steal Application Access Token</div> <div>Unsecured Credentials (2)</div>	<div>Container and Resource Discovery</div> <div>Network Service Discovery</div> <div>Permission Groups Discovery</div>	<div>Use Alternate Authentication Material (1)</div>	<div>Data Destruction</div> <div>Endpoint Denial of Service</div> <div>Inhibit System Recovery</div> <div>Network Denial of Service</div> <div>Resource Hijacking (2)</div>

MITRE ATT&CK - Containers Matrix

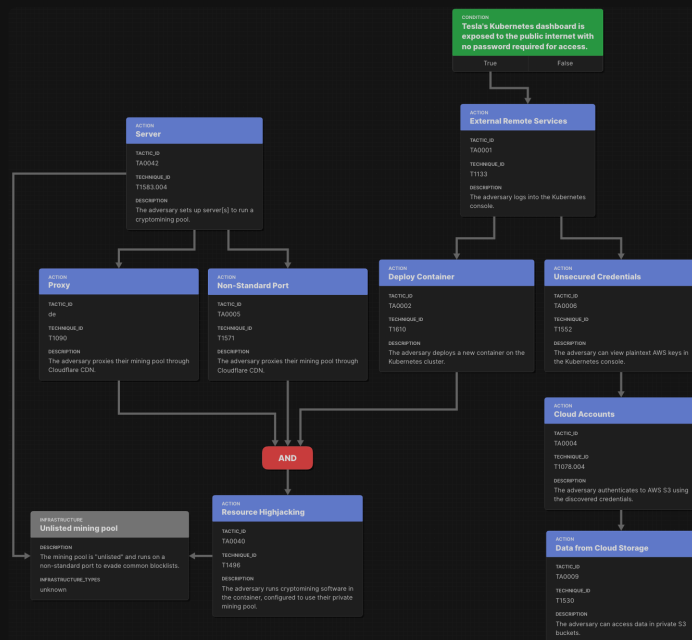
Attack Graph

= combination of TTPs

Resource-centric

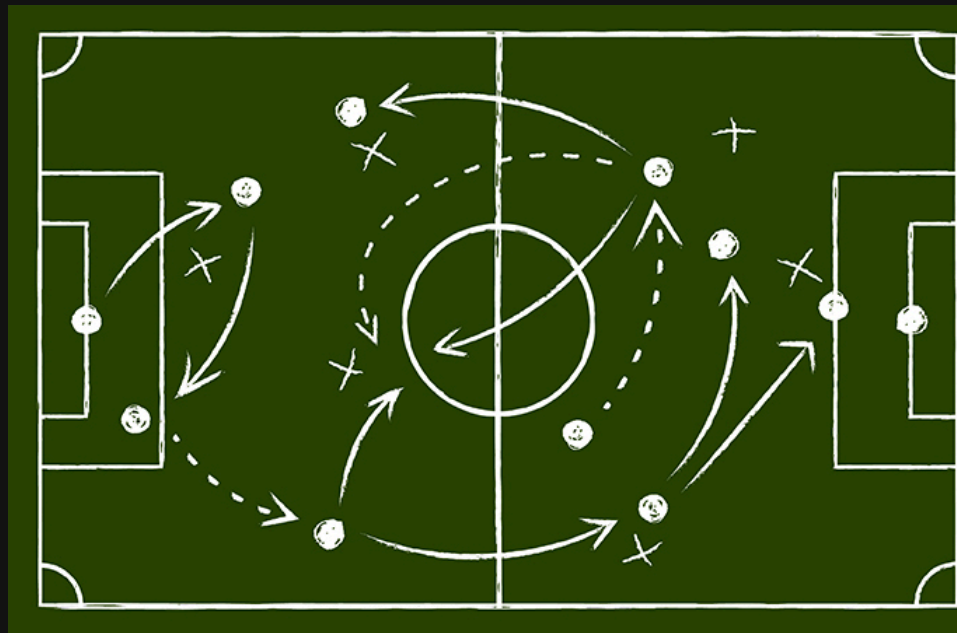


Attack-centric



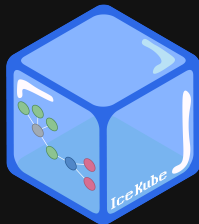
Attack Path Analysis

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

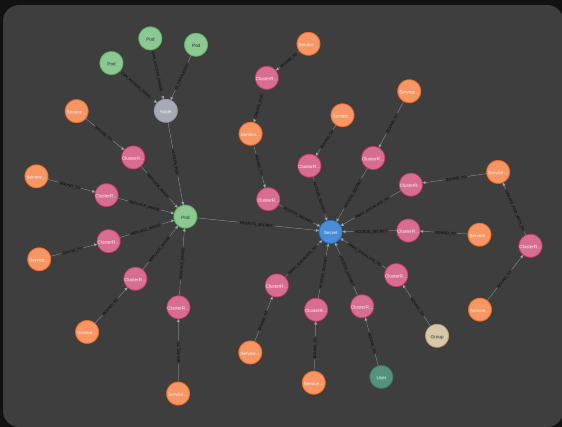


Attack Path Analysis Tools

IceKube



- 25 TTPs
- uses Neo4J
- Query using Cypher



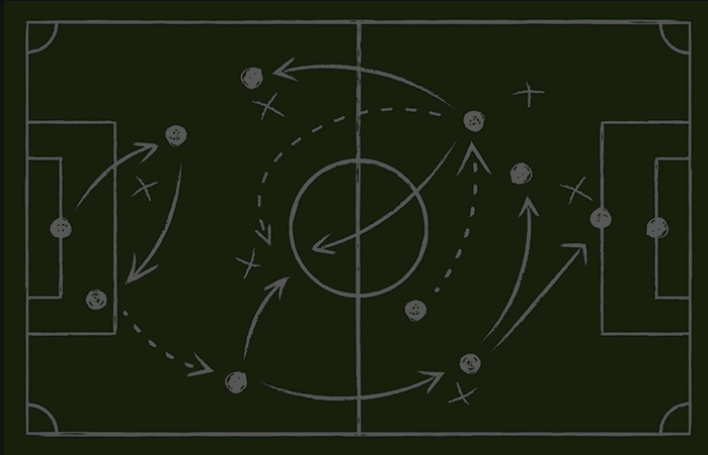
KubeHound



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

Getting real

Attack Path Analysis

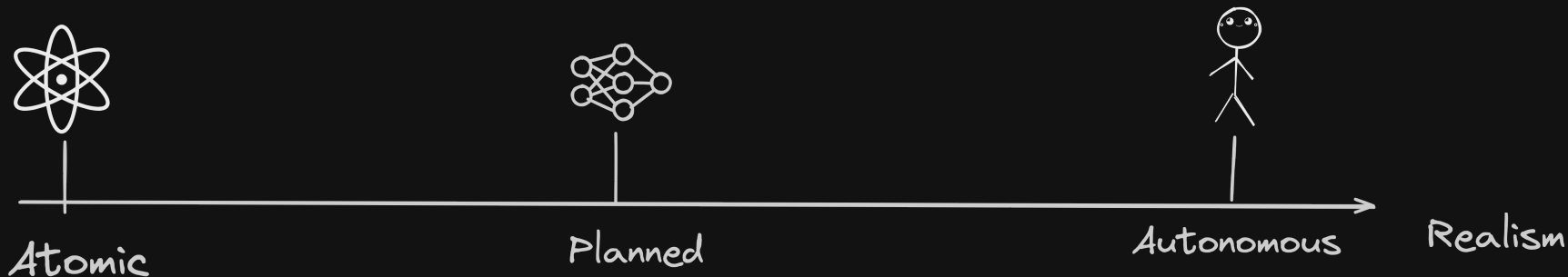


Adversary Emulation



Adversary Emulation

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

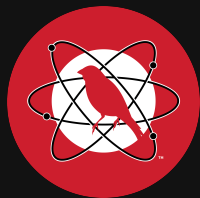


Atomic Emulation

- 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

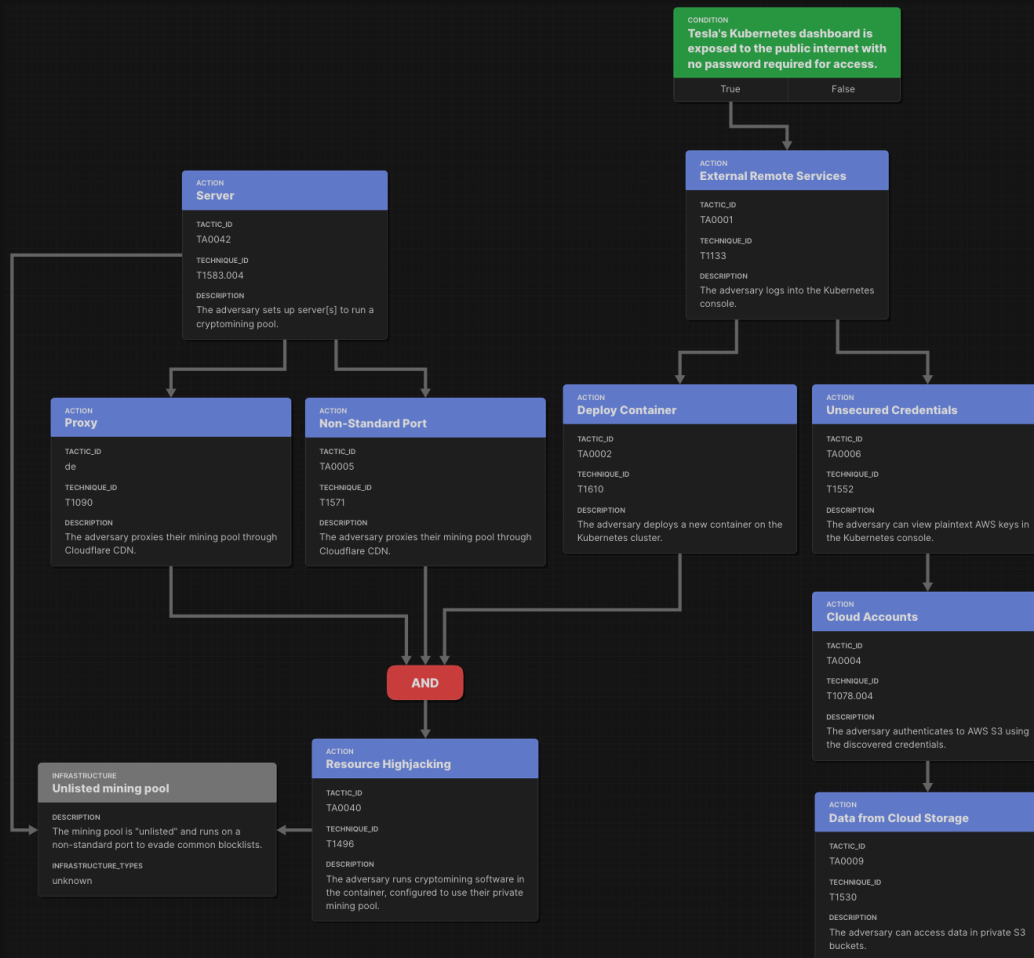
Stratus Red Team



- 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

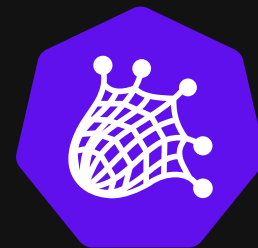


Use Cases

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



Tools



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

