Cloud native Threat Detection

Using Trivy and Falco to Detect Malware and exploitable binaries in a Kubernetes Environment.

08 September 2022

Thought Machine

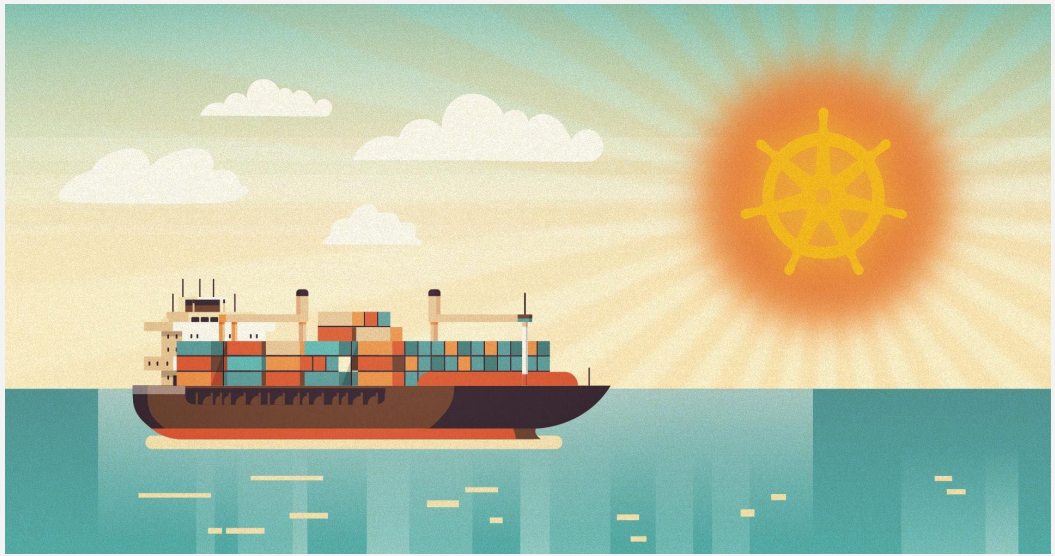
Introduction

Marco Mancini

Tech Lead - Threat Operations

https://MarcoJMancini.com/about/

Cloud native tech stack

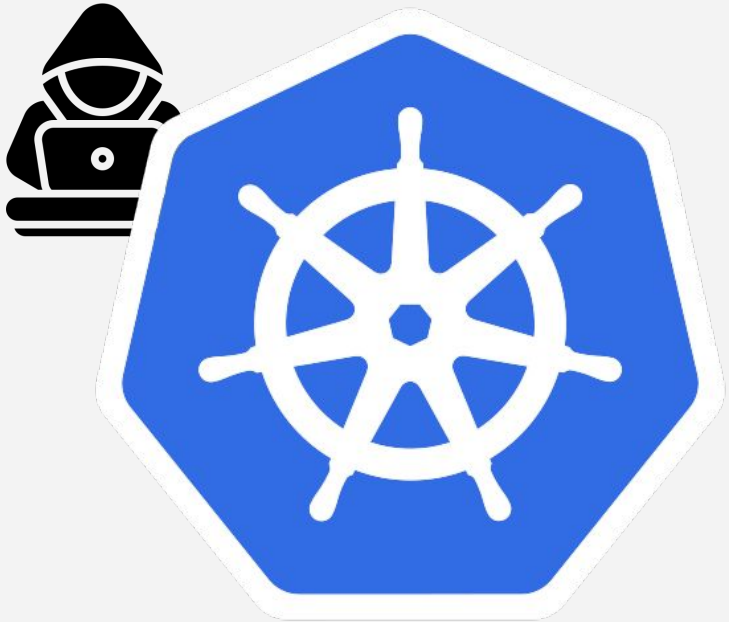


Source: Linode “Kubernetes Simplified: Managing Your Containers”

- Microservices architecture
- 100+ deployments per day
- Kubernetes
- Multi-cloud
- Cloud Native

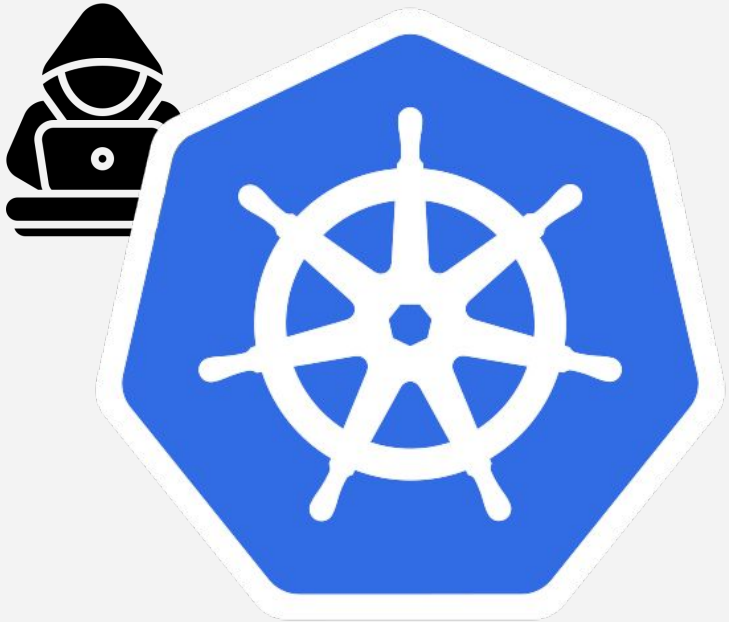
Kubernetes issues

- Vulnerable images on containers
- Malware in clusters
- Misconfigurations on clusters
- Among other fun stuff!



Kubernetes issues

- **Vulnerable images on containers**
- **Malware in clusters**
- Misconfigurations on clusters
- Among other fun stuff!



What is Falco?

Falco is an open source runtime security tool

What does Falco do? *[From the docs]*

- Falco uses system calls to secure and monitor a system, by:
  - Parsing the Linux system calls from the kernel at runtime
  - Asserting the stream against a powerful rules engine
  - Alerting when a rule is triggered

We can also use the alerting to baseline behaviour that is not malicious but it's of interest!

What is Trivy?

Trivy is an open source scanner. Ideal for kubernetes

Targets:

- Container Image
- Filesystem
- Git repository (remote)
- **Kubernetes cluster or resource**

Scanners:

- OS packages and software dependencies in use (SBOM)
- **Known vulnerabilities (CVEs)**
- IaC misconfigurations

Sensitive information and secrets

And now has a k8s operator!

Detection engineering

How to detect threats!

- Identify threats, weaknesses and attackers
- Capture context to prioritize better, different data sources can be merged for added context.

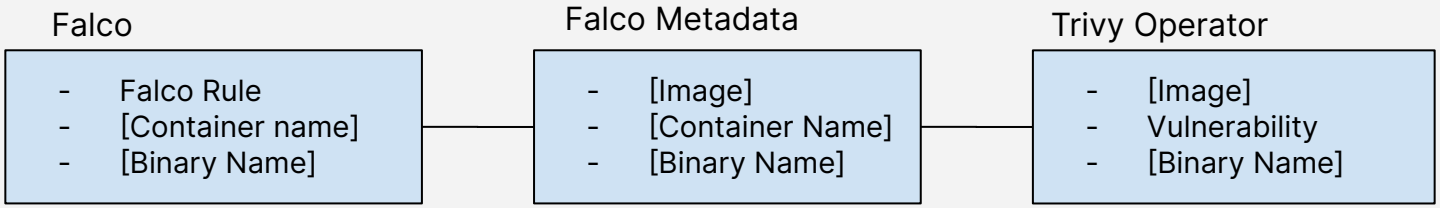
Idea!

- Falco gets context on the system
- Trivy gets context on vulnerabilities

Prioritise vulnerabilities which are exposed

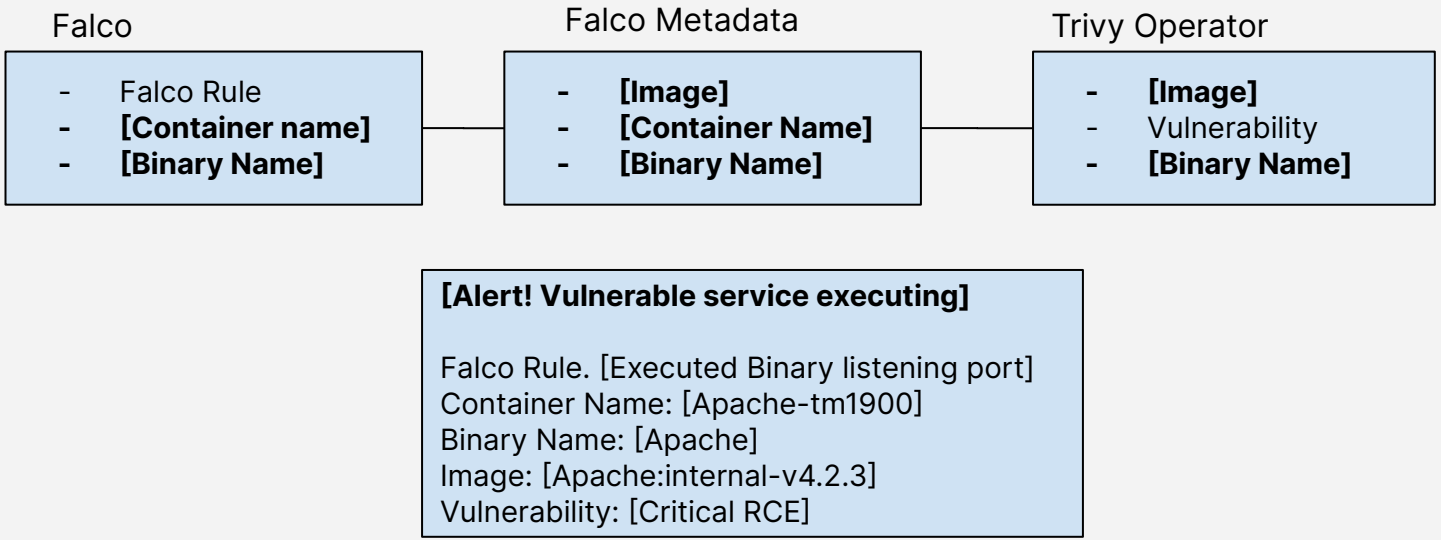
Detection context

- Vulnerable web servers cause breaches!
- Kubernetes clusters can have thousands of instances of web servers
  - **Correlate with trivy and Falco to identify packages that are internet exploitable the moment they appear in the environment.**

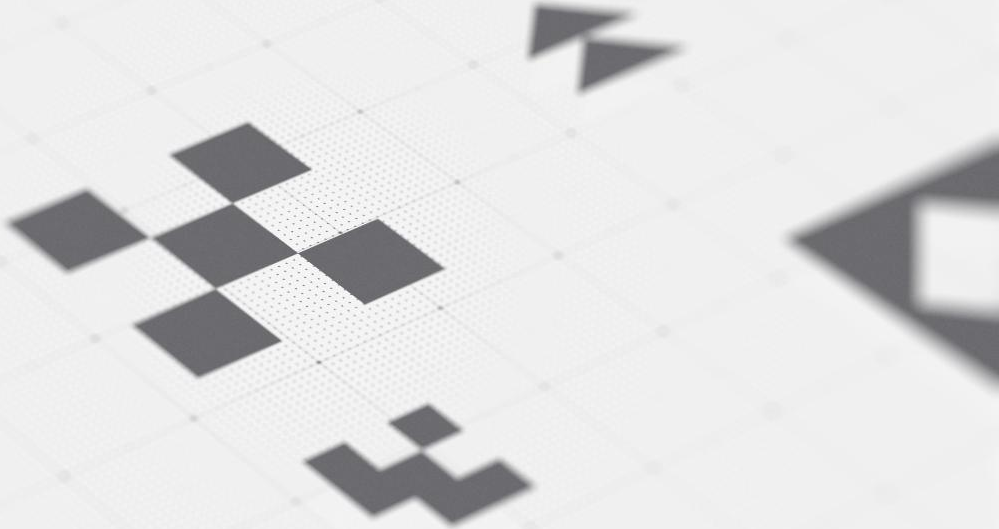


[Alert! Vulnerable service executing]

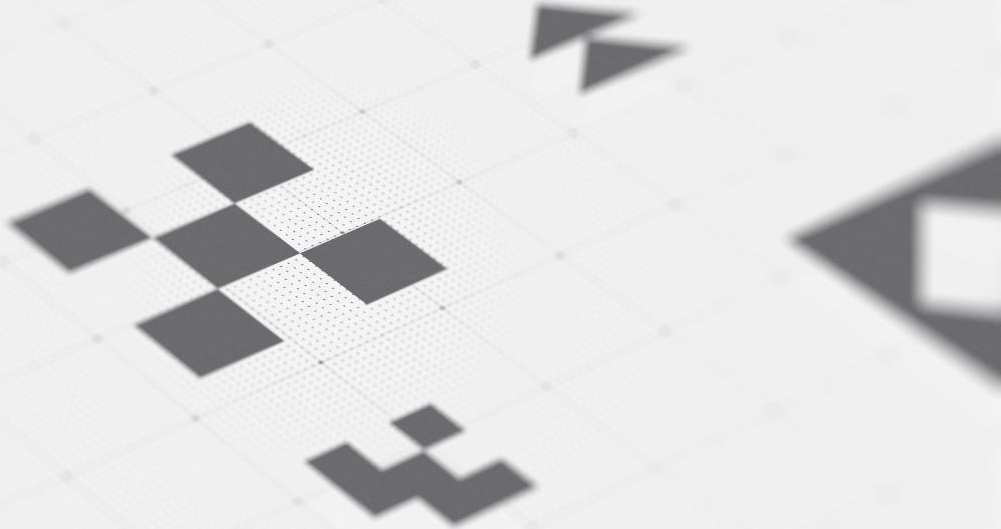
Alert outcome



Thank you



We are hiring!



Security Engineering at Thought Machine

Engineering guiding principles

- **Engagement by everyone** - We all work together to create as a team
- **Cloud-native** - all our infrastructure lives in Kubernetes
- **Standardisation of audit data formatting**
- **Feedback early to encourage experimentation**
- **Configuration as code** - to the extent possible, we commit our configuration to our repositories
- **Deploy frequently, deploy automatically on commit** - we deploy our infrastructure multiple times a day, including our Elasticsearch clusters
- **Analysts are engineers and engineers are analysts** - the entire team does on-call, the entire team helps maintain our infrastructure
- **Automated configuration of security monitoring** - via Puppet and Terraform recipes

Threat Detection Guiding principles

- **Detection as code** - All our alerts are defined as code and managed with git
- **Alert documentation** - All alerts have an associated documentation to speed the learning of new analysts.
- **Correlate information** - We integrate data from different sources to speed investigation.
- **Analyst over the loop** - Our detections need to scale so we create systems that move at machine speed and are reviewed by analysts.
- **Empowered analyst** - Analyst are empowered to review and propose a fix to alerts after an incident.
- **Support the business** - We integrate our alerts into business and engineering processes to nudge the best practices.
- **Simulations of incidents** - Create scenarios for the IR team to respond and train processes before a disaster

Thought Machine Applications!

Security Engineering roles

- https://thoughtmachine.avature.net/careers/JobDetail/Application-Security-Engineer-United-Kingdom/33

Threat Operations roles

- https://thoughtmachine.avature.net/careers/JobDetail/Security-Engineer-United-Kingdom/113