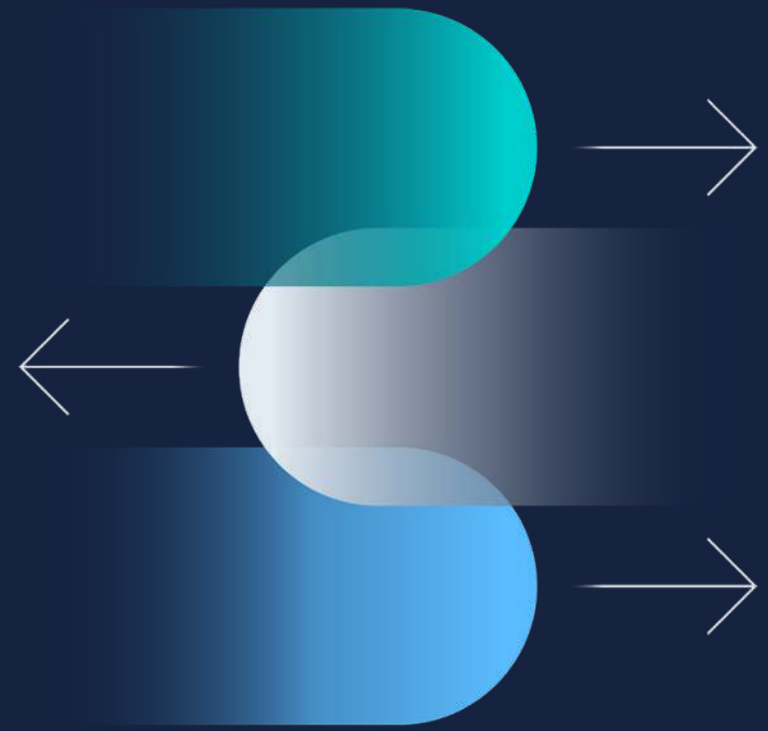
FORM3
FINANCIAL CLOUD

The Hacker's Guide to Kubernetes



Patrycja Wegrzynowicz

Lead Engineer

@yonlabs

Hello! 👋

- 20+ professional experience

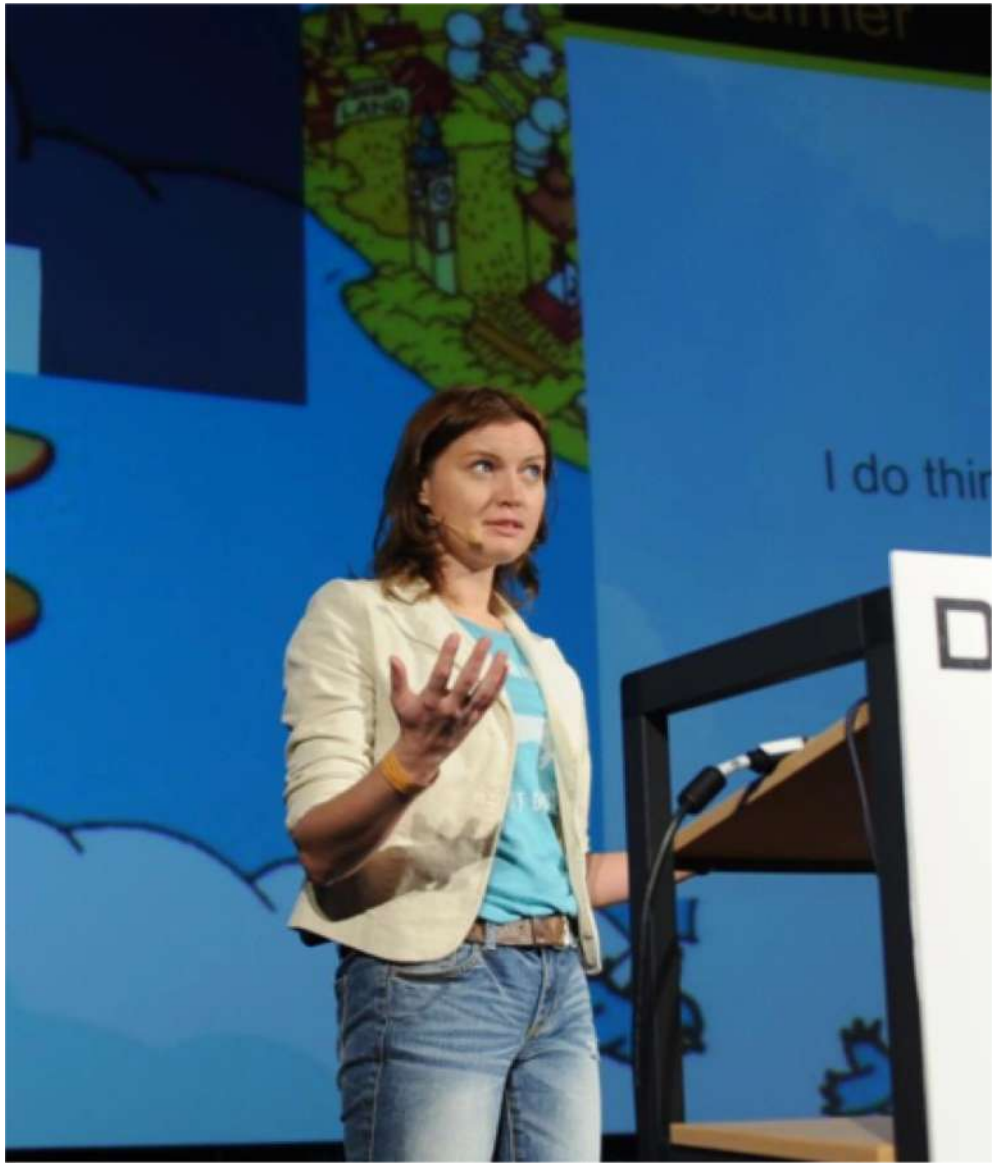
  software engineer, architect, researcher, head of R&D
- Author and speaker

  JavaOne, CodeOne, Devoxx, JFokus, JavaZone, and more
- Top 10 Women in Tech in Poland
- Oracle Groundbreaker Ambassador
- Form3, Financial Cloud

  Lead SRE Engineer
- Founder at Yon Labs

  Automated tools for detection and refactoring of software defects.

  Performance, security, concurrency.



Form3, Financial Cloud

Business Model 💸

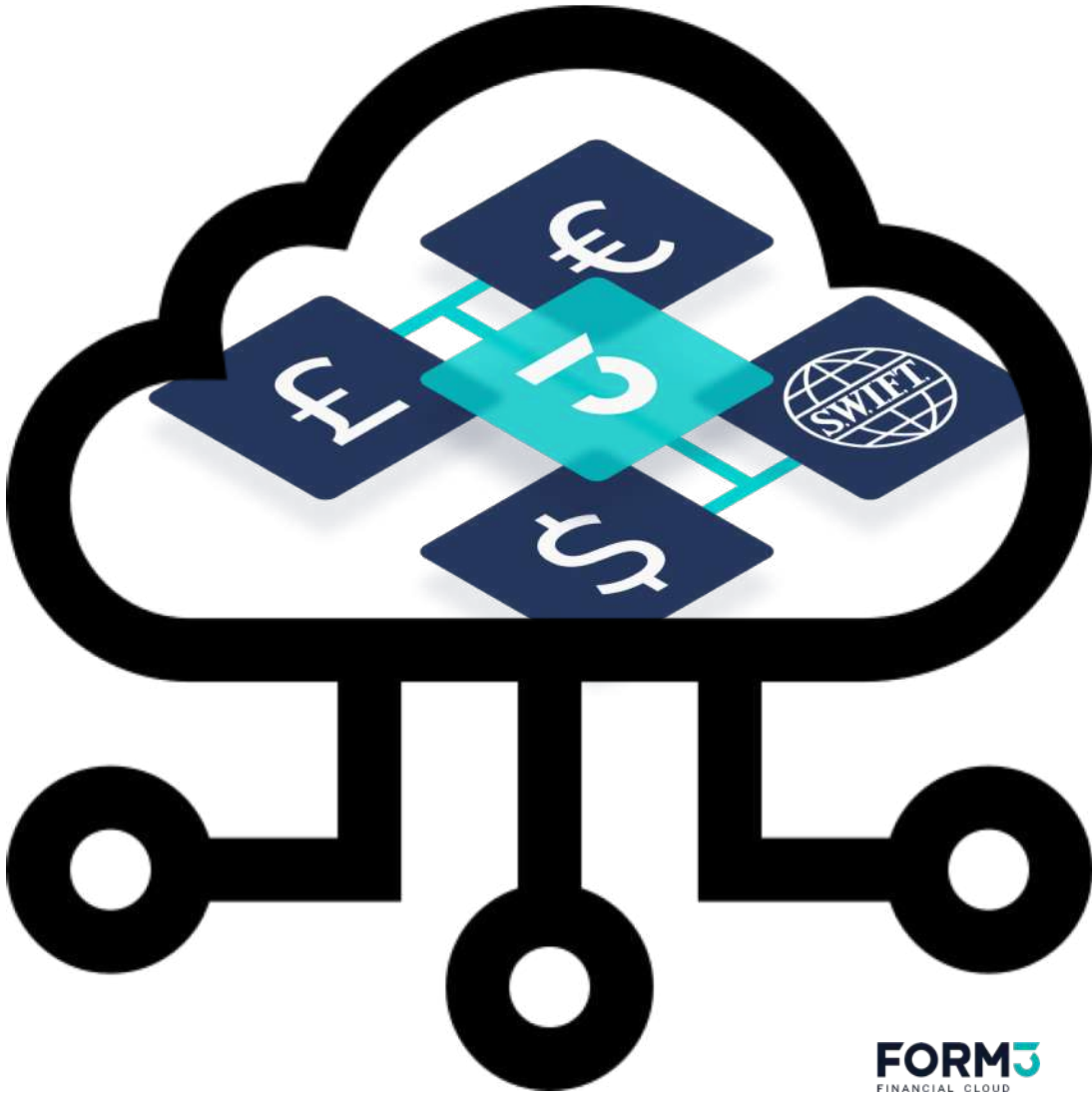
- Provides a payment platform for financial institution
- Integrates across multiple payment schemes
- Makes integration easier and quicker

Work Model 😎☁

- Fully remote
- Pair programming
- Only senior engineers

Technology 🚀

- Multi-cloud platform: AWS, GCP, Azure
- Microservices: (mostly) Go and (little) Java
- Infrastructure as Code: Terraform



FORM3
FINANCIAL CLOUD

Agenda

01 Introduction to Kubernetes Architecture

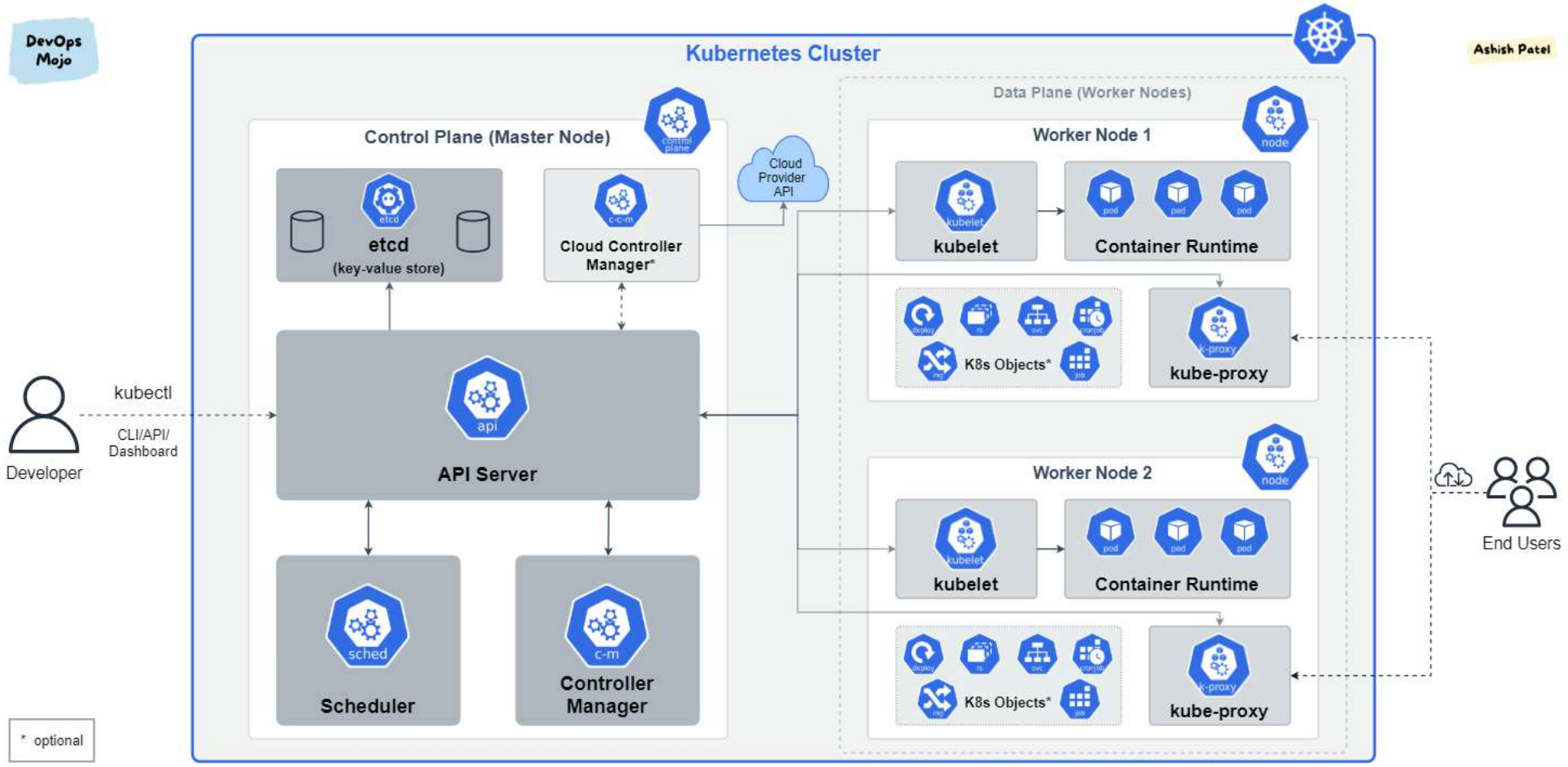
02 Introduction to OWASP Kubernetes Top 10

03 Demos

04 Summary

Introduction to Kubernetes Architecture

Kubernetes Components



Source: https://medium.com, Kubernetes - Architecture Overview by Ashish Patel

Introduction to OWASP Kubernetes Top 10

OWASP
Open Web Application Security Project

OWASP Kubernetes Top 10 2022

- K01 Insecure Workload Configuration
- K02 Supply Chain Vulnerabilities
- K03 Overly Permissive RBAC Configurations
- K04 Lack of Centralized Policy Enforcement
- K05 Inadequate Logging and Monitoring
- K06 Broken Authentication Mechanisms
- K07 Missing Network Segmentation Controls
- K08 Secrets Management Failures
- K09 Misconfigured Cluster Components
- K10 Outdated and Vulnerable Kubernetes Components

FORM3
FINANCIAL CLOUD

Demos – 101 Kubernetes hacking

Let the fun begin!

Demo Fun Time – Overview

- **Demo application**
  https://kubecon.yonlabs.com
  (or checkout https://twitter.com/yonlabs)
  register a new account
  each account has a secret data
  log in
  wait to be hacked :D

- **Objective**
  to hack your accounts and learn your secrets
  hacking 101

Demo #1

Demo #1

Open kubelet API

--anonymous-auth Default: true

Enables anonymous requests to the Kubelet server. Requests that are not rejected by another authentication method are treated as anonymous requests. Anonymous requests have a username of `system:anonymous`, and a group name of `system:unauthenticated`. (DEPRECATED: This parameter should be set via the config file specified by the Kubelet's `--config` flag. See https://kubernetes.io/docs/tasks/administer-cluster/kubelet-config-file/ for more information.)

--authorization-mode string

Authorization mode for Kubelet server. Valid options are `AlwaysAllow` or `Webhook`. `Webhook` mode uses the `SubjectAccessReview` API to determine authorization. (default "AlwaysAllow" when `--config` flag is not provided; "Webhook" when `--config` flag presents.) (DEPRECATED: This parameter should be set via the config file specified by the Kubelet's --config flag. See https://kubernetes.io/docs/tasks/administer-cluster/kubelet-config-file/ for more information.)

Demo #1

Vulnerabilities

- Open kubelet API

  K09 Misconfigured Cluster Components
- Containers: writable filesystem

  K01 Insecure Workload Configuration
- Containers: run as root

  K01 Insecure Workload Configuration
- Containers: quite a few tools available

  reverse shell possible
- Networking: unencrypted traffic
- Networking: open egress to Internet

Demo #2

Demo #2

Vulnerabilities

- RCE in one (!) Kubernetes deployment

  K10 Outdated and Vulnerable Components
- Missing network segmentation

  K07 Missing Network Segmentation Controls
- Container: quite a few tools available

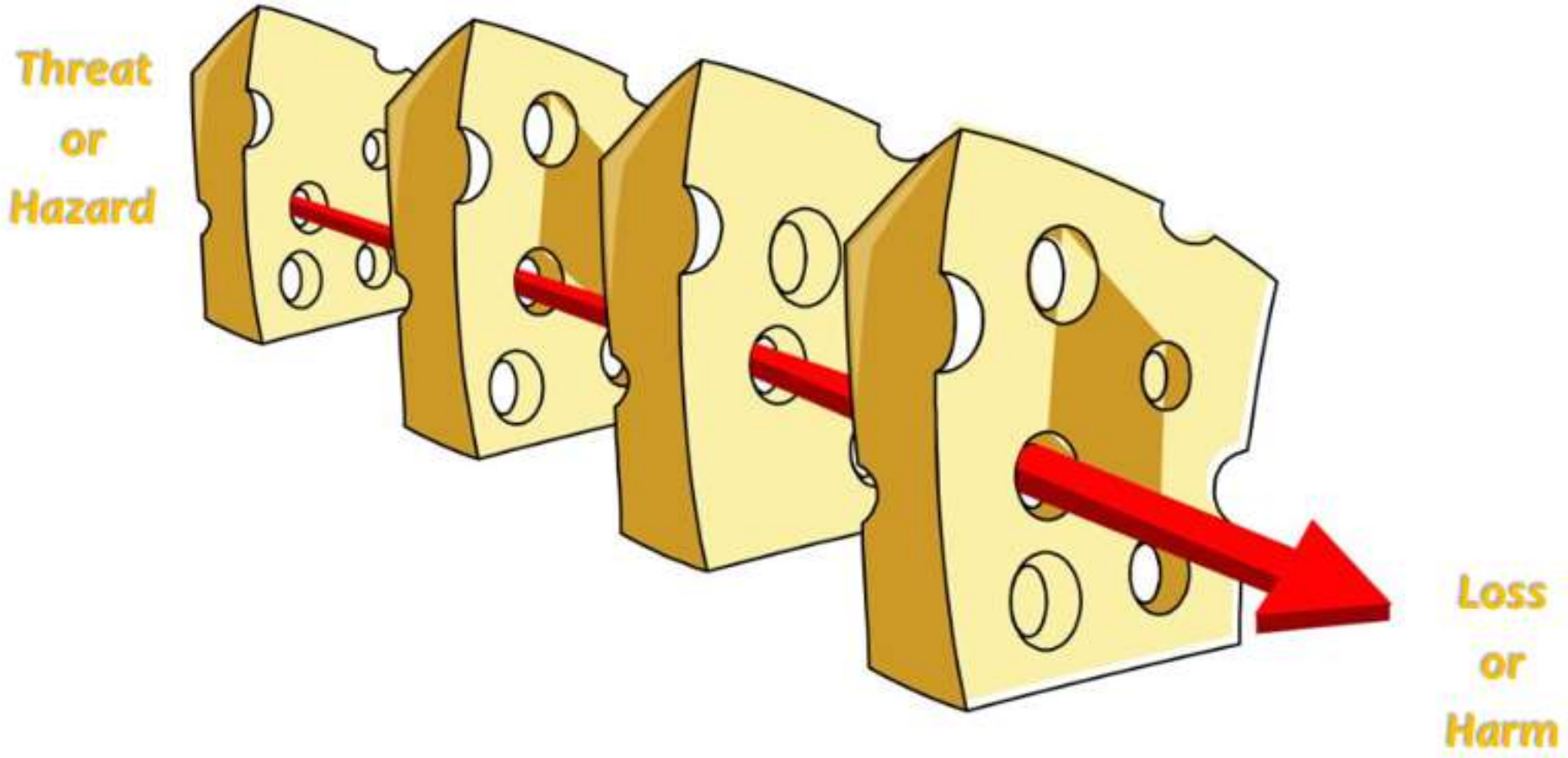
  reverse shell possible
- Anonymous access to Redis

Summary

Kubernetes Security

FORM3
FINANCIAL CLOUD

Swiss Cheese Security Model



A fool with a tool is only a fool

FORM3
FINANCIAL CLOUD

Continuous Learning

FORM3
FINANCIAL CLOUD

Thank you!

@yonlabs