# DevSecOps in Practice

28.9.2023 - Manuel Jeckelmann

Low Altitude Alpinism for Engineers

# Who am I?

Manuel Jeckelmann

Graduated HEIA-FR in 2008

Security Lead/CISO at FAIRTIQ

linkedin.com/in/jeckelmm
mj@fairtiq.com

# Introducing FAIRTIQ

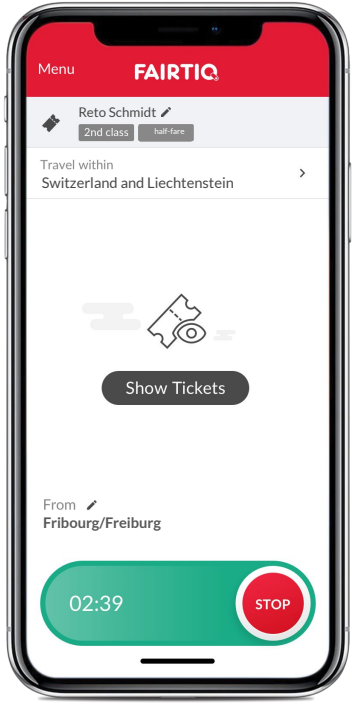
FAIRTIQ is the easiest way to public transportation

# Introducing FAIRTIQ

Active in ~30 regions in CH, DE, AT, FR, BE, and more

Total trips processed: 128’000’000

Number of Employees: 130



# A Tech & Product Start-up

You build it, you run it.

High effectiveness: Lean & Agile.

Quality is the highest Priority.


# “Sec” Activities in DevSecOps

Base Idea

Implementation at FAIRTIQ



# “Sec” Activities in DevSecOps

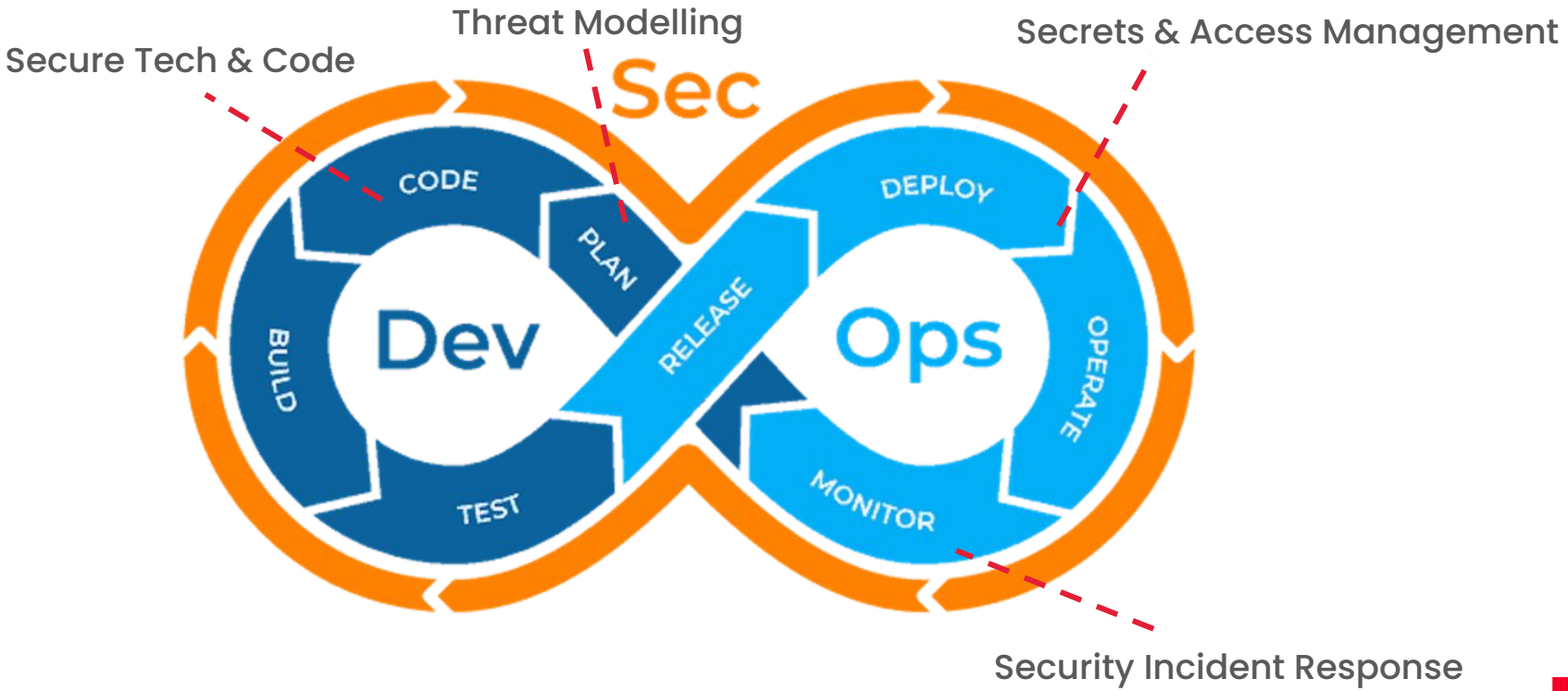
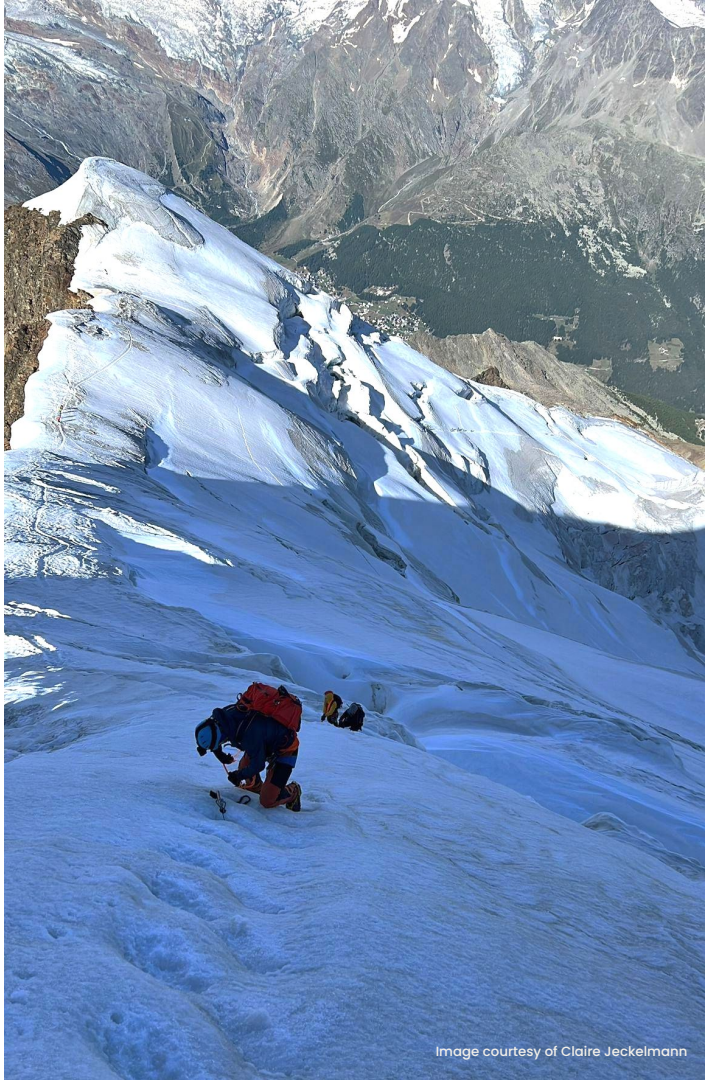



Image source: https://www.pagerduty.com/blog/devsecops-ops-guide/

# Threat Modelling

"What can go wrong?"
– Every engineer
(before they start coding)



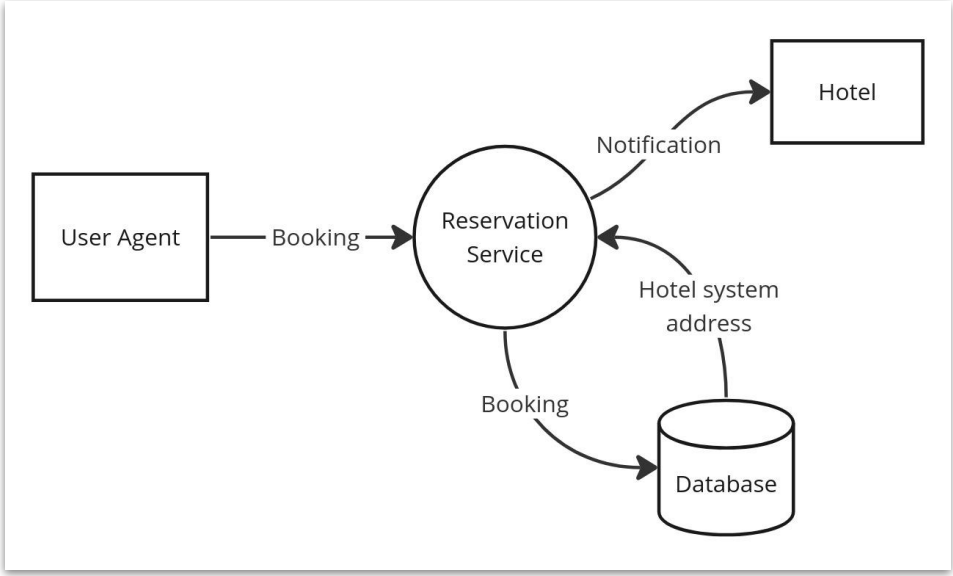
# Threat Modelling

Design Documents

Empowerment via simplicity


Image courtesy of Bruno Rohner

# Threat Modelling




**S**poofing
**T**ampering
**R**epudiation
**I**nformation Disclosure
**D**enial of Service
**E**levation of Privilege

# Secure Tech & Code

Secure Products via...

...secure Languages

...vetted Frameworks

...solid Software Architectures

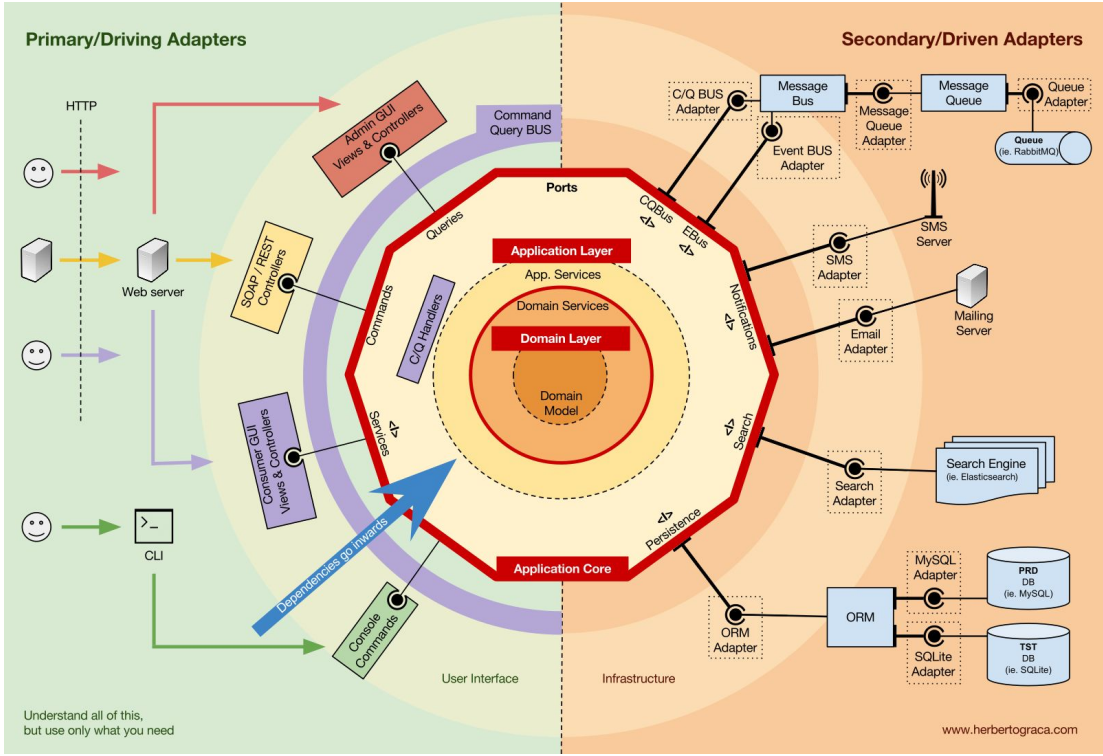
# Secure Tech & Code

Strongly typed language

Up-to-date framework

Hexagonal Architecture

Consistent application of paradigms



# Secrets & Access Management

Least Privilege

Timely Access

Dedicated Credentials

“No password is the best password”

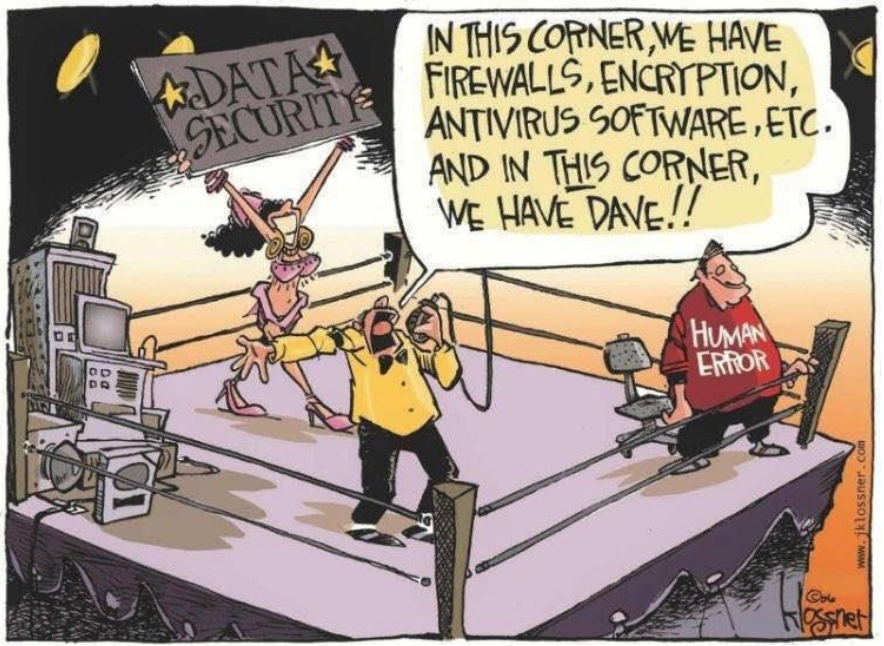
# Secrets & Access Management

Restricted scope only

Temporary users

Single Sign-On

Facilitate Password Rotation



# Security Incident Response

Prepare for the Unforeseeable

Leadership Buy-in

# Security Incident Response

Playbooks

Tabletop exercises

Post-Mortems



# Wrapping up

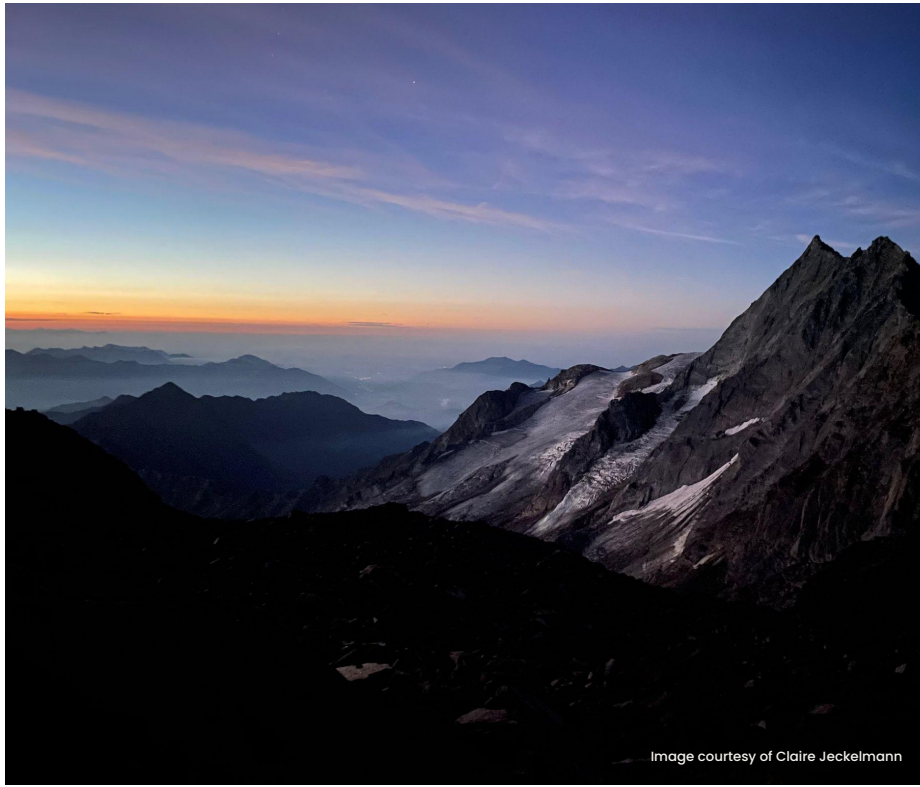
Engineering Culture

Ask “what can go wrong?”

Secure Tech

Credential Management

Prepare for Incident




security@fairtiq.com

# Links

- Hexagonal Architecture: https://herbertograca.com/2017/11/16/explicit-architecture-01-ddd-hexagonal-onion-clean-cqrs-how-i-put-it-all-together/