Cloud Security

from Docker to Kubernetes

Matteo Baiguini

Workshop-Tage 2022

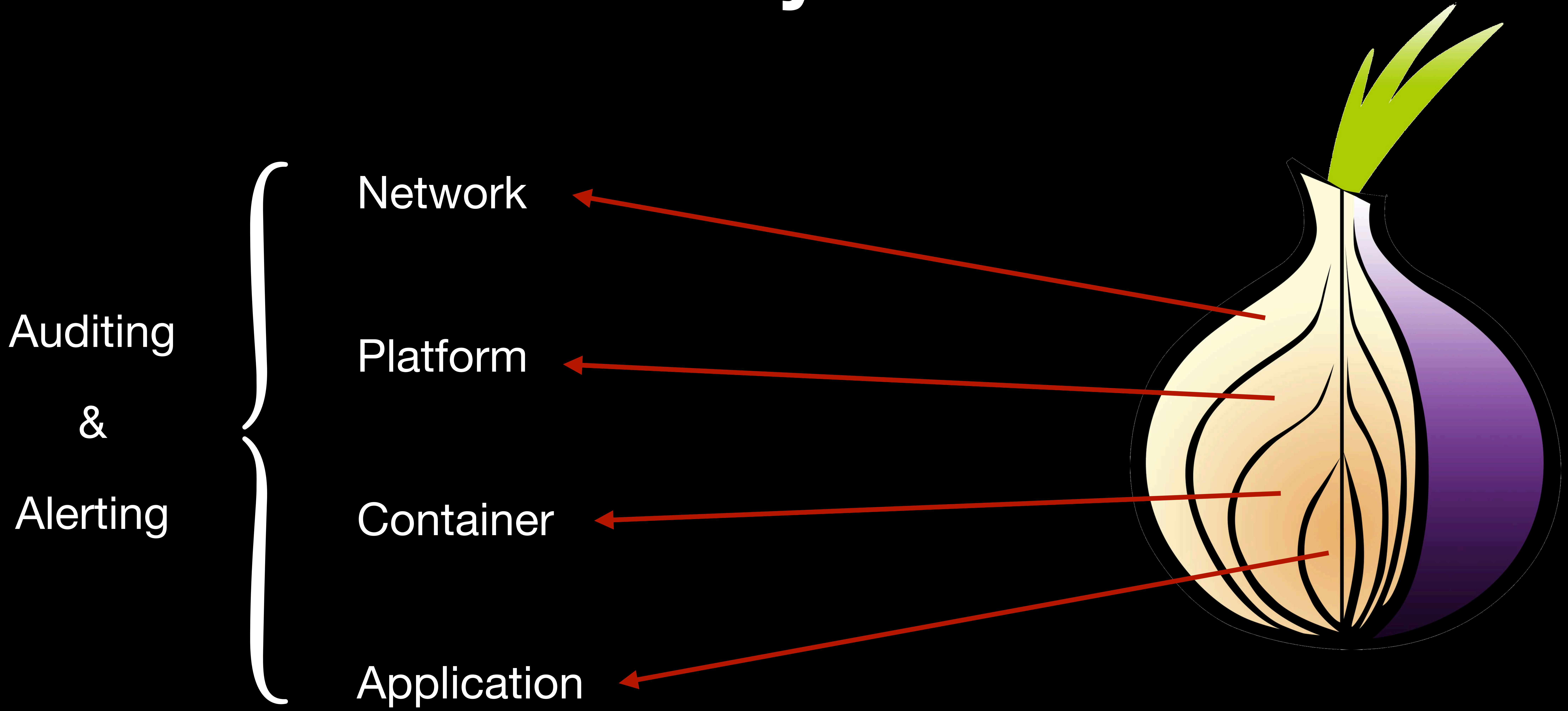
ℹ️

The goal of this workshop is to give
only an overview of Cloud security
and an introduction to some useful tools

whoami

- Computer Sciences Master Degree
- Java developer
- Golang developer
- DevOps, infrastructure and CI/CD expert
- Experience in multiple areas (e.g. eCommerce, telecommunications, trading/exchange)
- DevOps and Cloud advocate
- Observability advocate
- Kubernetes certified
- Freelance experience with various customers in Europe
- Head of DevOps and Security at Swissblock Technologies

Security Onion



Auditing

&

Alerting

Network

Platform

Container

Application

Application

- Enable DB passwords
- Use only verified libraries in codebase
- Scan codebase for vulnerabilities
- Don’t log sensitive information
- Expose metrics
- Expose meaningful logs

Container

- Scan container for vulnerabilities
- Scan base images for vulnerabilities
- Scan container content for misconfigurations
- Scan container content for secrets

Platform

- Enable authentication
- Enable authorisation
- Apply “least privileges” principle
- Collect metrics and logs

Network

- Forbid all incoming connections by default, allowing only required ones
- Forbid all outgoing connections by default, allowing only required ones
- Collect metrics and logs

Auditing & Alerting

- These concepts are pretty underestimated, but it’s a big mistake
- Don’t protect only the perimeter, but look constantly inside for suspicious activities
- Setup proper alerting including all security aspects

The tools

K8s Authentication with Dex

K8s Security Context

K8s Pod Security Standards and Admission

K8s RBAC

K8s Network Policies

RBAC-Manager

RBAC-Looup

Rakkess

Trivy

Polaris

Popeye

Starboard

Falco

The repo

bit.ly/wt22-cloud-security