TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

K8s Security 101

Date of the training: **June 26-27, 2023** in Heidelberg, Germany

Book now using the voucher code: **TR23_HMTRAINING** and save an additional 5% of the current valid rate of any package!

Overview

Container orchestration has been the driver for velocious software development and reliability engineering. But how to ensure the secure operation of your apps in a Kubernetes (K8s) cluster? This workshop gives a crash course about OCI, Docker and K8s basics. Afterwards, we take the perspective of a security auditor and attacker to attack and defend a managed EKS Kubernetes cluster together.

Container, microservices, Kubernetes, GitOps - all those terms dominate the modern software development teams and processes. In the first part of this course, you learn the technological basics behind all those terms. In the second part, you take the perspective of a security auditor and finally of an attacker and learn to attack and defend a managed Kubernetes cluster. Among others, you will gain answers for the following questions:

- How to work with Docker and Kubernetes?
- How to continuously deploy containers with GitOps?
- How to audit the security of a Kubernetes cluster?
- How to compromise a Kubernetes cluster?

All topics are guided by and demonstrated with practical hands-on exercises in a managed Kubernetes cluster (AWS EKS). At the end of this workshop the participants will have gained in-depth knowledge about the hardening and attacking of Kubernetes clusters and the impact of misconfigurations for deployed application architectures and the operation of a modern microservice

infrastructure. The workshop ends with an attack and defense game where the participants attack other participants and defend themselves by applying their knowledge learned along the way.

Who should attend this training?

- Security professionals who want to learn how to audit and pentest a K8s cluster.
- Kubernetes operators who want to learn how to defend a cluster and impact of misconfigurations.

Requirements

The attendees should have:

- Basic knowledge of using the Linux Bash command line.
- Ideally offensive security practice to have fun during the attack & defense.

About the Trainers:

Florian Bausch studied Digital Forensics and wrote his Master thesis about a forensic analysis of Ceph (distributed storage). Since 2019 he has been working as an incident responder and pentester at ERNW Research GmbH.

Sebastian Funke is an IT Security Analyst and Researcher at ERNW Enno Rey Netzwerke GmbH with more than 7 years of experience. In his daily work he performs security assessments and penetration tests in large and complex enterprise environments with focus on classic web app, desktop app and network security, well as container hardening and cloud account configuration reviews.

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR23_HMTRAINING
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German.
+49 6221 480390 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hm-ts.de
+49 6022 5089999 / https://hm-ts.de