

# Training:

## Cloud Security Masterclass: Defender's Guide to Securing Public Cloud Infrastructure

Date of the online training: **October 25-26, 2021**

### Overview

This hands-on CTF-style training focuses on elevating your security knowledge into the cloud. Learn to defend your public cloud infrastructure by building automated detection, alerting and response pipelines for your public cloud workloads by using native cloud services. This training focuses on building security knowledge on the cloud and for the cloud.

This training focuses on elevating your threat detection, investigations, and response knowledge into the cloud. This hands-on training with CTF-style exercises simulates real-life attack scenarios on cloud infrastructure & applications. It then teaches you to build defensive guard rails against such attacks by using cloud native services on AWS. This makes it an ideal class for red & blue teams.

By the end of this training, we will be able to:

- Use cloud technologies to detect IAM attacks.
- Understand and mitigate cloud native pivoting and privilege escalation and defense techniques.
- Use serverless functions to perform on-demand threat scans.
- Containers to deploy threat detection services at scale.
- Build notification services to create alerts.
- Analyze malware-infected virtual machines to perform automated forensic investigations and artifacts collection.
- Use Elasticsearch and Athena for building SIEM and security data-lake for real-time threat intelligence and monitoring.

For more detailed information about the training content please check our website:

<https://troopers.de/troopers21-otm-2/trainings/fmzwen/>

## Who should attend this training and why?

- Red Team members
- Blue team and Purple team members
- Cloud Security Teams
- Incident responders, Analysts
- Malware investigators and Analysts
- Threat intelligence analysts and Responders

This is a unique course which is on the cloud and for the cloud. It not only helps train the individuals on cloud terminologies but also enables them to build scalable defense mechanisms for their services running in the public cloud. The training explicitly focuses on threat detection, Incident response, malware investigations and forensic analysis of cloud infrastructure which is still a very less known domain in the market.

Students will learn:

- Using cloud native technologies to build your own security services for your applications and services running in the cloud.
- Building real-time detection, monitoring and response capabilities for threat tracking and intelligence gathering.
- Building Advanced automated pipelines through Detection-as-code features to defend public cloud infrastructures.

## Prerequisites

- Basic understanding of cloud services
- System administration and Linux cli
- Able to write basic programs in python

## Requirements

- Laptop with internet access
- Free tier account for AWS

Students will be provided with:

- PDF versions of slides that will be used during the training.
- Complete course guide in containing 200+ pages in PDF format. It will contain step-by-step guidelines for all the exercises, labs and detailed explanation of concepts discussed during the training.
- Slack channel to continue the discussion and access even after the training ends.
- Infrastructure-as-code templates to deploy the test environments & simulations for continued practice after the class ends.
- Access to Github account for accessing custom-built source codes and tools.
- Collection of test malware samples, forensic images, detection rules and queries.

## About the Trainers

**Abhinav Singh** is a cybersecurity researcher with close to a decade long experience working for global leaders in security technology, financial institutions and as an independent trainer/consultant. He is the author of Metasploit Penetration Testing Cookbook (first, second & third editions) and Instant Wireshark Starter, by Packt. He is an active contributor to the security community in the form of patents, open-source tools, paper publications, articles, and blogs. His work has been quoted in several security and privacy magazines, and digital portals. He is a frequent speaker at eminent international conferences like Black Hat, RSA & Defcon. His areas of expertise include malware research, reverse engineering, enterprise security, forensics, and cloud security.

## Booking

Recommended online booking of trainings through:

<https://tickets.ernw.de/troopers/tr21training/>

## Contact

**Need assistance?** Don't hesitate to call us. We are fluent in English and German.  
+49 6221 480390 or [info@troopers.de](mailto:info@troopers.de)

**Booking is also possible offline through your trusted partner:**

**HM Training Solutions**, Falkenstrasse 6, 63820 Elsenfeld, Germany

+49 6022 508200 / [info@hmtrainingsolutions.com](mailto:info@hmtrainingsolutions.com)

+49 6022 5089999 / [www.hmtrainingsolutions.com](http://www.hmtrainingsolutions.com)