

Training:

Incident Analysis

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

This training is a practical Incident Analysis workshop, focusing on Windows systems and a bit traffic analysis with lots of hands-on exercises. It is designed for anybody with IT background, willing to learn some of the essential steps during an incident analysis. This is not an advanced class, but more of an incident analysis 101 with a steep learning curve. Topics such as incident handling and incident response will not be part of this course.

During this course you will (hopefully 😊) learn a lot about windows/malware internals, and how to:

- Identify Indicators of Compromise
- Analyze network traffic for suspicious behavior
- Investigate disk images
- Analyze memory dumps with volatility
- Differentiate malware from harmless software
- Analyze malware (behavior)
- Correlate gathered logfiles to a specific incident

The language of this course depends on the attendees: if only Germans attend the training, it will be done in Deutsch, otherwise the training will be done in English.

Who should attend this training?

- Persons who are interested in incident analysis but do not have deep knowledge yet.
- Persons with a job that touches incident analysis, and they want to improve results.
- Persons who manage teams that do incident analysis, and they want to understand their team's work better.
- (IT) Students who consider CSIRT/CERT/SOC/... as a future working place.

Requirements

The attendees should have:

- A laptop with administrative privileges and pre-installed VirtualBox
- TCP/IP Knowledge
- Be familiar with a shell

Good to have, but not necessary:

- Experience with at least one programming language
- Basic knowledge about hacking techniques

About the Trainers:

Frank Block is a security researcher working for ERNW Research GmbH with more than 13 years of experience, and an external PhD student at the University of Erlangen-Nuremberg (Department Informatik) with a focus on memory forensics. His main fields of interest are incident analysis and penetration testing. When not involved in customer projects, he enjoys doing research in all kinds of areas and usually presents the results at conferences such as DFRWS USA, Black Hat USA/EU and Troopers.

Justus Hoffmann is a Incident Analyst and Pentester at ERNW Research.

Dr. Matthias Hamann studied computer science with a focus on IT security at the University of Mannheim and subsequently wrote his PhD thesis about lightweight cryptography on ultra-constrained RFID devices. Following this, he gave lectures such as IT Security, Internet-of-Things (IoT) Security, and Cryptography at the university for several years. Since 2021, he has been working as a security analyst and incident responder at ERNW Research GmbH.

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>