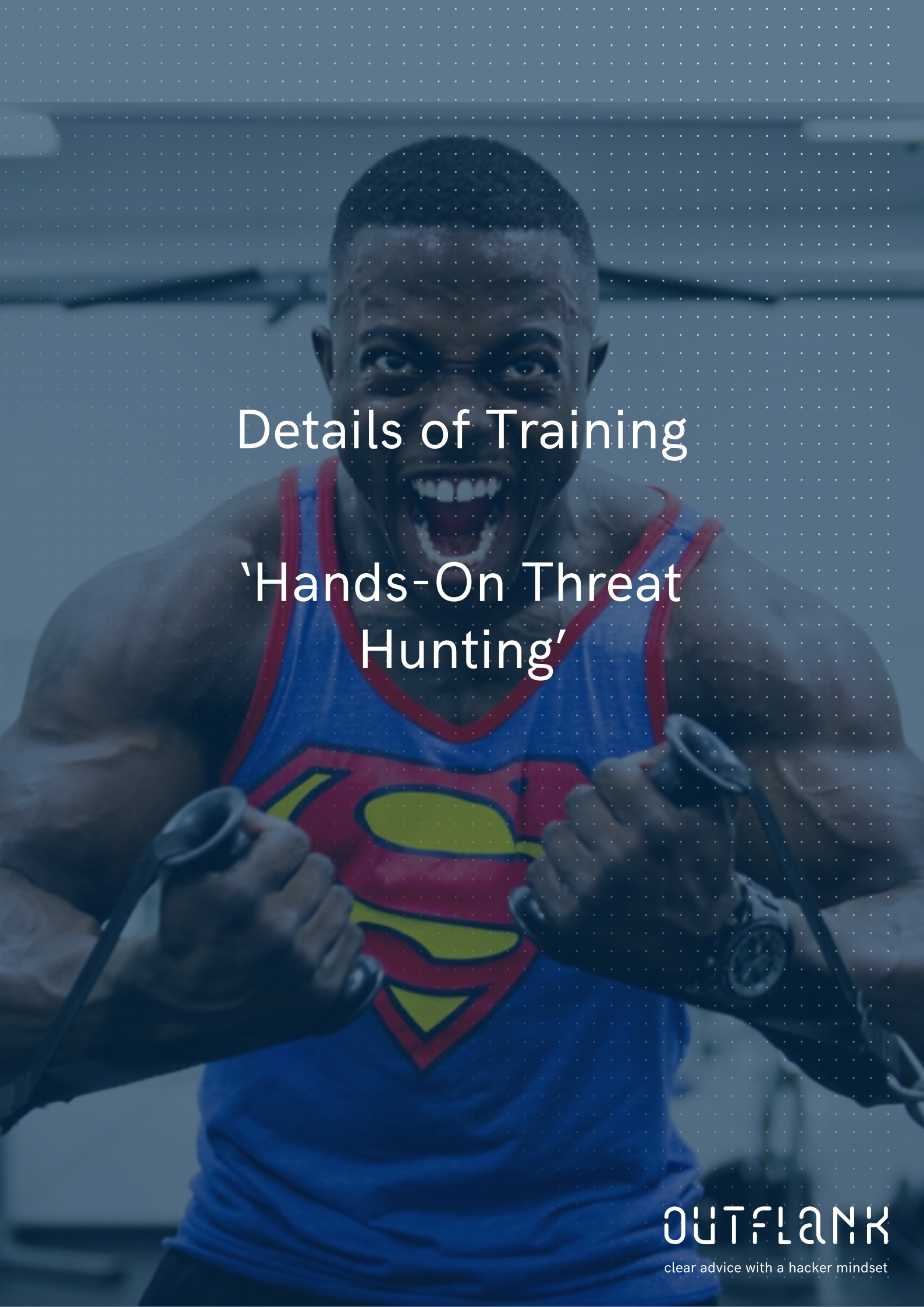

Details of Training

‘Hands-On Threat Hunting’

OUTFLANK

clear advice with a hacker mindset

Overview

Threat Hunting is all the new buzz nowadays. But what defines Threat Hunting, and what not?

This 2-day technical training is the right choice for everybody interested in getting beyond the buzzwords. Combining a large and private hands-on lab and having instructors experienced in both offensive and defensive security, you will leave this training excited and prepared for Threat Hunting.

Key learning objectives

During this training you will:

- Better understand what Threat Hunting is, and what it is not.
- Learn the different steps in the process of Threat Hunting, and the outcome of each step.
- Understand how to get started with Threat Hunting, and how to gradually increase and improve.
- Measure Data Quality and know how to improve the quality of your organisation's data used for security monitoring and threat hunting.
- Get a better understanding of key offensive actions used by real threat actors, and how to detect these actions.
- Dive into several key security concepts in Windows and Active Directory, as well as how real threat actors abuse insecurities.
- Learn the theory, as well as getting hands-on practical experience in a realistic lab environment.

Approach

This training uses the same approach as other trainings by Outflank. This means:

- Interactive setting with multiple trainers, each brining their dedicated area of expertise.
- A combination of theory and learning by doing.
- Large lab environments per student that represent real office networks.
- Students will learn about and perform both offensive and defensive steps in the lab; working with Cobalt Strike and with modern security monitoring tools like Splunk, ELK and Sentinel.
- Detailed labmanual that guides the students through each lab assignment, including extra assignments for more experienced students.
- Full set of training material to take home and restudy at a later moment.

Content and topics

The following topics are covered during the training:

- Introduction to Threat hunting, and its key differences when comparing to security monitoring and other SOC related roles
- Understanding key theoretical concepts like Kill Chain, Attacker's/Intruder's Dilemma, MITRE ATT&CK, and the relation to Threat Hunting for each of these
- Theory of Threat Hunting, including getting experience with creating and following hunting hypotheses.
- Measuring and improving Data Quality.

- An introduction to data science.
- Key items of Windows endpoint and Active Directory security that modern attackers abuse and every security specialist should know about.
- Deep dive into logging and monitoring in Windows.
- Key important tools in the Threat Hunter's tool bag: Splunk, Azure Sentinel and Jupyter Notebooks.

Who should attend?

This training is suited for everybody who is interested in the topics of Threat Hunting and security monitoring. Specifically, this training is suited for:

- People currently in a Threat Hunters position, both novice as well as experienced
- Members of CERTs, SOCs and CDCs in any role
- Red teamers and pentesters interested in getting a better idea of how blue teams perform detections and hunts
- People generally occupied with technical aspects of IT security
- People who previously have done the Outflank DAMTA training and looking for a deeper dive into advanced detection capabilities

Note 1: Windows and Active Directory are key aspects of this training as these technologies are prominently existing in modern office environments. Although some experience is helpful, it is not expected that students are experts in Windows security.

Note 2: For students familiar with other Outflank trainings, i.e. 'Defend Against Modern Targeted Attacks' or 'Windows and Active Directory Security'; this is a different training that perfectly fits alongside these other trainings. At the same time, it is not required to have done these other trainings.

About the trainers

Your trainers are Mark Bergman, Pieter Ceelen and Marc Smeets. They work as specialists at the IT security company Outflank, which they also co-founded. They have tuned their many years of experienced in both offensive security (red teaming and adversary simulations) as well as defensive security (SOC-analysts and Threat Hunter) into this training, combining the best from both worlds.

Mark Bergman

Pieter Ceelen

Marc Smeets

Hardware requirements for attendees

A laptop that has the ability to run a Remote Desktop Connection.

Testimonials from past students

Below you can find a selection of quotes from previous attendees.

"Great training, really helps you on the way to Threat Hunting. Happy hunting"
Roel van Dartel - Network Engineer at Fontys Hogescholen

"Hunting is a fun and energising endeavour and so is this training. The combination of theory and practical workshops, that build on existing operational CERT or SOC experience, leave the student with a good sense on how to bring their team to the next maturity level."
Remon Klein Tank, ISO WUR/SURFcert

"Awesome training that fits perfectly with the day-to-day reality"
Folkert Jonker, System Engineer, Amsterdam UMC.