TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

ATT&CK based hunt engineering on Windows

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

Threat hunting is a hot topic at the moment; however, this entails a lot more than some random digging through data or copy pasting queries you've found on the internet. The pre-hunt process is a crucial factor in the whole chain to be truly effective in being able to catch any attacker in your network.

Understanding the techniques or tooling an attacker could utilize, the various options they can use and what kind of indicators can be extracted from them will help you build proper hunts, which ideally also lead to automated detection capabilities.

Log data obviously is a very important factor here, after executing various variants of an attack we examine all available data to see what kind of indicators were generated and which ones are of use with an acceptable false possible rate.

This training focusses on the whole cycle, from defining a hunt to researching the relevant techniques to building the hunting logic and executing it on a large dataset.

ERNW Insight GmbH
Carl-Bosch-Str. 4
69115 Heidelberg
BIC: GENODE61HD3

Tel. +49 – 6221 – 48 03 90
Fax +49 – 6221 – 41 90 08
Ust-ID DE 304 445 827
IBAN: DE84 6729 0100 0067 1236 03

Managing Director:
Kerstin Schröter

Who should attend this training?

The training is open to all audiences, junior to more experienced threat hunters. The content should be able to inspire and challenge all levels.

Requirements

- Laptop with a modern browser;
- VMWare, VirtualBox or Parallels installed.

Agenda

Day 1 - Pre-Hunt activities

- Introduction
- Hunting principles
- Different ways of hunting
- Using and understanding MITRE ATT&CK
- Understanding your adversaries and their techniques
- Understanding and assessing (your) data
- Information resources
- Using threat information
- Exercise: Research a technique and assess your visibility
- Data sources and hunt tooling
- Exercise: Defining a hunt from threat information
- Define the analytics for your hunt
- Exercise: Executing your hunt
- Reporting your findings

Day 2 - Hunting activities

- Filtering the noise
- Validation of your results
- Improving a hunt
- Threat briefing
- Threat Hunting application introduction
- Briefing Hunting Lab
- CTF Style lab

About the Trainers

Eduardo Gerosa works for Deloitte AG's Cyber Risk Services, where he leads a team specialized in providing technical consultancy services to client SOC's across Switzerland. Previously he led Deloitte UK's Cyber Engineering DevOps team, where he oversaw the development of automated reconnaissance tools to support red teaming and cyber threat intelligence engagements. He maintains a number of open source tools in the area of OSINT and DFIR and enjoys sharing his knowledge in this space at conference talks or trainings.

Olaf Hartong is a co-founder of FalconForce and a security researcher who specializes in understanding the attacker tradecraft and thereby improving detection. As a former Big4 employee he has a varied background in blue and purple team operations, network engineering, and security transformation projects. He has over 13 years of experience in security, he specializes in building and operationalizing SOC teams through the use of SIEM systems or log management systems such as Splunk. Olaf led the Blue team of a big4 and worked as a Security Officer for a large managed hosting provider serving Governmental and Commercial service clients. Olaf has spoken at MITRE ATT&CKcon, DerbyCon, Splunk .Conf, BlackHat, FIRST, Def Con.

TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Booking

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

Voucher code: TR20_HMTS
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. +49 151 16228365 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@hmtrainingsolutions.com
+49 6022 5089999 / www.hmtrainingsolutions.com