TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Defending Enterprises

Date of the online training: **October 21-22, 2021**

Overview

New for 2021, our immersive 2-day Defending Enterprises training is the natural counterpart to our popular Hacking Enterprises course.

From SIEM configuration to monitoring, alerting and threat hunting, you'll play a SOC analyst in our cloud-based lab and try to rapidly locate IOA's and IOC's from a enterprise breach.

You'll use a combination of Microsoft Azure Sentinel and Elastic platforms to perform practical exercises. In each instance, filters and/or expressions will be supplied for both platforms (where applicable).

Highlights of some of the key areas covered are…

- Detecting phishing attacks
- Detecting credential exploitation
- Detecting lateral movement
- Detecting data exfiltration
- Detecting persistence activities
- much more!

We know 2 days isn't a lot of time, so you'll also get 14-days FREE lab time after class and Discord access for support.

Agenda

Day 1

- MITRE ATT&CK framework
- Defensive OSINT
- Linux auditing and logging

- Windows auditing, events, logging and Sysmon
- Using Logstash as a data forwarder
- Overview of fields, filters and queries in ELK and Azure Sentinel

Attacks and host compromises will be actioned by the trainers and delegates will be asked to configure real-time alerting and monitoring using the provided lab infrastructure, in order to identify these events.

- Identifying Indicators of Attack (IOA) and Indicators of Compromise (IOC)
- Detecting phishing attacks (Office macros, HTA's and suspicious links)
- Creating alerts and analytical rules
- Detecting credential exploitation (Kerberoasting, PtH, PtT, DCSync)

Day 2

- Detecting lateral movement within a network (WinRM, WMI, SMB, DCOM, MSSQL)
- Detecting data exfiltration (HTTP/S, DNS, ICMP)
- Detecting persistence activities (userland methods, WMI Event Subscriptions)
- C2 Communications

Who should attend this training?

This training is suited to a variety of students, including:

- Penetration testers
- SOC analysts
- Security professionals
- IT Support, administrative and network personnel

Prerequisites

Detection methods will be taught during training, however an understanding of networking concepts would be beneficial, and previous SOC experience and/or pentesting is advantageous but not required.

About the Trainers

Will Hunt co-founded In.security in 2018. Will's been in infosec for over a decade and has helped secure many organisations through technical security services and training. Will's delivered hacking courses globally at several conferences including Black Hat and has spoken at various conferences and events. Will also assists the UK government in various technical, educational and advisory capacities. Before Will was a security consultant he was an experienced digital forensics consultant and trainer.

Owen Shearing (@rebootuser) is a co-founder of In.security, a specialist cyber security consultancy offering technical and training services based in the UK. He has a strong background in networking and IT infrastructure, with well over a decade of experience in technical security roles. Owen has provided technical training to a variety of audiences at bespoke events as well as Black Hat, Wild West Hackin' Fest, NolaCon, 44CON and BruCON. He keeps projects at https://github.com/rebootuser.

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

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://www.hm-ts.de