TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Intrusion Analysis and Threat Hunting with Open Source Tools

Date of the online training: **November 03-04, 2021**

Overview

In today's threat landscape, sophisticated adversaries have routinely demonstrated the ability to compromise enterprise networks and remain hidden for extended periods of time. In Intrusion Analysis and Threat Hunting with Open Source Tools, you will learn how to dig deep into network traffic to identify key evidence that a compromise has occurred, learn how to deal with new forms of attack, and develop the skills necessary to proactively search for evidence of new breaches. We will explore all phases of adversary tactics and techniques - from delivery mechanisms to post-infection traffic and data exfiltration to get hands-on analysis experience. Open-source tools such as Suricata, Moloch and Kibana will be utilized to generate data, perform exhaustive traffic analysis, and develop comprehensive threat hunting strategies. By the end of this course, you will have the knowledge and skills necessary to discover new threats in your network and build an effective threat hunting program.

Closing the gap between when an infection occurs and when it is detected is a key goal of an effective threat hunting program. While many security solutions focus on detecting adversarial activity in real time, skilled threat actors have demonstrated the ability to bypass these security tools. This can leave an organization vulnerable to further compromise and data breaches. Having the right data available during an incident or when performing proactive threat hunting activities is crucial for success. More than just an IDS/IPS, Suricata can provide the visibility to solve incidents quickly and more accurately by enabling context before, during, and after an alert. In this course, attendees will learn the skills required to identify, respond and protect against threats in their network day to day as well as identify new threats through structured data aggregation and analysis. Adversary tactics and techniques from delivery mechanisms to post-infection traffic and data exfiltration will be explored in-depth to gain

comprehensive analysis experience. Hands-on labs consisting of real-world malware and network traffic will reinforce course concepts while utilizing the latest Suricata features. By the end of this course, you will have the knowledge and skills to seek out indicators of anomalous or malicious activity in your network traffic and discover threats you have been missing!

This course will cover the fundamental aspects of Suricata such as rule comprehension, managing rule sets, validating alerts, working through false positive/negatives and customizing rules to provide more visibility into your traffic. In-depth analysis of network traffic and the development of threat hunting strategies to detect anomalous or malicious activity will be accomplished with tools such as Arkime, Kibana and CyberChef. Hands-on real-world exercises will be used to reinforce the detection techniques and tactics explained throughout the course. Threat intelligence feeds and other online resources will also be explored to learn how to pivot between data sources while performing proactive threat hunting activities. This is an ideal course for security analysts, blue teams and malware researchers to get hands-on diving deep into malicious traffic.

Who should attend this training?

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

- Security Administrators
- Enterprise Defenders
- Incident Responders
- Security Operations Specialists
- Security Analysts
- Malware Analysts
- Network Engineers

Prerequisites

This course is accessible to many who work or have an interest in network-based security. However, it is not recommended for anyone without fundamental computer

knowledge such as Linux operating systems, working with a terminal, understanding network traffic, or a basic understanding of malware operations.

About the Trainers

Josh Stroschein is an experienced malware analyst and reverse engineer and has a passion for sharing his knowledge with others. He is the Director of Training for OISF, where he leads all training activity for the foundation and is also responsible for academic outreach and developing research initiatives. Josh is an accomplished trainer, providing training in the aforementioned subject areas at BlackHat, DerbyCon, Toorcon, Hack-In-The-Box, Suricon, and other public and private venues. Josh is an Associate Professor of Cyber Security at Dakota State University where he teaches malware analysis and reverse engineering, an author on Pluralsight, and a threat researcher for HP.

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