TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Advanced Deployment and Architecture for Network Traffic Analysis

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

Network-based threat detection is crucial for developing a comprehensive security strategy, whether it is on-premise or in the cloud. In Suricata Advanced Deployment and Architecture, you will learn how to maximize the visibility that Suricata can provide into your network. You will gain deep technical understanding and hands on experience with Suricata's versatile arsenal of features and capabilities for a variety of deployment, usage, and integration scenarios. Tuning and optimizing Suricata for threat/anomaly detection, file extraction, and/or protocol detection are critical for a successful deployment.

You will also learn traditional and non-traditional tips, tricks, and techniques to implement Suricata and its newest features based on real-world deployment experiences, to include cloud-based deployments. This class also offers a unique opportunity to bring in-depth use cases, questions, and challenges directly to the Suricata team. By the end of this course, you will be able to successfully design, deploy, implement, optimize and hunt with your high-performance Suricata deployment.

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

The foundation for effective intrusion detection and response is based on proper sensor placement and configuration. Sensor placement is crucial for developing a comprehensive network security and monitoring solution. Misconfigurations and improper placement can lead to gaps in network visibility, which can allow attackers to go undetected for prolonged periods of time and to penetrate deeper into your network.

In Suricata Advanced Deployment and Architecture, you will learn the skills necessary to successfully design, deploy and optimize a high-performance network monitoring and security solution. Filled with hands-on exercises and comprehensive demonstrations, this class will elevate your skills to maximize your network visibility and data management with Suricata. By the end of this course you will deep technical understanding and hands on experience with Suricata's versatile arsenal of features and capabilities for a variety of deployment, usage, and integration scenarios.

This course will go in-depth in Suricata configuration and deployment considerations. You will learn which capture method is best for traffic acquisition, maximizing performance with run modes and dive deep into Suricata's detection engine and multi-pattern matchers. Discover how to expand Suricata's detection and output capabilities with Lua scripting as well as anomaly detection and file extraction capabilities. Gain a deeper understanding of performance and tuning considerations through CPU affinity, Numa, threading and NIC RSS hashing.

Alongside that understand specifics about deployments the cloud and the pros and cons of those. Details of what and how needs to be in place for the cloud security monitoring. Learn how to perform effective and exhaustive troubleshooting when situations like packet loss and system overloading occur. Finally, learn how to handle elephant flows, work with eXpress Data Path, how output generation affects your deployment and how to integrate Suricata with other tools such as an ELK stack, Splunk and other Linux-based distributions such as SELKS. This class also offers a unique opportunity to bring in-depth use cases, questions, challenges, and new ideas directly to the Suricata team. Take your deployment and configuration skills to an expert level with Suricata Advanced Deployment and Architecture!

Prerequisites

- Basic experience with installing, compiling, configuring and running Suricata is a must;
- Hands on Linux command line;
- TCP/IP networking.

Requirements

A laptop that has the following available:

- Be able to run a VM with at least 2 vCPUs and 6+ GB RAM;
- VMware Player or Latest VirtualBox, VMware Workstation/Fusion;
- Administrative rights;
- No AV / Ability to temporarily disable;
- Please do not bring a company laptop containing sensitive materials or that you cannot modify!

About the Trainers

Peter Manev has been involved with Suricata IDS/IPS/NSM from its very early days in 2009 as QA lead, currently a Suricata executive council member. Peter has 15 years' experience in the IT industry, including enterprise and government level IT security practice. As an adamant admirer and explorer of innovative open source security software he is also one of the creators of SELKS - an open source threat detection security distro. He is also one of the founders of Stamus Networks, a company providing security solutions based on Suricata.

Eric Leblond is an active member of the security and open source communities. He is a Netfilter Core Team member working mainly on communications between kernel and userland. He works on the development of Suricata, the open source IDS/IPS since 2009 and he is currently one of the Suricata core developers. He is also one of the founders of Stamus Networks, a company providing security solutions based on Suricata.

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