Masterclass: Advanced Malware Hunting

Varighed: 5 Days Kursus Kode: AMH Leveringsmetode: Virtuel deltagelse

Beskrivelse:

This course teaches the ways of identifying how malware looks like, what malicious activities you should look out for and the ways of removing it. You will also learn how to implement and manage preventive solutions both for small and medium sized for enterprises and organizations. During this course you learn what makes piece of code malicious, go through historic examples and get familiar with different kinds of malware and how to identify various cases. Once we have sufficient understanding of techniques and capabilities of malware, we will start system and network hardening – you will implement security in depth solutions, such as whitelisting or virtualization, in order to protect assets.

Målgruppe:

Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.
To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5-8 years in the field is recommended.

Forudsætninger:

- To attend this training, you should have a good hands-on experience in administering Windows infrastructure. At least 5-8 years in the field is recommended.

Test og certificering

- After finishing the course, you will be granted a CQURE **Certificate of Completion**. Please note that after completing the course you will also be eligible to claim **CPE points!**

Indhold:

Module 1: What is malware

a) Malware History

b) Malware Goals

c) Types of Malware

d) Advanced Persistent Threats

e) Indicators of Compromise

Module 2: Introduction to Malware Analysis

a) Types of malware analysis

b) Goals of malware analysis

c) Impact analysis

d) Containment and mitigation

e) Incident prevention and response playbooks

f) Setting up sandbox environment

g) Cloud-based malware analysis

Module 3: Static malware analysis

a) Executable analysis

b) Extracting secrets

c) Determining if file is packed or obfuscated

d) Fingerprinting the malware

e) Pattern matching using YARA

Module 4: Behavioral malware analysis

a) Malware detonation

b) Sysinternals suite

c) Network communication analysis

d) Monitoring system events

e) Memory dump analysis

f) Simulating real environment

Module 5: Malicious non-exe files

a) Alternative binaries

b) PowerShell scripts

c) Office documents

d) JScript

e) HTML documents

f) Living off the land binaries

Module 6: Advanced techniques used by malware

a) Malware persistence methods

b) Malware stealth techniques

c) Covert channel communication

d) Domain Generator Algorithms

e) Anti-VM and Anti-debugging tricks

Module 7: Defending against malware

a) Windows security solutions

b) Anti-Virus software

c) EDR software

d) Principle of least privilege

e) Application Whitelisting

f) Virtualization

g) Network and domain segmentation

Additional Information:

Intense exercises:
This course is packed with unique labs exercises! To get more practice we offer three extra weeks of labs online!After the training concludes, you may practice even more and repeat to consolidate newly gained skills and knowledge.
Platform and Technical Requirements:
To participate in the course you need a Stable internet connection. For the best learning experience we also need you to have a webcam, headphones and a microphone. Open RDP port 3391 for the connection to the Lab environment is needed as well. We will setup a secure Zoom classroom for every day of the course – we will send you a safe link to join the conference by e-mail.

Flere Informationer:

For yderligere informationer eller booking af kursus, kontakt os på tlf.nr.: 44 88 18 00

training@globalknowledge.dk

www.globalknowledge.com/da-dk/

Global Knowledge, Stamholmen 110, 2650 Hvidovre