Virtuelt kursus
5 dage **DKK 24.999**
Nr. 91035 A ekskl. moms

Dato **Sted**

Masterclass: Advanced Malware Hunting [AMH]

Lær at identificere hvordan malware ser ud, hvilke ondsindede aktiviteter du skal passe på, og hvordan du fjerner den. Du vil bl.a. lære at implementere og håndtere forebyggende løsninger både for små og mellemstore virksomheder og organisationer. Kurset foregår på engelsk med live underviser.

Beskyt din virksomhed mod malware

I løbet af kurset lærer du, hvad der gør kodestykket ondsindet, vi gennemgår historiske eksempler og du bliver fortrolig med forskellige former for malware og lærer, hvordan man identificerer forskellige tilfælde. Når vi har tilstrækkelig forståelse for teknikker og kapaciteter til malware, starter vi system- og netværkshærdning – hvor du implementerer sikkerhedsdybdegående løsninger, såsom hvidliste eller virtualisering, for at beskytte aktiver.

Deltagerprofil

Kurset er for dig der fx er: Enterprise-administrator, infrastrukturarkitekt, sikkerhedsmedarbejder, systemtekniker, netværksadministrator, IT-fagperson, sikkerhedskonsulent, eller dig der har ansvar for at implementere netværks- og perimetersikkerhed i din organisation.

Forudsætninger

Du skal have god praktisk erfaring med administration af Windows-infrastruktur for at deltage på kurset. Vi anbefaler, at

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

du har mindst 8 års praktisk erfaring.

Udbytte

- Lær at identificere malware
- Bliv trænet i at opdage og stoppe ondsindede aktiviteter
- Lær at implementere forebyggende tiltag i din organisation
- Lær at implementere dybdegående sikkerhedsløsninger
- Bliv fortrolig med forskellige former for malware

Det får du på arrangementet

- Øvelser og inddragelse
- Kursusbevis
- Erfaren underviser
- Maks. 12 deltagere
- Casearbejde
- Materiale på engelsk
- Undervisning på engelsk

Indhold

Module 1: What is malware?

- Malware History
- Malware Goals
- Types of Malware
- Advanced Persistent Threats
- Indicators of Compromise

Module 2: Introduction to Malware Analysis

- Types of malware analysis
- Goals of malware analysis
- Impact analysis
- Containment and mitigation
- Incident prevention and response playbooks
- Setting up sandbox environment
- Cloud-based malware analysis

Module 3: Static malware analysis

- Executable analysis
- Extracting secrets
- Determining if file is packed or obfuscated
- Fingerprinting the malware
- Pattern matching using YARA

Module 4: Behavioral malware analysis

- Malware detonation
- Sysinternals suite
- Network communication

Module 5: Malicious non-exe files

- Alternative binaries
- PowerShell scripts

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

- Office documents
- JScript
- HTML documents
- Living off the land binaries

Module 6: Advanced techniques used by malware

- Malware persistence methods
- Malware stealth techniques
- Covert channel communication
- Domain Generator Algorithms
- Anti-VM and Anti-debugging tricks

Module 7: Defending against malware

- Windows security solutions
- Anti-Virus software
- EDR software
- Principle of least privilege
- Application Whitelisting
- Virtualization
- Network and domain segmentation

Form

Kurset er virtuelt med live underviser.

Før du deltager i det virtuelle kursus, vil vi altid forsøge at arrangere en testsession på 15 - 20 minutter en uges tid før, for at sikre, at du er i stand til at deltage i masterclassen. Herunder finder du kravene til at oprette forbindelse til det virtuelle kursus:

- En computer med en stabil internetforbindelse (skal helst køre Windows eller Mac OS).
- Tilladelser til udgående RDP-forbindelser til eksterne servere (til vores laboratoriemiljø) – port 3389
- Et headset (hovedtelefoner og mikrofon)
- Webcam (indbygget eller tilsluttet)
- En ekstra skærm er nyttig, men ikke påkrævet

Materiale

Du får adgang til unikke værktøjer, over 150 sider med øvelser og præsentationsslides med noter i løbet af kurset. Alle labs forbliver online i yderligere 3 uger, så du kan øve endnu mere, efter kurset er afsluttet. Alle øvelser er baseret på Windows Server 2016 og 2019, Windows 10 og Kali Linux.

UNDERVISER

Paula Januszkiewicz

Paula er verdenskendt som sikkerhedsekspert. Paula elsker at lave penetrationstests, IT-sikkerhedsevalueringer, og hendes motto er: "harden em all!". Hun er Enterprise Security MVP og -underviser (MCT), og så er hun Microsoft Security Trusted Advisor.

Har du faglige spørgsmål så kontakt

Malene Kjærsgaard

Teknologisk Institut
kurser@teknologisk.dk
+45 72 20 30 00

+45 72202523
mch@teknologisk.dk