THREAT HUNTING ACADEMY

Hands-on Technical Online Training

DESCRIPTION

Enterprises are facing more and more breaches and it's clear that a pure prevention based approach is simply not enough. In this two day training we will teach students how to add early detection and response capabilities to their current defense-in-depth security infrastructure. Not only will students learn what to look for in their environment, but we will also go in depth into TTP's (Mitre) and do a deep dive into how these common attack techniques work, to build accurate detections.

DETAILED COURSE DESCRIPTION

DAY ONE of this vendor agnostic training will cover how to build your own Threat Hunting Environment. The hunting platform, running on an Azure deployed lab environment, will teach students how to collect endpoint telemetry using windows event logs and sysmon (EDR). We will provide light introductions into using Git, Docker, Elasticsearch, Logstash and Kibana. We will have a look at Microsoft group policies (GPO's), Windows Eventlog Collection, forwarding and Winlogbeat configuration. Students will get to build their own data lake, log collection and alerting system.

On DAY TWO students will get their own Kali Linux and Windows 10 client, perform Red Team exercises within their environment, and then learn how these common TTP's (attack techniques - MITRE ATT&CK) work and the underlying methodology to detect them, as performed by a Blue Team:

- Recon
- Persistence
- Privilege Escalation
- Kerberoasting
- Code execution and payload delivery
- Process spawning and Macro weaponization
- Lateral Movement (Pass the hash)

- Duration: 2 days
- Format: Instructor Led (online) technical training
- Language: English
- Private Courses available
- Contact our sales department for partner price or other requests
- Schedule: **https://www.exclusive-networks.com/nl/events/categorie/training/threat-hunting-academy/lijst/**

TARGET AUDIENCE

The course is aimed at individuals that want to gain a better understanding in how to design, build, and operate their hunting platform to quickly identify threats.

The course is accessible to persons that are part of a SOC, Incident Response or Threat Hunting team, but also to General security practitioners, system administrators and security architects.

Companies looking to build their own SOC, or that are looking to make vendor choices for SIEM/EDR solutions will get a clear understanding of how these technologies work, what they can and cannot do, and how they work together.

WHAT YOU WILL LEARN

- After following this training, students will
- Know which logs to collect and how to ship them centrally
- Build advanced detections to catch adversary TTP's
- have a full understanding of building a complete Threat Hunting pipeline (BLUE TEAM)
- work with Docker – optimizing the deployment of your hunting platform
- Use Git , and have access to all the code to build your personal lab (for after the training)
- Perform RED TEAM exercises with the Metasploit Framework
- Understand Windows GPO's
- End point log telemetry (EDR)
- Have a full ELK (Elastic, Logstash and Kibana) deployment completely docker based

PRE-REQUISITES

Familiarity with Linux and Windows is mandatory.

BASE HARDWARE REQUIREMENTS

Students need to bring their own laptops with the following minimum system requirements

- Windows 10 Pro or recent macOS
- A recent web-browser (Chrome would be preferred)
- As we are running everything in the cloud, nothing needs to be installed on the student machines
- A broadband internet connection

EXCLUSIVE NETWORKS

Meer informatie over de Threat Hunting Academy
kunt u contact opnemen ons.

Exclusive Networks NL
Ekkersrijt 4601,5692 DR SON
Tel: +31 (0)499 462121
Email: services@exclusive-networks.nl