clarified security
we break security to bring clarity

Hunt The Hacker

A practical training that teaches attendees how to discover hackers that have bypassed existing security mechanisms, and are now operating invisibly within the internal network. This course is Windows domain centric.

Brought to you by professional hackers!

Training duration: 2 days of instruction, predominantly in the form of hands-on hunting labs.

Group size: ***10 participants*** maximum

Target audience: Everybody who needs to know more about what threat hunting is, why it is necessary, what is required to start doing it, and how it should be done. Appropriate roles include: CISOs, Security Managers, SOC staffers, Incident Responders, Forensic Analysts and System Administrators.

Pre-requisites: To maximize value to the attendee, prior HOHE participation is highly recommended, but not mandatory.

Trainer: (in English or Estonian upon demand)

- **James Dodd**
- **Taavi Sonets**

Training methods: The trainers engage participants with lectures, live demonstrations and Q&A sessions. Each participant spends the majority of their time performing a wide variety of hands-on hunts within our fully-patched (yet thoroughly hacked) Windows 10 lab network, using a range of highly effective threat hunting technologies and techniques. Technologies used: Sysmon, the Elastic stack (formerly "ELK"), WinRM, PowerShell, YARA.

Intended outcome: Participants will understand what threat hunting is, be utterly convinced of the need for it, know what infrastructure is required to facilitate it, and be able to start doing it with confidence within their own organizations.

Delivery: We can deliver on-site at group pricing anywhere in the world where good broadband connection is available. Ask us for the group pricing or for times and locations of our public courses. Public groups are currently available directly or via partners in: ***Estonia, Finland, Sweden***.

More info from our website: https://clarifiedsecurity.com/hunt-the-hacker-course/