



Applied Threat Intelligence

Abstract

Join some of the industry's elite for this two-day course and learn the secrets to getting the most from threat intelligence.

Rooted in traditional intelligence analysis techniques, threat intelligence is one of the best tools today for understanding and dealing with the ever-growing complexity of the threat landscape. However, it's generally poorly applied and understood.

Learn how to collect, analyze and use threat intelligence data, tools and frameworks with the support of experts, and immerse yourself in hands-on, real-life threat hunting and incident response scenarios plus how to apply findings in order to protect a particular network.

This course is offered in two formats: Hunting and Defending. Choose either or both to benefit from the most relevant best practice, expert insights, plus practical tools and frameworks.

Learning Objectives

Students will understand:

- Understand how to distill a huge volume of data and transform it into intelligence
- Get to grips with threat hunting fundamentals and adversary profiling
- Gain practical skills for applying threat intelligence data in various scenarios including defending, incident response and forensic analysis

Target Audience

- Operations Center (SOC) Analysts
- Threat Intelligence Analysts
- SIEM Analysts
- CERT Managers and Analyst

- Law Enforcement Specialists
- Incident Response Team Member
- IT Security Consultants
- Information Security Managers

Prerequisites:

- Basic knowledge of cybersecurity concepts and the cyber threat landscape.
- Familiarity with different types of malware and attack vectors.
- Basic experience with command-line interfaces and basic (CLI).
- Some programming/scripting experience will be beneficial but not mandatory (e.g., Python, PowerShell)