ARCADIA
Cyber Defense

# THE HIGHEST QUALITY CYBER SECURITY TRAINING

We believe your cyber security team deserves a better learning experience

# APT TACTICS AND DEFENSE

3 days

## Course Overview

In this short course, we aim to present how malware relates to APTs and how they differ from that used in more common, untargeted attacks.

We detail the typical intentions of an attacker and the tools and processes they would leverage to attain these goals.

Lastly, the course presents key approaches to detect and terminate the process of an APT, and the infrastructure required for effective incident response.

## Materials to bring

Laptop computer able to run 64-bits virtual machines.

VMware Workstation 11+, or VMware Fusion 6+, or VMware Player 11+

## Course prerequisites

None

## Course Breakdown

**Day 1** Targeted attacks: why and how

- Goals of the APT
- Software attacks
- Non-software attacks
- People-based attacks

**Day 2** Tactics and footprint of targeted attacks

- Defense systems and their weaknesses
- Signs of attacks

**Day 3** Effective defense against targeted attacks

- Pitfalls of attribution and deniability
- Reverse engineering
- Undermining exploitation
- CERT team cooperation and sharing