ARCADIA
Cyber Defense

THE HIGHEST QUALITY CYBER SECURITY TRAINING

We believe your cyber security team deserves a better learning experience

THREAT DETECTION AND SIMULATED ENGAGEMENT

5 days

Course Overview

Introduction of malware detection through its behaviours, storage and persistence tricks.

The first part of the course covers how to use Windows system introspection tools to find occurrences of running malware. While using Arc4dia's SNOW technology, the second part involves hands-on detection of malware and attacks live across a lab infrastructure.

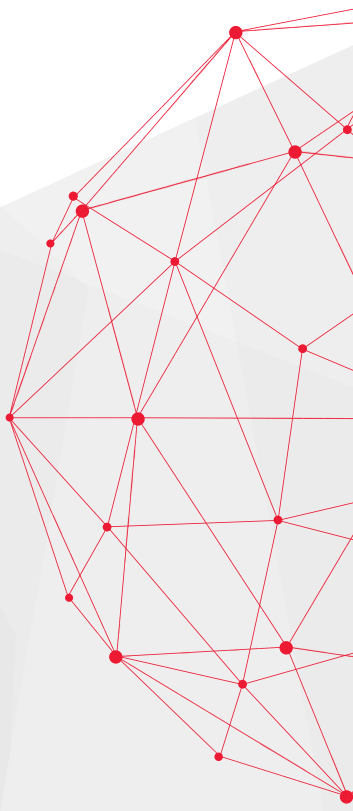
Materials to bring + vm

Laptop computer able to run 64-bits virtual machines.

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

Course prerequisites </>

Intro to Reverse Engineering



Course Breakdown

Day 1 Dynamic malware hunting

- Hunting with Sysinternals tools
- Thread injection
- Hiding modules
- Autoruns
- API hooking

Day 2 Malware appearance and behaviour

- False positives and false negatives
- Destructive malwares
- Rootkits

Day 3 Forensic analysis

- Volatility framework
- System dumping
- Process hiding
- Code injection
- Process dumping
- Footprints

Day 4 Hunting with SnowBoard 1

- Introduction to Snow
- Introduction to the SnowBoard interface
- Alert investigation
- Statistic investigation

Day 5 Hunting with SnowBoard 2

- Clustering rules
- Cloud modules
- Malware profiles