KOENIG SOLUTIONS · COURSE OUTLINE

# APT Hunting: Malware Analysis & Reverse Engineering

Learn to hunt, analyse and reverse-engineer APT malware, from indicators of compromise to strategic defence and team collaboration.

| 5 Days | 5 | 29 |
| --- | --- | --- |
| 8 HOURS A DAY | MODULES | TOPICS |

## COURSE OVERVIEW

This course covers the foundations of advanced persistent threats and malware, including their lifecycle, behaviours, persistence and evasion techniques, and the indicators of compromise they leave behind. It then addresses the principles of proactive threat hunting, covering network-focused and behavioral strategies alongside approaches to detecting malware through process, file and log analysis. It moves into static and dynamic malware analysis and reverse engineering, including decoding malware functionality and identifying command-and-control channels. It closes with APT detection and incident response, proactive defense through hardening, and building a threat hunting framework that integrates threat intelligence and collaboration between red and blue teams.

## WHO THIS COURSE IS FOR

- **Threat Hunters**
- **Malware Analysts**
- **Incident Responders**
- **SOC Analysts**
- **Reverse Engineers**
- **Security Operations Teams**

## LEARNING OBJECTIVES

- Explain the characteristics and lifecycle of advanced persistent threats
- Identify indicators of compromise linked to APT and malware activity
- Apply network-focused and behavioral threat hunting strategies
- Analyse suspicious processes, files and log data for anomalies
- Perform static and dynamic analysis of malware samples
- Interpret reverse-engineered malware to find C2 channels
- Assess APT activities such as lateral movement and privilege escalation
- Plan incident response, proactive defense and threat hunting frameworks

COURSE SYLLABUS

# 5 Modules, 29 Topics

01

## Foundations of APT and Malware Analysis

### UNDERSTANDING ADVANCED PERSISTENT THREATS (APTS)

- Characteristics and objectives of APTs
- The APT attack lifecycle

### INTRODUCTION TO MALWARE

- Types of malware and their behaviors
- Techniques used for persistence and evasion

### RECOGNIZING INDICATORS OF COMPROMISE (IOCS)

- Identifying key signs of APT and malware activity

02

## Principles of Threat Hunting

### INTRODUCTION TO THREAT HUNTING

- Purpose and benefits of proactive threat hunting
- Differences between threat hunting and traditional detection

### APT HUNTING STRATEGIES

- Network-focused approaches
- Behavioral analysis techniques

### APPROACHES TO MALWARE DETECTION

- Analyzing suspicious processes and files
- Examining log data for anomalies

03

## Advanced Malware Analysis Techniques

### STATIC MALWARE ANALYSIS

Examining file properties and structure · Recognizing malicious patterns

### DYNAMIC MALWARE ANALYSIS

Observing malware behavior during execution · Monitoring system and network changes

### INTRODUCTION TO REVERSE ENGINEERING

Decoding malware functionality · Identifying command-and-control (C2) channels

04

## APT Detection and Mitigation Strategies

### IDENTIFYING APT ACTIVITIES

- Spotting lateral movement and privilege escalation
- Uncovering stealth tactics used by attackers

### RESPONDING TO APT INCIDENTS

- Steps for containment and eradication
- Post-incident recovery and analysis

### PROACTIVE DEFENSE AGAINST APTS

- Building resilience through network and system hardening
- Implementing proactive threat detection strategies

05

## Integration and Strategic Defense

### DEVELOPING A THREAT HUNTING FRAMEWORK

- Establishing processes for continuous improvement
- Incorporating threat intelligence

### COLLABORATION BETWEEN TEAMS

- Aligning red and blue team activities
- Enhancing detection with combined efforts

### PRACTICAL APPLICATIONS OF APT AND MALWARE HUNTING

- Implementing best practices to secure the environment
- Building long-term defensive strategies

WHAT IS INCLUDED

## Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

## Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

## Learn the Way That Suits You

Classroom Training | Live Online Classes (ILO) | Fly-Me-A-Trainer (FMAT) | Flexi (Self-Paced) | 1-on-1 Training

### Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com | info@koenig-solutions.com