

## KL 057.7:

# Kaspersky Anti Targeted Attack. Investigation

## Course description

Kaspersky Anti Targeted Attack is a platform designed to protect an organization's IT infrastructure and detect sophisticated threats such as zero-day attacks, targeted attacks and advanced persistent threats (APTs). The solution is designed for enterprises and consists of three functional blocks, two of which are described in this course:

- Kaspersky Anti Targeted Attack (KATA), which protects the perimeter of the corporate IT infrastructure.
- Network Detection and Response (NDR), which protects the organization's internal network.

The theoretical part of the course and hands-on labs provide participants with the knowledge of how the solution works and the skills needed to detect and hunt for threats using Kaspersky Anti Targeted Attack.

## Duration

2 days (16 hours)

## Requirements for participants

To successfully master all the materials in this course, you will benefit from the knowledge and skills acquired by working with Kaspersky Anti Targeted Attack, which you can obtain by taking the following training course:

- KL 025.7 Kaspersky Anti Targeted Attack. Kaspersky EDR. Administration

You also need a general understanding of contemporary attacks and how they can be detected.

## Contents

1. Introduction
2. KATA NDR use
3. Sandbox analysis results
4. Reports and notifications

[Lab 1](#) Kaspersky Anti Targeted Attack activation

[Lab 2](#) Analyzing unencrypted protocol versions

[Lab 3](#) Network scanning

- Lab 4 Brute-force attack on the Alex domain account
- Lab 5 Sending remote commands and opening a remote shell session with a domain controller
- Lab 6 Remote collection of information on all domain users, and an ASREPROAST attack
- Lab 7 Pass-the-hash attack
- Lab 8 Collecting domain data
- Lab 9 Collecting data about the system, using steganography, data exfiltration
- Lab 10 Drive-by download attack
- Lab 11 Attack using the Caldera framework
- Lab 12 SYN flood attack
- Lab 13 DNS amplification attack
- Lab 14 Brute-force on the Administrator user of a corporate Linux server
- Lab 15 ARP spoofing and SSL stripping attack
- Lab 16 Launching a malicious container on a corporate server
- Lab 17 Exploiting web server vulnerabilities
- Lab 18 Ransomware and encryption key exfiltration
- Lab 19 Attack using the Caldera framework
- Lab 20 Reports