

## Kaspersky Anti Targeted Attack. Investigation (057.7)

ID KL-057.7 Цена 75 000,- руб. Длительность 2 дня

### Кому следует посетить

- Инженеры, отвечающие за внедрение и эксплуатацию систем защиты промышленных объектов от киберугроз.
- Сотрудникам службы информационной безопасности, которые осуществляют мониторинг состояния защиты промышленного объекта и реагируют на инциденты.
- Пресейл-специалисты.

### Предварительные требования

Чтобы успешно усвоить весь материал данного курса вам будут полезны знания и навыки работы с Kaspersky Anti Targeted Attack, которые вы можете получить пройдя учебный курс:

[Kaspersky Anti Targeted Attack. Kaspersky EDR. Administration \(025.7\)](#)

Также необходимые общие знания о типах современных атак, способах их выявления.

### Цели курса

Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет понять принципы использования решения и сможет выполнять задачи по детектированию и обнаружению угроз, используя Kaspersky Anti Targeted Attack.

### Содержание курса

Kaspersky Anti Targeted Attack – платформа, предназначенная для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats ("АПТ"). Решение разработано для корпоративных пользователей и включает в себя три функциональных блока, но в данном курсе будут рассмотрены два из них:

- Kaspersky Anti Targeted Attack ("КАТА"), обеспечивающий защиту периметра IT-инфраструктуры предприятия.
- Network Detection and Response ("NDR"), обеспечивающий защиту внутренней сети предприятия.

### Программа курса

Модуль 1. «Введение»

Модуль 2. «Эксплуатация КАТА NDR»

Модуль 3. «Результаты анализа Sandbox»

Модуль 4. «Отчетность и оповещения»

Лабораторная работа 1. Активация Kaspersky Anti Targeted Attack

Лабораторная работа 2. Анализ нешифрованных версий протоколов

Лабораторная работа 3. Сканирование сети

Лабораторная работа 4. BruteForce доменного пользователя Alex

Лабораторная работа 5. Удаленное выполнение команд, и открытие удаленной shell сессии до контроллера домена

Лабораторная работа 6. Удаленный сбор данных о всех пользователях домена и проведение атаки ASREPROAST

Лабораторная работа 7. Атака Pass-the-Hash

Лабораторная работа 8. Сбор данных о домене

Лабораторная работа 9. Сбор данных о системе, использование стеганографии, эксфильтрация данных

Лабораторная работа 10. Атака Drive by download

## Kaspersky Anti Targeted Attack. Investigation (057.7)

---

Лабораторная работа 11. Атака с использованием фреймворка Caldera

Лабораторная работа 12. Атака Syn flood

Лабораторная работа 13. Атака DNS Amplification

Лабораторная работа 14. BruteForce пользователя Administrator корпоративного linux сервера

Лабораторная работа 15. Атака Arp spoofing and sslstripping

Лабораторная работа 16. Запуск вредоносного контейнера на корпоративном сервере

Лабораторная работа 17. Эксплуатация уязвимостей веб-сервера

Лабораторная работа 18. Ransomware и эксфильтрация ключа шифрования

Лабораторная работа 19. Атака с использованием фреймворка Caldera

Лабораторная работа 20. Отчетность