



## **Kaspersky Unified Monitoring and Analysis Platform. Administration**

Код курса: KL 034.4

# Kaspersky Unified Monitoring and Analysis Platform. Administration

Код курса: KL 034.4

<b>Длительность</b>	20 ак. часов
<b>Формат</b>	
<b>Разработчик курса</b>	Лаборатория Касперского
<b>Тип</b>	Учебный курс
<b>Способ обучения</b>	Под руководством тренера

## О курсе

Kaspersky Unified Monitoring and Analysis Platform (KUMA) является решением класса SIEM, для сбора, хранения обработки, корреляции и визуализации разрозненных данных. Курс знакомит с архитектурой и возможностями решения, рассказывает и показывает, как выполнить установку и настройку решения на многочисленных примерах. Материалы курса включают слайды с описанием принципов работы и настройки, а также лабораторные работы для закрепления практических навыков настройки.

## Подробная информация

### Профиль аудитории:

- инженеры технической поддержки
- пресейл-инженеры

### Предварительные требования:

- понимание основ сетевых технологий: TCP/IP, DNS, электронной почты, web
- базовые навыки администрирования ОС Windows и Linux
- базовые знания об информационной безопасности
- представления о том, что такое регулирование

### По окончании курса слушатели изучат:

- развертывание Kaspersky Unified Monitoring and Analysis Platform для демонстрации решения
- настройку получения событий из разных источников и в разных форматах
- донастройку нормализации, агрегацию и обогащение событий согласно требованиям
- настройку корреляционных правил для обнаружения инцидентов
- настройку взаимодействия с внешними системами с целью обогащения событий и реагирования на инциденты
- обработку инцидентов и ручной анализ события
- настройку уведомлений и создание отчетов о работе решения

## Программа курса

1. Общие сведения
2. Архитектура
3. Установка
4. Сбор и обработка событий
5. Интеграции
6. Хранение событий
7. Корреляция
8. Алерты
9. Реагирование
10. Мониторинг состояния источников и метрики

### Лабораторные работы^

Лабораторная работа 1. Установить Kaspersky Unified Monitoring and Analysis Platform

Лабораторная работа 2. Настроить получение событий с помощью агента Windows (WMI)

Лабораторная работа 3. Настроить получение событий из DNS

Лабораторная работа 4. Настроить получение событий от Kaspersky Endpoint Security для Windows

Лабораторная работа 5. Настроить получение событий Linux

Лабораторная работа 6. Настроить получение событий Kaspersky Security Center

Лабораторная работа 7. Настроить получение событий Kaspersky Anti Targeted Attack Platform

Лабораторная работа 8. Настроить получение EDR-телеметрии из KATA

Лабораторная работа 9. Импортировать информацию о компьютерах из Kaspersky Security Center

Лабораторная работа 10. Настроить обогащение событий с помощью Active Directory

Лабораторная работа 11. Настроить интеграцию с Kaspersky Endpoint Detection and Response

Лабораторная работа 12. Настроить интеграцию с CyberTrace

Лабораторная работа 13. Настроить холодное хранение событий в KUMA

Лабораторная работа 14. Настроить мониторинг состояния источника

Лабораторная работа 15. Выполнить резервное копирование ядра (дополнительно)

Лабораторная работа 16. Настроить получение событий с помощью агента Windows (WEC)  
(дополнительно)

Лабораторная работа 17. Настроить маршрутизацию событий (дополнительно)

Лабораторная работа 18. Настроить авторизацию через Active Directory

Лабораторная работа 19. Настроить получение событий через rsyslog

Лабораторная работа 20. Обеспечить отказоустойчивость ядра

Лабораторная работа 21. Обеспечить отказоустойчивость коллектора

[Посмотреть расписание курса и записаться на обучение](#)

**Обращайтесь по любым вопросам**  
к менеджерам Учебного центра Softline

**8 (800) 505-05-07** | [edusales@softline.com](mailto:edusales@softline.com)

**Ждём вас на занятиях в Учебном центре Softline!**



## Почему Учебный центр Softline?

**Лидер** на рынке корпоративного обучения.

**Более 300 тысяч** подготовленных IT-специалистов.

**Гибкий индивидуальный подход** в обучении, скидки и акции.

**Широкая сеть представительств** в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

**Высокотехнологичное** оборудование

Более **18 лет** опыта работы

**Международные сертификаты** для IT-специалистов и пользователей в Центрах тестирования

**Сертифицированные тренеры** с богатым практическим опытом работы

**Авторизации от мировых производителей ПО** (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперского, Oracle, Autodesk, Код безопасности и других).

**Разработка курсов и тестов под заказ**, внедрение корпоративных систем обучения.

**Подробнее об Учебном центре Softline**

Вы можете узнать из [профайла](#).