

Kaspersky Unified Monitoring and Analysis Platform. Administration (034.4)

ID KL-034.4 Цена 84 900,- руб. Длительность 2 дня

Кому следует посетить

Курс ориентирован на инженеров технической и предпродажной поддержки.

Предварительные требования

От участников требуется:

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

Цели курса

По окончании курса слушатели смогут:

- Развернуть Kaspersky Unified Monitoring and Analysis Platform для демонстрации решения
- Настроить получение событий из разных источников и в разных форматах
- Настроить взаимодействие с внешними системами с целью обогащения событий и реагирования на инциденты
- Отслеживать состояние источников и компонентов системы

Содержание курса

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.

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