KL 034.2.1:

Kaspersky Unified Monitoring and Analysis Platform

Изучаемые продукты

Основной продукт:

- Kaspersky Unified Monitoring and Analysis Platform 2.0.1
- Kaspersky Unified Monitoring and Analysis Platform 2.1

Смежные продукты, выступающие источниками событий, источниками данных для обогащения и средствами реагирования в лабораторных работах:

- Kaspersky Security Center 14
- Kaspersky Endpoint Security 11.10
- Kaspersky Security for Windows Server 11.1
- Kaspersky Anti Targeted Attack Platform 4.1

Смежные продукты, выступающие источниками данных для обогащения в теоретических материалах:

- Kaspersky CyberTrace 4.1
- Kaspersky Threat Lookup

Описание 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.

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 нормализацию, агрегацию и обогащение событий согласно требованиям
- Настроить корреляционные правила для обнаружения инцидентов
- Настроить взаимодействие с внешними системами с целью обогащения событий и реагирования на инциденты
- Обработать инциденты и вручную проанализировать события
- Настроить уведомления и создать отчеты о работе решения

Основные лабораторные работы выполняются на KUMA 2.0. Затем предлагается выполнить дополнительные лабораторные работы на KUMA 2.1, в том числе и обновление с версии 2.0 на 2.1.

Длительность

3 дня

Требования к участникам

Курс ориентирован на инженеров технической и предпродажной поддержки. 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
- Представление о том, что такое регулярные выражения

Содержание

Лабораторная работа 8. **Импортировать информацию о компьютерах из KSC**
Лабораторная работа 9. **Настроить обогащение данными из LDAP**
Лабораторная работа 10. **Настроить обогащение данными из CyberTrace**

8. Работа с событиями

9. Корреляция

9.1. Виды правил корреляции
9.2. Простые правила корреляции
9.3. Стандартные корреляционные правила: селекторы, группы корреляции
9.4. Локальные и глобальные переменные

Лабораторная работа 11. **Создать простое корреляционное правило**
Лабораторная работа 12. **Создать стандартное корреляционное правило**
Лабораторная работа 13. **Настроить алерт на события в определенном порядке**

9.5. Активные списки и операционные правила корреляции
9.6. Ретроспективный поиск

Лабораторная работа 14. **Создать техническое корреляционное правило для наполнения активного списка**
Лабораторная работа 15. **Создать корреляционное правило с использованием активного списка**
Лабораторная работа 16. **Создать корреляционное правило с использованием локальной переменной**
Лабораторная работа 17. **Применить ретроспективный поиск**

10. Работа с алертами

11. Реагирование

11.1. Реагирование задачей Kaspersky Security Center
11.2. Реагирование запуском скрипта
11.3. Реагирование задачей Kaspersky Endpoint Detection and Response

Лабораторная работа 18. **Настроить реагирование запуском задачи Kaspersky Security Center**
Лабораторная работа 19. **Настроить реагирование запуском задачи Kaspersky Endpoint Detection and Response**

12. Отчетность

12.1. Панели мониторинга
12.2. Отчеты
12.3. Метрики

Лабораторная работа 20. **Изучить отчетность**
Лабораторная работа 21. **Отправить запрос в Kaspersky Unified Monitoring and Analysis Platform через REST API (опционально)**

13. Что нового в KUMA 2.1

Лабораторная работа 22. **Обновить Kaspersky Unified Monitoring and Analysis до версии 2.1**
Лабораторная работа 23. **Добавить актуальный контент из репозитория доступных обновлений Лаборатории Касперского**
Лабораторная работа 24. **Настроить «холодное» хранение событий в Kaspersky Unified Monitoring and Analysis Platform**