KL 034.3.2:

Kaspersky Unified Monitoring and Analysis Platform

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
- Донастроить 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

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

Темы

1. **Введение в SIEM**
2. **Архитектура и принципы работы KUMA**
3. **Установка**

   Варианты установки: all-in-one, распределенная, установка в режиме высокой доступности
4. **Сбор событий**

   Принцип работы коллектора, настройки подключения и коннектора, получение событий.
5. **Нормализация**

   Модель данных KUMA, настройки нормализатора, преобразование данных, дополнительные нормализаторы
6. **Обработка событий коллектором**

   Фильтрация, агрегация, обогащение.
7. **Интеграции**

   Интеграция с Kaspersky Security Center и работа с активами, интеграция с LDAP и работа с учетными записями, интеграция с Kaspersky Threat Lookup, Kaspersky CyberTrace и Kaspersky Endpoint Detection and Response.
8. **Работа с событиями**
9. **Корреляция**

   Виды правил корреляции, переменные, активные списки и ретроспективный поиск.
10. **Работа с алертами**
11. **Реагирование**

    Реагирование задачей Kaspersky Security Center, реагирование запуском скрипта, реагирование задачей Kaspersky Endpoint Detection and Response.
12. **Отчетность**

    Панели мониторинга, отчеты, покрытие матрицы MITRE ATT&CK, метрики

Лабораторные работы

Лабораторная работа 1.	Установить Kaspersky Unified Monitoring and Analysis Platform
Лабораторная работа 2.	Настроить получение событий из Windows Event Log
Лабораторная работа 3.	Настроить получение событий из журнала Windows DNS Analytic (факультативно)
Лабораторная работа 4.	Настроить получение событий Linux (факультативно)
Лабораторная работа 5.	Настроить получение событий Kaspersky Security Center
Лабораторная работа 6.	Настроить получение событий Kaspersky Anti Targeted Attack Platform

Лабораторная работа 7.	Настроить получение EDR-телеметрии из KATA
Лабораторная работа 8.	Настроить обогащение событий данными из DNS
Лабораторная работа 9.	Настроить обогащение событий данными по GeoIP
Лабораторная работа 10.	Импортировать информацию о компьютерах из Kaspersky Security Center
Лабораторная работа 11.	Настроить обогащение событий с помощью Active Directory
Лабораторная работа 12.	Настроить обогащение данными из CyberTrace
Лабораторная работа 13.	Настроить «холодное» хранение событий в KUMA
Лабораторная работа 14.	Создать простое корреляционное правило
Лабораторная работа 15.	Создать стандартное корреляционное правило
Лабораторная работа 16.	Настроить алерт на события в определенном порядке
Лабораторная работа 17.	Создать корреляционное правило с использованием локальной переменной
Лабораторная работа 18.	Создать техническое корреляционное правило для наполнения активного списка
Лабораторная работа 19.	Создать корреляционное правило с использованием активного списка
Лабораторная работа 20.	Применить ретроспективный поиск
Лабораторная работа 21.	Настроить реагирование запуском задачи Kaspersky Security Center
Лабораторная работа 22.	Настроить реагирование запуском задачи Kaspersky Endpoint Detection and Response
Лабораторная работа 23.	Изучить отчетность
Лабораторная работа 24.	Отправить запрос в KUMA через REST API (факультативно)
Лабораторная работа 25.	Настройка Event router service (факультативно)
Лабораторная работа 26.	Создание правила на основе функции вычисления энтропии (факультативно)