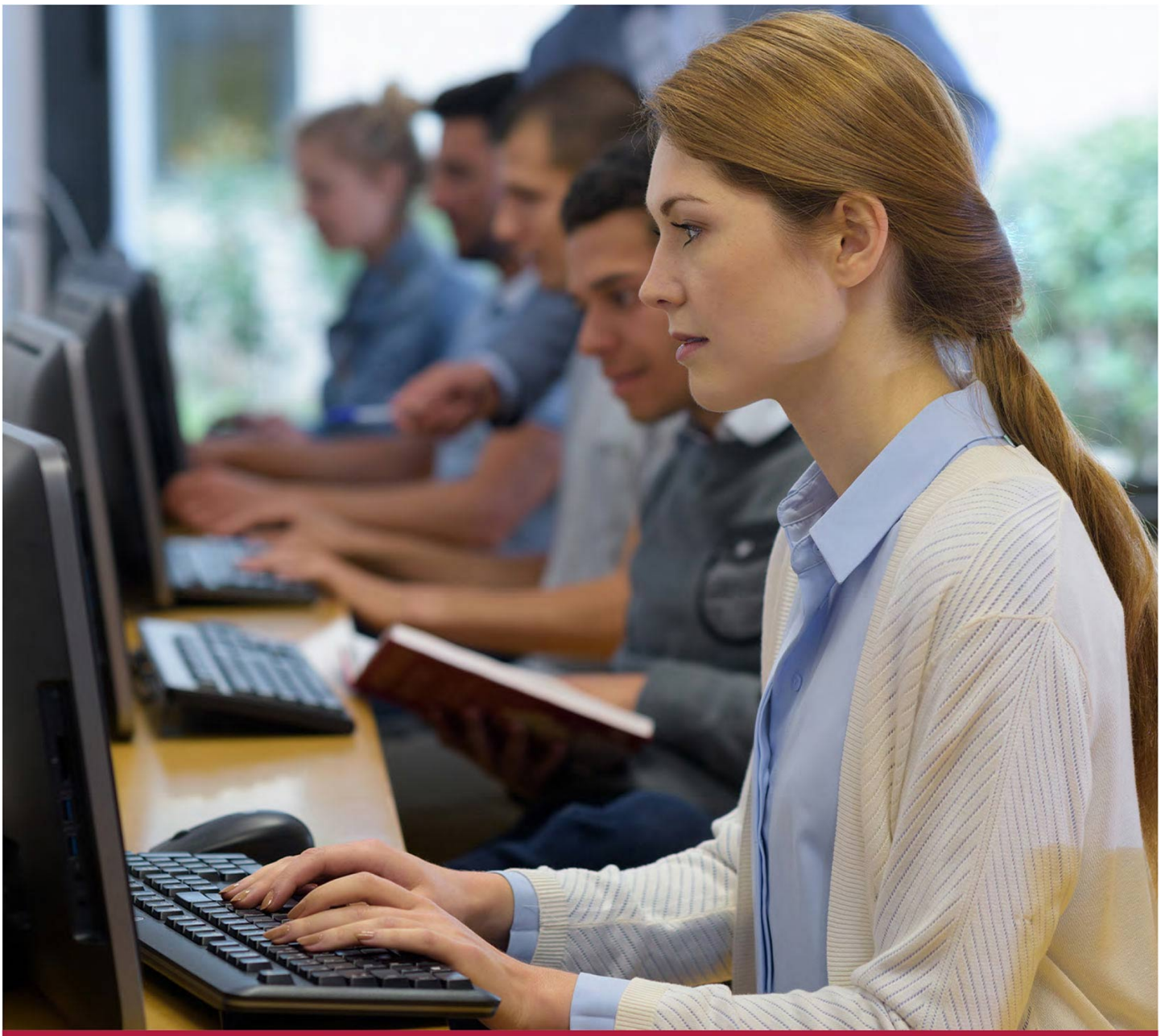
softline учебный центр



Kaspersky Unified Monitoring and Analysis Platform

Код курса: KL 034.3.2

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Kaspersky Unified Monitoring and Analysis Platform

Код курса: KL 034.3.2

Длительность	24 ак. часа
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Kaspersky Unified Monitoring & Analysis Platform 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:

Курс ориентирован на инженеров технической и предпродажной поддержки.

Предварительные требования:

- 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

По окончании курса слушатели смогут:

- Развернуть Kaspersky Unified Management & Analysis 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

Программа курса

Модуль 1. Общие сведения

- Введение в SIEM
- Введение в KUMA

Модуль 2. Архитектура и принципы работы KUMA

- Архитектура KUMA
- Принципы работы KUMA

Модуль 3. Установка

- Варианты установки: all-in-one, распределенная, установка в режиме высокой доступности

Модуль 4. Сбор событий

- Принцип работы коллектора
- Настройки подключения и коннектора
- Получение событий

Модуль 5. Нормализация

- Модель данных KUMA
- Настройки нормализатора
- Преобразование данных
- Дополнительные нормализаторы

Модуль 6. Обработка событий коллектором

- Фильтрация
- Агрегация
- Обогащение

Модуль 7. Интеграции

- Интеграция с Kaspersky Security Center и работа с активами
- Интеграция с LDAP и работа с учетными записями
- Интеграция с Kaspersky Threat Lookup
- Интеграция с Kaspersky CyberTrace
- Интеграция с Kaspersky Kaspersky Endpoint Detection and Response

Модуль 8. Работа с событиями

- Принципы работы событий

Модуль 9. Корреляция

- Виды правил корреляции
- Простые правила корреляции

- Локальные и глобальные переменные
- Активные списки
- Ретроспективный поиск

Модуль 10. Работа с алертами

- Основные принципы

Модуль 11. Реагирование

- Реагирование задачей Kaspersky Security Center
- Реагирование запуском скрипта
- Реагирование задачей Kaspersky Endpoint Detection and Response

Модуль 12. Отчетность

- Панели мониторинга
- Отчеты
- Покрытие матрицы MITRE ATT&CK
- Метрики

- 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)

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | 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.