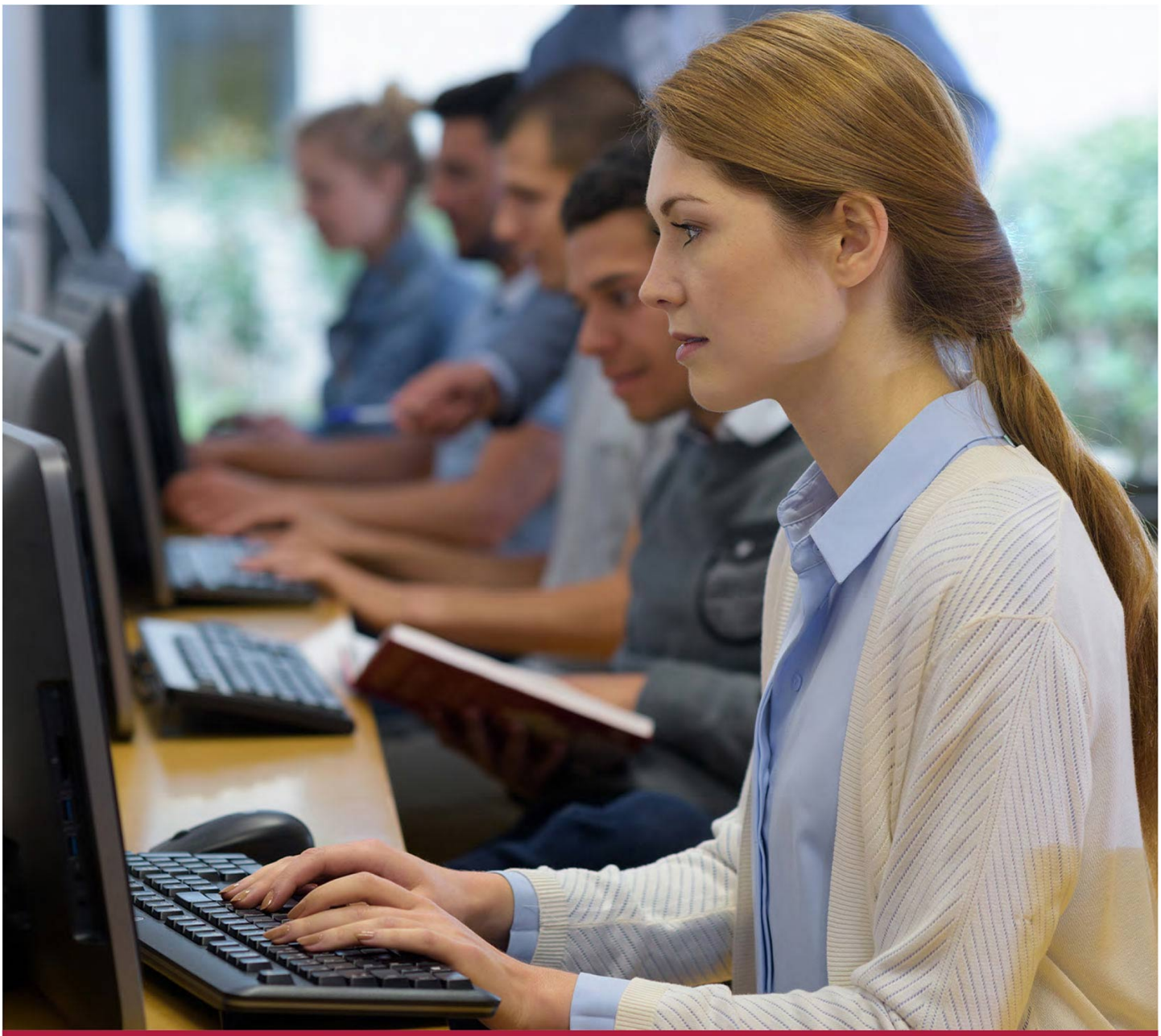
softline учебный центр



Kaspersky Unified Monitoring and Analysis Platform. Investigation

Код курса: KL 051.4

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

Kaspersky Unified Monitoring and Analysis Platform. Investigation

Код курса: KL 051.4

Длительность	20 ак. часов
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	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. Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет выполнять задачи по детектированию и обнаружению угроз, используя Kaspersky Unified Monitoring and Analysis Platform.

Подробная информация

Профиль аудитории:

- инженеры технической поддержки
- пресейл-инженеры

Предварительные требования:

- Базовые навыки администрирования ОС Windows и Linux
- Базовые знания об информационной безопасности
- Общие знания о типах современных атак, способах их выявления
- Освоение материала курса KL 034.4 Kaspersky Unified Monitoring and Analysis Platform.

По окончании курса слушатели изучат:

- Процесс настройки обработки событий (нормализация, агрегация, обогащение и тд.)
- Создание правил корреляции и анализа данных для выявления угроз
- Создание различных правил реагирования на угрозы
- Процесс использования ресурсов и функций KUMA для анализа и выявления угроз (активные списки, словари, переменные, API и тп.)
- Выявление угроз, анализируя полученные события

Программа курса

1. Введение
2. Сбор событий
3. Работа с активами
4. Поиск событий
5. Корреляция
6. AI
7. Реагирование
8. Панели мониторинга и отчеты

Лабораторные работы

- Лабораторная работа 1. Активация KUMA
- Лабораторная работа 2. Нормализация событий нового источника
- Лабораторная работа 3. Нормализация событий еще одного нового источника
- Лабораторная работа 4. Настройка обогащения событий
- Лабораторная работа 5. Сбор данных и эксфильтрация, установка C&C туннеля
- Лабораторная работа 6. Сбор данных о системе, использование стеганографии, эксфильтрация данных
- Лабораторная работа 7. Kerberoasting, эксфильтрация данных через HTTP GET
- Лабораторная работа 8. Атака Pass-the-hash, эксфильтрация данных через ssh
- Лабораторная работа 9. Атака HTA
- Лабораторная работа 10. Shadow session и Dll hijacking
- Лабораторная работа 11. Закрепление в системе
- Лабораторная работа 12. Самостоятельное задание
- Лабораторная работа 13. Отображение текущего состояния

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.