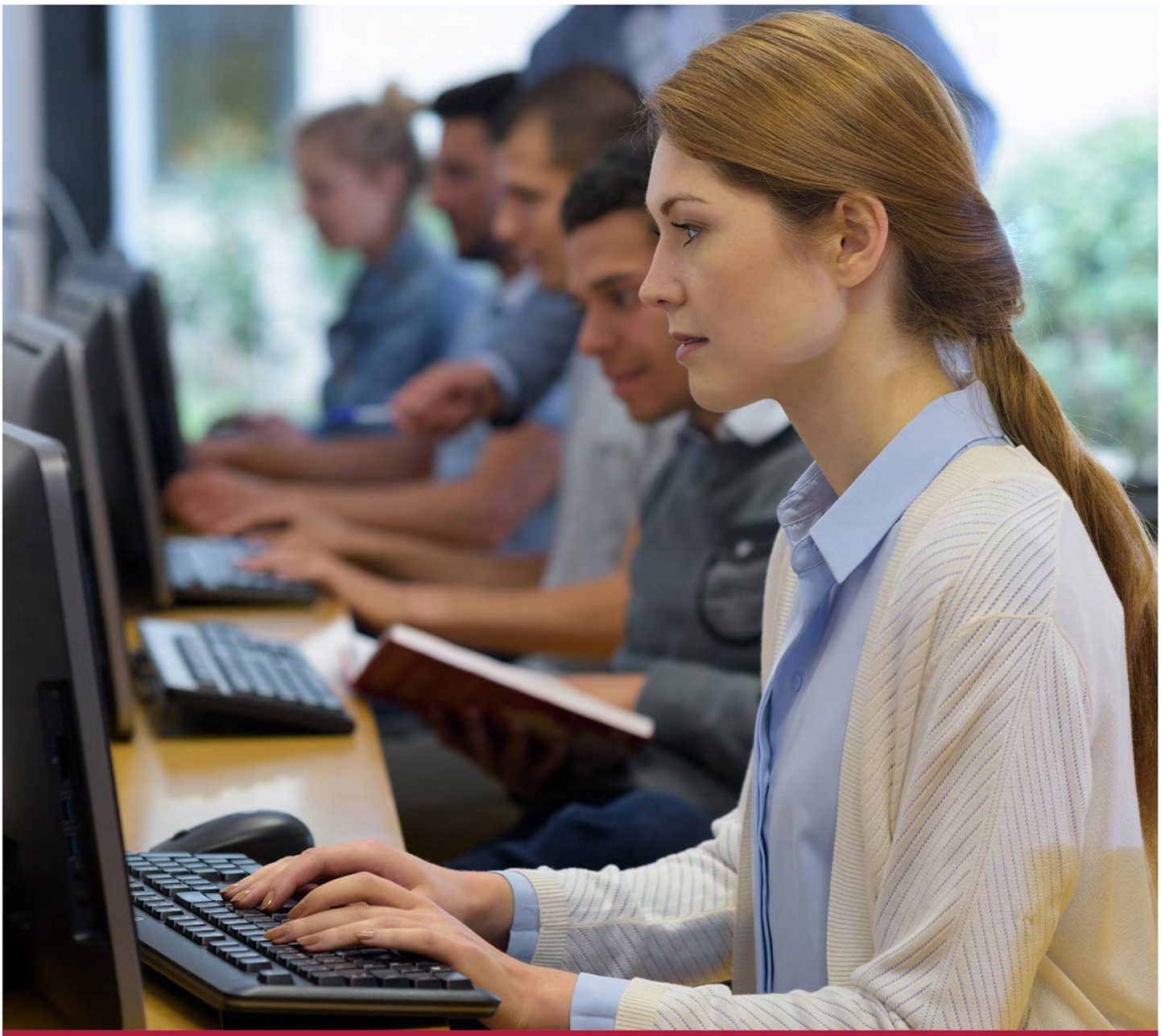
softline учебный центр



Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response

Код курса: KL 025.5

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

Kaspersky Anti Targeted Attack Platform, Kaspersky Endpoint Detection and Response

Код курса: KL 025.5

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

О курсе

Платформа Kaspersky Anti Targeted Attack совместно с Kaspersky EDR представляет собой решение класса XDR (Extended Detection and Response) нативного типа и помогает организациям построить надежную систему защиты корпоративной инфраструктуры от сложных кибератак. Теоретический материал и лабораторные работы дают слушателям необходимые знания и навыки, благодаря которым слушатель сможет спланировать и выполнить развертывание и настройку решения, будет понимать принципы использования решения и сможет выполнять задачи по его обслуживанию.

Подробная информация

Профиль аудитории:

Курс ориентирован на иженеров, отвечающих за внедрение и эксплуатацию систем защиты промышленных объектов от киберугроз.

Сотрудникам службы информационной безопасности, которые осуществляют мониторинг состояния защиты промышленного объекта и реагируют на инциденты

Специалистам предпродажной подготовки, которые консультируют заказчика по вопросам возможностей и оптимальных сценариев внедрения и использования продукта

Цели: обучить слушателей основным продуктам:

Kaspersky Anti Targeted Attack Platform 5.0

Kaspersky Endpoint Detection and Response 5.0

Kaspersky Endpoint Agent 3.14

Kaspersky Security Center 14.0

Kaspersky Endpoint Detection and Response (Cloud) — отдельный модуль

Предварительные требования:

Понимание основ работы с Kaspersky Security Center.

Понимание основ сетевых технологий: DNS, маршрутизации, электронной почты, Web.

Базовые навыки администрирования Windows и Linux.

Представление о современных угрозах и тенденциях развития информационных технологий.

По окончании курса слушатели смогут:

Спланировать и выполнить развертывание и настройку решения

Понимать принципы использования решения

Выполнять задачи по его обслуживанию

Программа курса

Модуль 1. Введение

- Изучаемые продукты и приложения
- Ландшафт угроз
- Проблемы при построении системы ИБ
- Подходы к построению системы ИБ
- Какие задачи заказчика помогает решить KATA Platform

Модуль 2. Подготовка к внедрению

- Основные возможности
- Приложения и компоненты
- Системные требования
- Масштабирование
- Типичные топологии

Модуль 3. Развертывание платформы KATA

- Организация процесса
- Установка серверов
- Активация и первоначальная настройка
- Распределенная установка
- Установка Kaspersky Endpoint Agent
- Лабораторная работа 1. Установить и настроить центральный узел
- Лабораторная работа 2. Настроить Kaspersky Sandbox
- Лабораторная работа 3. Подключить центральный узел к Sandbox
- Лабораторная работа 4. Активировать Центральный узел
- Лабораторная работа 5. Создать учетную запись сотрудника службы информационной безопасности

Модуль 4. Эксплуатация KATA

- Подключение к источникам трафика
- Технологии обнаружения KATA
- Обработка обнаружений
- Идентификация угроз в трафике
- Лабораторная работа 6. Подключить центральный узел к сетевой инфраструктуре (SPAN)
- Лабораторная работа 7. Проверить, что анализ трафика работает
- Лабораторная работа 8. Подключить центральный узел к почтовой системе по протоколу SMTP
- Лабораторная работа 9. Настроить почтовый сервер посылать копии сообщений на центральный узел
- Лабораторная работа 10. Проверить, что анализ почты работает
- Лабораторная работа 11. Устранить многократную проверку почтовых сообщений
- Лабораторная работа 12. Подключить сенсор к прокси-серверу (ICAP)
- Лабораторная работа 13. Проверить, что анализ ICAP-трафика работает
- Лабораторная работа 14. Устранить многократную проверку http-трафика

Модуль 5. Эксплуатация KEDR

- Технологии обнаружения KEDR
- Расследование инцидента
- Реагирование на инцидент

Модуль 6. Технология Sandbox

- Технология Sandbox

Модуль 7. Обслуживание платформы KATA

- VIP-статус
- Проверка архивов с паролем
- External API
- Отчеты
- Почтовые уведомления
- Интеграция с SIEM
- Мониторинг сервера по SNMP
- Сбор информации о системе
- Обновление
- Сохранение и восстановление настроек
- Обновление версии
- Изменение системных настроек
- Kaspersky Private Security Network (KPSN)
- Лабораторная работа 15. Установить Kaspersky Endpoint Agent с помощью KSC
- Лабораторная работа 16. Подключить Kaspersky Endpoint Agent к центральному узлу
- Лабораторная работа 17. Активировать Kaspersky Endpoint Agent
- Лабораторная работа 18. Проверить, что подсистема TAA работает

- Лабораторная работа 19. Симулировать вредоносную нагрузку
- Лабораторная работа 20. Продемонстрировать результаты работы KATA
- Лабораторная работа 21. Демонстрация анализа и реагирования на обнаружение TAA
- Лабораторная работа 22. Изучить подробности выполнения файла в песочнице
- Лабораторная работа 23. Добавить сторонние правила IDS
- Лабораторная работа 24. Написать свое правило IDS
- Лабораторная работа 25. Создать исключение для IDS-правила
- Лабораторная работа 26. Написать свое правило Yara
- Лабораторная работа 27. Настроить интеграцию с Active Directory
- Лабораторная работа 28. Работа с API

Модуль 8. Отдельный модуль Kaspersky Endpoint Detection and Response (Cloud)

- Kaspersky Endpoint Detection and Response (Cloud)

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.