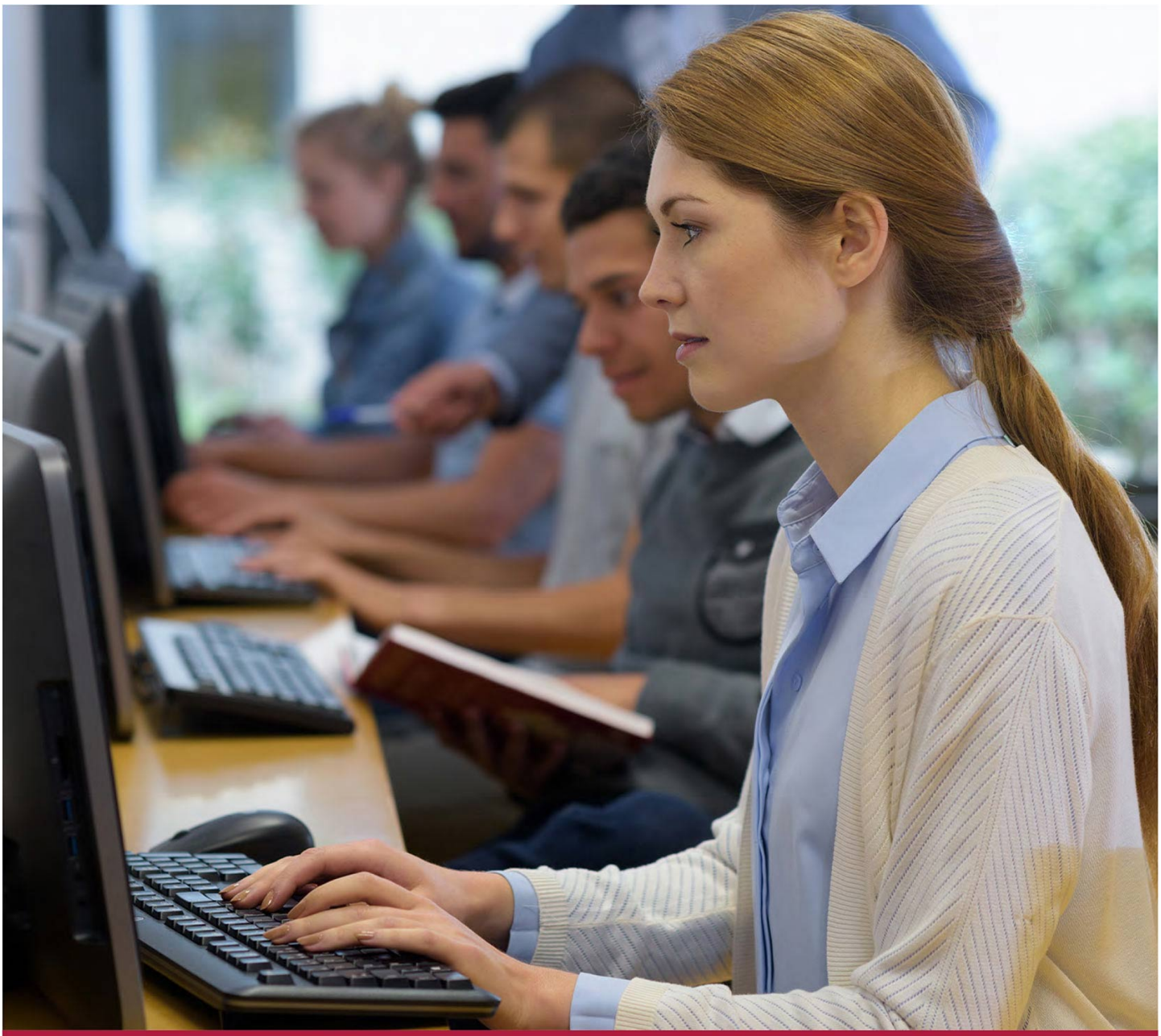
softline учебный центр



Kaspersky Anti Targeted Attack. Investigation

Код курса: KL 057.7

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

Kaspersky Anti Targeted Attack. Investigation

Код курса: KL 057.7

Длительность	16 ак. часов
Формат	
Разработчик курса	Лаборатория Касперского
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

Kaspersky Anti Targeted Attack – платформа, предназначенная для защиты IT-инфраструктуры организации и своевременного обнаружения таких угроз, как атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats ("APT"). Решение разработано для корпоративных пользователей и включает в себя три функциональных блока, но в данном курсе будут рассмотрены два из них: Kaspersky Anti Targeted Attack ("KATA"), обеспечивающий защиту периметра IT-инфраструктуры предприятия. Network Detection and Response ("NDR"), обеспечивающий защиту внутренней сети предприятия. Теоретический материал и лабораторные работы дают необходимые знания и навыки, благодаря которым слушатель сможет понять принципы использования решения и сможет выполнять задачи по детектированию и обнаружению угроз, используя Kaspersky Anti Targeted Attack.

Подробная информация

Профиль аудитории:

- Инженеры, отвечающие 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.
- Пресейл-специалисты.

Предварительные требования:

- Чтобы успешно усвоить весь материал данного курса вам будут полезны знания и навыки работы с Kaspersky Anti Targeted Attack: KL 025.7 Kaspersky Anti Targeted Attack. Kaspersky EDR. Administration
- 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 детектированию и обнаружению угроз.

Программа курса

Модуль 1. «Введение»

Модуль 2. «Эксплуатация KATA NDR»

Модуль 3. «Результаты анализа Sandbox»

Модуль 4. «Отчетность и оповещения»

Лабораторная работа 1. Активация Kaspersky Anti Targeted Attack

Лабораторная работа 2. Анализ нешифрованных версий протоколов

Лабораторная работа 3. Сканирование сети

Лабораторная работа 4. BruteForce доменного пользователя Alex

Лабораторная работа 5. Удаленное выполнение команд, и открытие удаленной shell сессии до контроллера домена

Лабораторная работа 6. Удаленный сбор данных о всех пользователях домена и проведение атаки ASREPROAST

Лабораторная работа 7. Атака Pass-the-Hash

Лабораторная работа 8. Сбор данных о домене

Лабораторная работа 9. Сбор данных о системе, использование стеганографии, эксфильтрация данных

Лабораторная работа 10. Атака Drive by download

Лабораторная работа 11. Атака с использованием фреймворка Caldera

Лабораторная работа 12. Атака Syn flood

Лабораторная работа 13. Атака DNS Amplification

Лабораторная работа 14. BruteForce пользователя Administrator корпоративного linux сервера

Лабораторная работа 15. Атака Arp spoofing and sslstripping

Лабораторная работа 16. Запуск вредоносного контейнера на корпоративном сервере

Лабораторная работа 17. Эксплуатация уязвимостей веб-сервера

Лабораторная работа 18. Ransomware и эксфильтрация ключа шифрования

Лабораторная работа 19. Атака с использованием фреймворка Caldera

Лабораторная работа 20. Отчетность

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.