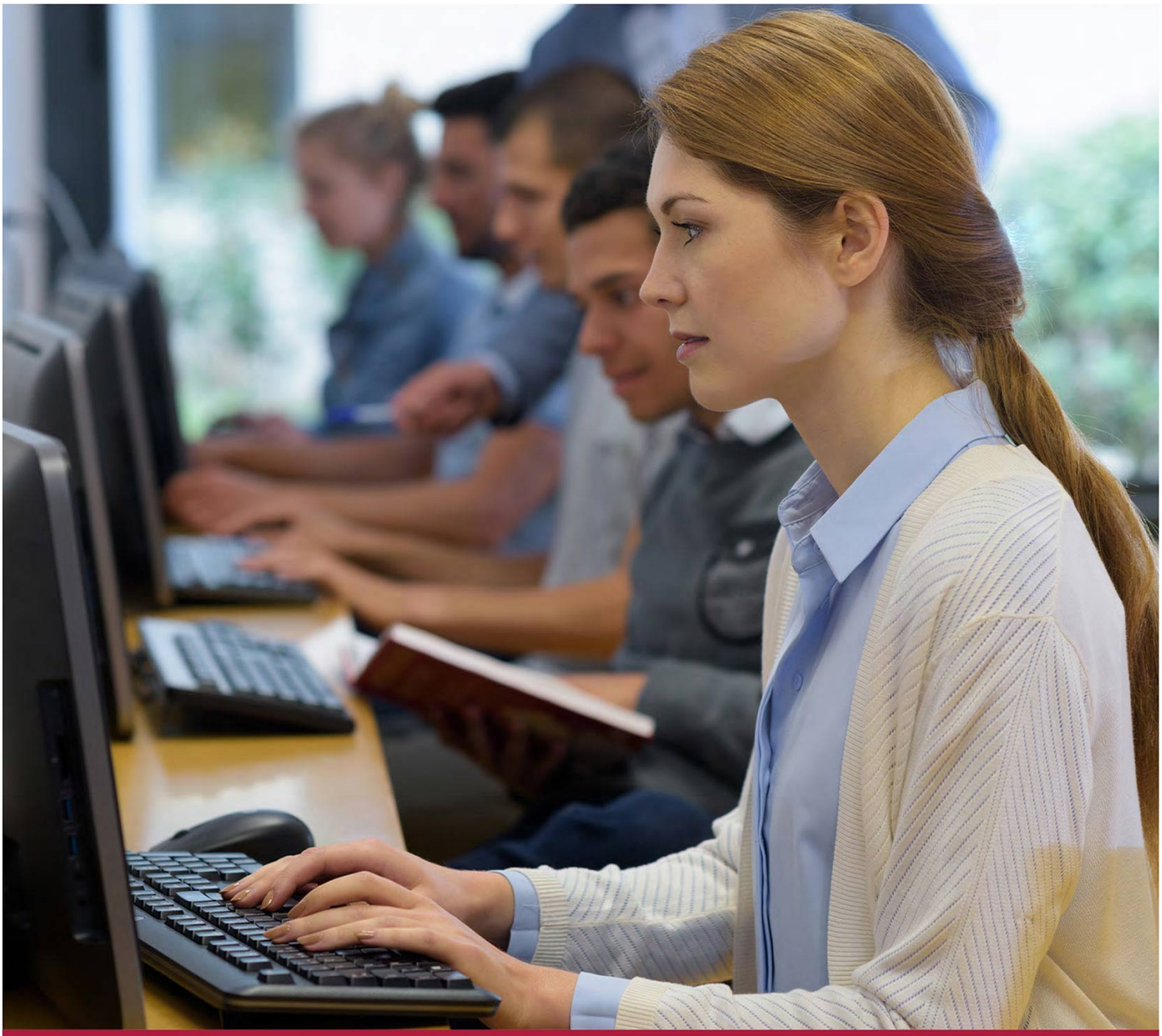
softline®

Учебный центр Softline



Эффективное обнаружение угроз с помощью YARA

Код курса: KL-YARAKU

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

Эффективное обнаружение угроз с помощью YARA

Код курса: KL-YARAKU

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

О курсе

Данный курс предназначен для ИТ-специалистов в чьи рутинные обязанности входит отслеживание инцидентов и поиск угроз (threat hunting). Аудиторию курса составляют аналитики и инженеры в области безопасности, аналитики вредоносного кода, специалисты в области сетевой безопасности, APT-аналитики. Курс подходит как начинающим, так и опытным пользователям Yara с опытом реверс-инжиниринга и без. Слушатели научатся создавать эффективные правила Yara, тестировать их и улучшать их для нахождения любых угроз. Во время курса слушатели также получат доступ к некоторым внутренним утилитам Kaspersky Lab и научатся разрабатывать эффективные стратегии обнаружения APT с использованием Yara. Данный курс проводит Kaspersky Lab, привлекая собственных тренеров (только очно, г. Москва)

Подробная информация

Профиль аудитории:

- Аналитики и инженеры в области безопасности, аналитики вредоносного кода, специалисты в области сетевой безопасности, APT-аналитики.

Предварительные требования:

- Начальный опыт работы с Yara;
- Опыт расследования инцидентов и обнаружения угроз.

По окончании курса слушатели смогут:

- Создавать эффективные правила Yara
- Повысить уровень и качество процесса обнаружения угроз безопасности.

Программа курса

Модуль 1 Краткий обзор синтаксиса Yara

Модуль 2 Советы по быстрому созданию эффективных правил

Модуль 3 Генераторы Yara

Модуль 4 Тестирование правил на ложные срабатывания

Модуль 5 Поиск новых сэмплов в VT

Модуль 6 Использование внешних модулей Yara для повышения эффективности обнаружения

Модуль 7 Поиск аномалий

Модуль 8 Примеры из реальной жизни

Модуль 9 Упражнения для закрепления материала

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 **17 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 Касперсокого, 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 и презентации