kaspersky

Отражайте APT-угрозы с помощью YARA наравне с экспертами GReAT

Экспертный онлайн-тренинг по кибербезопасности для ИБ-специалистов

Экспертам «Лаборатории Касперского» удалось выявить большое количество громких APT-атак. Хотите научиться обнаруживать угрозы так же эффективно? Для вас наш тренинг. Он расширит ваши знания об активном поиске угроз, поможет улучшить стратегию реагирования на инциденты и откроет вам доступ к опыту профессионалов. И все это – в режиме онлайн. Наши эксперты расскажут о важной системе обнаружения киберугроз – YARA.

Тренинг проходит в произвольном темпе. Вам доступна виртуальная лаборатория со множеством эксклюзивных заданий, основанных на реальных случаях из практики исследователей «Лаборатории Касперского»

Подкрепим теорию практикой
В виртуальной лаборатории можно выполнить более 20 практических заданий, основанных на эксклюзивных исследованиях APT-угроз, проведенных экспертами «Лаборатории Касперского».

Поможем развить новые навыки
Когда вы научитесь определять угрозы быстрее и с меньшими усилиями, ваши навыки в сфере кибербезопасности перейдут на новый уровень.

Поделимся опытом
Эксперты «Лаборатории Касперского» были одними из первых специалистов по активному поиску угроз. Они расскажут, как используют YARA для обнаружения APT-атак, которые не может выявить никто другой.

Содержание тренинга

Тренинг подходит как начинающим, так и опытным пользователям YARA и не требует серьезных навыков обратной разработки.

Почему YARA?

Для профессионалов в сфере кибербезопасности

- Совершенствуйте навыки активного поиска угроз
- Боритесь с угрозами еще эффективнее
- Находите образцы APT с помощью VirusTotal
- Создавайте эффективные стратегии выявления угроз

Для крупного бизнеса

- Научите своих специалистов находить новые образцы вредоносного ПО, эксплойты и угрозы нулевого дня
- Ускорьте реагирование на инциденты
- Укрепите защиту с помощью собственных YARA-правил

Практический результат

На тренинге вы узнаете, как создавать наиболее эффективные YARA-правила, тестировать и улучшать их, чтобы выявлять угрозы, которые не удается обнаружить другим.

Вы научитесь

- Писать четкие и эффективные YARA-правила
- Использовать советы и приемы для быстрого создания действенных правил
- Применять YARA-генераторы для экономии времени и сил при написании кода
- Тестировать YARA-правила на ложные срабатывания, которые могут исказить результат
- Выявлять скрытые образцы вредоносного ПО в своей инфраструктуре и на облачных платформах
- Использовать внешние модули в YARA для еще более эффективного поиска угроз
- Проводить продвинутый поиск аномалий
- Проверять свои знания на реальных примерах, таких как атаки групп BlueTraveller и DiplomaticDuck

Особенности тренинга

Доступ	Курс доступен в течение 6 месяцев с момента активации кода
Язык	Все материалы предоставляются на английском языке (включая субтитры)
Темп	Возможность выбрать график, который подходит именно вам
Продолжительность	Около 15 часов
Скачиваемые материалы	Материалы тренинга и рекомендации в формате PDF
Технические требования	Браузер на компьютере, телефоне или планшете (кроме занятий в виртуальной лаборатории, для которых требуется RDP-клиент)
Автор тренинга	Костин Райю, руководитель GReAT, «Лаборатория Касперского»
Видеоматериалы	Более 50 видео, которые помогут пройти курс
Работа в виртуальной лаборатории	200 часов практических занятий
Поддержка	Задайте вопрос через форму на сайте help.kasperskyxtraining.com, и мы ответим вам по электронной почте

Автор тренинга

Костин Райю,
руководитель GReAT

Костин возглавляет глобальный центр исследований и анализа угроз (GReAT) «Лаборатории Касперского», специалисты которого изучали такие угрозы и киберпреступные группы, как Stuxnet, Duqu, Flame, Carbanak, Turla, Lazarus, Equation Group и многие другие.

Костин работает в сфере кибербезопасности уже более 25 лет. Его специализация – анализ APT-угроз и высокоуровневых кибератак.

Костин является членом технического консультативного совета журнала Virus Bulletin, участником Организации антивирусных исследований (CARO) и корреспондентом проекта The WildList Organization International.

Наши эксперты по кибербезопасности – одни из лучших в отрасли, и на этом онлайн-тренинге они поделятся опытом, наработками и собственными ноу-хау.
Сотрудники GReAT работают по всему миру – в России, Европе, Северной и Южной Америке, в Азии и на Ближнем Востоке. Они знают все о выявлении и анализе самых изощренных угроз, в том числе связанных с кибершпионажем и киберсаботажем.

На счету исследователей GReAT расследование более 400 киберкампаний разной сложности. Мировые СМИ регулярно обращаются к ним за экспертными комментариями. Таким образом, вы будете получать знания у профессионалов своего дела, которых отличает огромный опыт, энтузиазм и жажда новых открытий.

Тренинги по кибербезопасности:
kaspersky.ru/enterprise-security/cyber-security-training