Kaspersky Cybersecurity Training

kaspersky

Одна из самых острых проблем, связанных с ИБ, — это нехватка квалифицированных специалистов, которые могут защитить инфраструктуру компании, в условиях когда IT-среда и ландшафт угроз постоянно меняются.

Тренинги «Лаборатории Касперского» были разработаны в ответ на постоянные перемены в ландшафте угроз.

Эксперты мирового уровня поделятся своим опытом и передадут участникам актуальные знания об эффективных стратегиях обнаружения угроз и снижения рисков.

Для ИБ-специалистов «Лаборатория Касперского» предлагает следующие тренинги:

Тренинг	Количество дней
Анализ и обратная разработка вредоносного ПО	5 дней
Анализ и обратная разработка вредоносного ПО (экспертный уровень)	5 дней
Расследование и реагирование на инциденты	5 дней
Тренинг по YARA	2 дня

Программы для специалистов по кибербезопасности
в промышленности и в области интернета вещей

Тренинг	Количество дней
Цифровая криминалистика в АСУ ТП	5 дней
Обнаружение уязвимостей с помощью фаззинга	3 дня
Поиск уязвимостей в устройствах IoT	3 дня

Проводите расследования вредоносных атак еще успешнее. Навыки, которыми вы овладеете после прохождения курсов:

Анализ и обратная разработка вредоносного ПО

- Обратная разработка вредоносных документов и эксплойтов
- Работа с обфусцированным и зашифрованным кодом вредоносного ПО
- Знакомство с инструментами обратной разработки, написанными на разных языках программирования, в том числе скриптовых и скомпилированных для разных архитектур операционных систем Windows и Linux с помощью разных компиляторов
- Изучение расширенных возможностей инструментов для обратной разработки, в том числе функции создания скриптов в IDA Pro
- Детальный разбор стеганографии
- Углубленное знакомство с ассемблированием
- Анализ шелл-кода

Анализ и обратная разработка вредоносного ПО (экспертный уровень)

Анализ современных образцов сложного кода: от получения первоначального артефакта до создания технического описания TTP с IoC

- Создание статических дешифраторов для решения реальных задач и дальнейший углубленный анализ вредоносного кода
- Анализ вредоносных документов, которые обычно используются для доставки вредоносных программ, и их извлечение
- Достоверная оценка причиненного атакой ущерба, точное и эффективное реагирование на инцидент

Овладейте практическими навыками выявления атак и методов реагирования на них

Некоторые темы курса:

Основы реагирования на инциденты

Создание лаборатории цифровой криминалистики

Сетевой анализ

Написание отчетов

Динамический анализ вредоносных программ

Воссоздание обстоятельств инцидента

Массовый анализ скомпрометированных систем

Навыки, которыми вы овладеете:

Анализ этапов процесса реагирования на инциденты

Реконструкция инцидентов

Сбор цифровых улик и грамотная работа с ними

Поиск следов вторжения

Расширьте ваши знания об активном поиске угроз и улучшите корпоративные стратегии реагирования на инциденты с помощью системы YARA.

Благодаря курсу вы сможете:

- Писать четкие и эффективные YARA-правила
- Использовать 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
- Проводить улучшенный поиск аномалий
- Проверять свои знания на реальных примерах, таких как атаки групп BlueTraveller и DiplomaticDuck

Узнайте о тонкостях расследования инцидентов на промышленных предприятиях

Основы расследования инцидентов в системах промышленной автоматизации

Исследование сети промышленного предприятия, поиск угроз, работа с сетевыми протоколами в АСУ ТП

Анализ систем архитектуры Intel X86/X64, включая специализированное ПО для систем промышленной автоматизации

Применение специальных инструментов и методов в промышленных системах

Цифровая криминалистика на специализированных устройствах систем промышленной автоматизации

Составление отчета о проведенном расследовании и подготовка рекомендаций

Изучите приемы и методы поиска уязвимостей для пресечения возможных кибератак на инфраструктуру предприятия

Обнаружение уязвимостей с помощью фаззинга

Изучение современных методов, техник, подходов и утилит, используемых для выявления уязвимостей в программном обеспечении методом фаззинга.

- Введение в техники фаззинга
- Написание собственного фаззера
- Практическое применение существующих инструментов, таких как Libfuzzer, AFL, DynamoRIO, WinAFL
- Проведение фаззинга как для исходного кода, так и для скомпилированных бинарных образов ПО
- Эмуляция для фаззинга других архитектур (ARM и MIPS)
- Эффективная генерация и мутация корпусов
- Анализ падений и их классификация

Поиск уязвимостей в устройствах IoT

Обучение специалистов по безопасности проведению полного и всестороннего исследования устройств интернета вещей (IoT) на уязвимости.

- Определение термина интернета вещей; приложения, архитектура IoT и примеры уязвимостей
- Аппаратные платформы и архитектура IoT, отладка устройств с использованием различных интерфейсов
- Угрозы и уязвимости в интернете вещей; векторы атак для различных уровней
- Получение и анализ прошивок
- Автоматизация задач реверс-инжиниринга
- Введение в динамический поиск уязвимостей
- Статистика по вредоносному ПО для устройств интернета вещей, ботнеты, анализ уязвимостей, защитные меры

Спасибо!