Программы тренингов «Лаборатории Касперского»

для специалистов по IT-безопасности

www.kaspersky.ru
#ИстиннаяБезопасность

Тренинги для специалистов по IT-безопасности

Количество и сложность угроз постоянно растет, и для успешной защиты от них требуются не только передовые решения, но и квалифицированные сотрудники. Тренинги «Лаборатории Касперского» помогут IT-профессионалам получить актуальные знания, расширить свою экспертизу и развить практические навыки в выбранных областях кибербезопасности.

Тренинги охватывают широкий спектр тем в области кибербезопасности, а также различных методик и практик, которые могут быть полезны как начинающим специалистам, так и опытным экспертам.

Все тренинги сочетают теоретическую и практическую часть. По завершении курса проводится оценка усвоенного участниками материала.

Тренинги проводятся на территории заказчика или в региональных офисах «Лаборатории Касперского».

Преимущества тренингов

Цифровая криминалистика и продвинутая цифровая криминалистика

Повысьте экспертизу ваших экспертов в области цифровой криминалистики и реагирования на инциденты. Задача тренингов – укрепить знания специалистов во всем, что касается поиска следов киберпреступления и анализа различных типов данных с целью установить источник и временные параметры атаки. После завершения тренинга участники смогут успешно проводить расследование компьютерных инцидентов, что повысит уровень безопасности компании в целом.

Анализ вредоносного ПО и обратная разработка (начальный и экспертный уровни)

Тренинг по обратной разработке поможет специалистам в области реагирования на инциденты успешнее проводить расследование вредоносных атак. Курс предназначен для сотрудников IT-департамента и системных администраторов. В ходе тренинга участники учатся анализировать вредоносное ПО, собирать индикаторы компрометации (IoCs), писать сигнатуры для обнаружения вредоносного ПО или зараженных машин, а также восстанавливать зараженные/зашифрованные файлы и документы.

Реагирование на инциденты

Тренинг поможет сотрудникам службы IT-безопасности больше узнать обо всех стадиях расследования инцидентов и даст все необходимые сведения для успешного самостоятельного устранения последствий инцидента.

YARA

Тренинг поможет узнать, как правильно писать, эффективно тестировать и улучшать правила YARA таким образом, чтобы с помощью них можно было успешно обнаруживать атаки.

Администрирование Kaspersky Anti Targeted Attack Platform

Тренинг по администрированию Kaspersky Anti Targeted Attack Platform (KATA) позволит узнать, как установить и настроить решение, а также как управлять им с максимальной эффективностью.

Анализ инцидентов Kaspersky Anti Targeted Attack Platform

Тренинг включает в себя множество упражнений, основанных на часто встречающихся на практике сценариях обнаружения угроз. Важную роль в них играет обработка уведомлений KATA – отслеживание, интерпретация, реагирование.

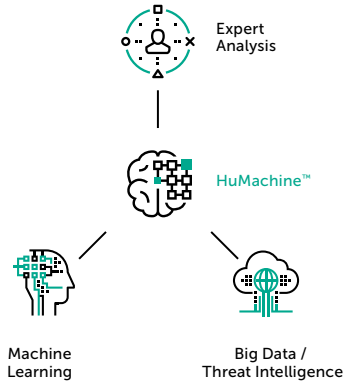
Успешный практический опыт

«Лаборатория Касперского» обладает обширным опытом обнаружения и исследования угроз. Эксперты компании – специалисты с мировым именем – обладают самой свежей, детальной и уникальной информацией о способах борьбы с кибератаками.

Темы	Продолжительность	Навыки
Цифровая криминалистика		
• Введение в цифровую криминалистику • Оперативное реагирование и сбор цифровых улик • Внутренняя структура реестра Windows • Анализ артефактов в Windows • Криминалистический анализ браузера • Анализ электронной почты	5 дней	• Организация лаборатории цифровой криминалистики • Сбор цифровых улик и порядок обращения с ними • Воссоздание хронологической картины инцидента с помощью временных меток • Выявление следов вторжения посредством анализа артефактов в ОС Windows • Анализ истории браузера и электронной почты • Эффективное применение средств и методов цифровой аналитики
Анализ и обратная разработка вредоносного ПО		
• Цели и методы анализа и обратной разработки вредоносного ПО • Внутреннее устройство ОС Windows, исполняемые файлы, ассемблер x86 • Базовые методы статического анализа (извлечение строк, анализ импортов, анализ точек входа исполняемого файла, автоматическая распаковка и т. д.) • Базовые методы динамического анализа (отладка, инструменты мониторинга, перехват трафика и т. д.) • Анализ файлов .NET, Visual Basic, Win64 • Методы анализа скриптов и программ, отличных от исполняемых файлов (пакетные файлы, Autolt, Python, JScript, JavaScript, VBS)	5 дней	• Построение безопасной среды для анализа вредоносных программ: развертывание «песочницы» и всех необходимых инструментов • Понимание принципов исполнения программ в ОС Windows • Распаковка, отладка и анализ вредоносного объекта, определение его функций • Обнаружение вредоносных сайтов путем анализа вредоносных скриптов • Проведение экспресс-анализа вредоносных программ
Цифровая криминалистика (экспертный уровень)		
• Экспертная криминалистика в ОС Windows • Восстановление данных • Сетевая и облачная криминалистика • Криминалистический анализ дампов памяти • Хронологический анализ • Практическая криминалистика реальных целевых атак	5 дней	• Глубокий анализ файловой системы • Восстановление удаленных файлов • Анализ сетевого трафика • Обнаружение вредоносной активности по дампам памяти • Восстановление хронологии инцидента

Темы	Продолжительность	Навыки
Анализ и обратная разработка вредоносного ПО (экспертный уровень)		
• Методы расширенного статического и динамического анализа (статический анализ шелл-кода, синтаксический анализ заголовка исполняемого файла, блоки переменных окружения потока (TEB) и окружения процесса (PEB), загрузка функций на основе различных алгоритмов хэширования) • Методы расширенного динамического анализа (структура исполняемого файла, ручная и экспертная распаковка, распаковка вредоносных архивов, содержащих полный исполняемый файл в зашифрованной форме) • Обратная разработка APT-угроз (полная проработка сценария APT-атаки, начиная с фишингового сообщения электронной почты и заканчивая как можно более глубоким анализом) • Анализ протоколов (анализ зашифрованных коммуникаций по протоколу C2, методы расшифровки трафика) • Анализ руткитов и буткитов (отладка загрузочного сектора при помощи IDA и VMware, отладка ядра при помощи двух виртуальных машин, анализ образцов руткитов)	5 дней	• Использование передовых методов обратной разработки и распознавание методов защиты от обратной разработки (обфускация, защита от отладки) • Расширенный анализ руткитов и буткитов • Анализ шелл-кода эксплойтов, внедренного в различные виды файлов, а также вредоносных программ для сред, отличных от Windows
Реагирование на инциденты		
• Общие сведения о реагировании на инциденты • Обнаружение и первичный анализ • Цифровой анализ • Создание правил обнаружения (YARA, Snort, Bro)	5 дней	• Отличие APT от других типов угроз • Понимание различных методов атаки и анатомии целевых атак • Применение специальных методов мониторинга и обнаружения • Выполнение процедуры реагирования на инциденты • Восстановление хронологической картины и логики инцидента • Создание правил обнаружения и подготовка отчетов
YARA		
• Введение в синтаксис правил YARA • Способы быстрого и эффективного создания правил • YARA-генераторы • Тестирование правил YARA на ложные срабатывания • Поиск новых необнаруженных образцов с помощью VirusTotal • Использование внешних модулей в YARA для эффективного поиска угроз • Поиск аномалий • Множество примеров из реальной практики • Набор упражнений для совершенствования навыков работы с YARA	2 дня	• Создание эффективных правил YARA • Тестирование правил YARA • Дальнейшее совершенствование правил для эффективного обнаружения угроз

Темы	Продолжи-тельность	Навыки
Администрирование KATA		
• Стандартная схема развертывания решения и размещения серверов • Системные требования • Модель лицензирования • Сервер «песочницы» • Консоль Central Node • Сенсоры • Интеграция с инфраструктурой • Установка сенсора на рабочих станциях • Добавление лицензии и обновление баз • Алгоритм работы решения	1 день	• Создание плана развертывания, оптимального для среды заказчика • Установка и настройка компонентов KATA • Поддержка и управление решением
Анализ инцидентов KATA		
• Интерпретация уведомлений (алертов) KATA • Объяснение технологий обнаружения и анализа • Объяснение механизмов скоринга и оценки риска	1 день	• Понимание того, как работает скоринг и как он используется механизмами оценки риска • Способность уверенно работать с уведомлениями KATA: отслеживать, интерпретировать, реагировать



www.kaspersky.ru

#ИстиннаяБезопасность