Укрепите первую линию кибероборонны

2022

Тренинг для IT-специалистов общего профиля

kaspersky

kaspersky.ru

Онлайн-курс по кибербезопасности для IT-специалистов (CITO)

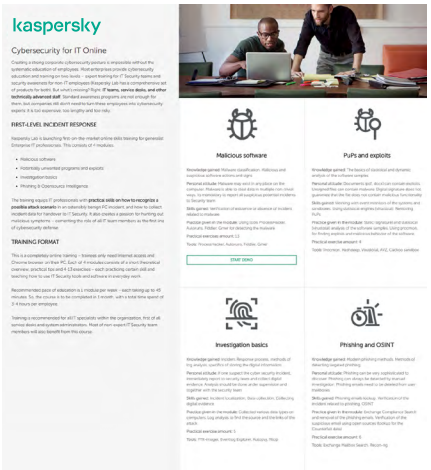
Интерактивный тренинг для IT-специалистов общего профиля, который поможет им вовремя распознать угрозы и стать первой линией кибероборонs вашей компании.

Систематическое повышение осведомленности всех сотрудников – важная часть обеспечения корпоративной безопасности. Большинство компаний обучают сотрудников на двух уровнях: повышают квалификацию сотрудников отдела IT-безопасности и учат основам кибербезопасности сотрудников, вообще не связанных с IT. Однако в этой картине не хватает важного элемента. А именно: эти тренинги не затрагивают IT-профессионалов общего профиля, службу IT-поддержки и других технических сотрудников. Стандартных программ осведомленности для них недостаточно, однако делать из технических специалистов полноценных экспертов по кибербезопасности за корпоративный счет слишком дорого, долго, рискованно – другими словами, не нужно.

Формат обучения

Тренинг проходит онлайн: нужны только доступ в интернет и браузер Chrome. Все модули состоят из короткой теоретической части, практических советов и 4-10 упражнений: каждое позволяет отработать определенный практический навык и учит использовать инструменты и защитное ПО в повседневной работе.

Текущая версия курса ориентирована на корпоративную среду на базе Windows



Первая линия кибероборонs

«Лаборатория Касперского» выпустила онлайн-курс для обучения корпоративных IT-специалистов общего направления. Курс состоит из четырех модулей:

- Вредоносное программное обеспечение
- Потенциально нежелательные программы и файлы
- Основы расследования инцидентов
- Реагирование на фишинг и разведка в открытых источниках

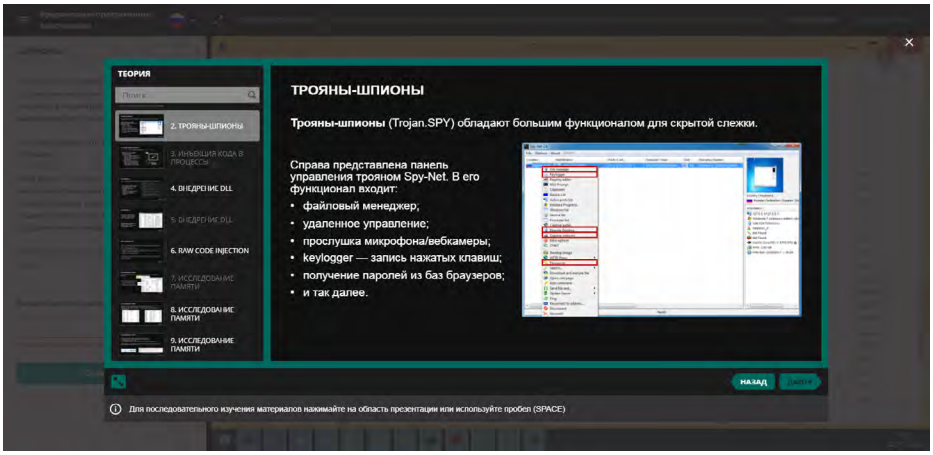
«Лаборатория Касперского» представляет программу обучения, предназначенную специально для IT-специалистов, которая учитывает их высокий уровень технической осведомленности и специфику их рабочих обязанностей.

Почему курс CITO эффективен?

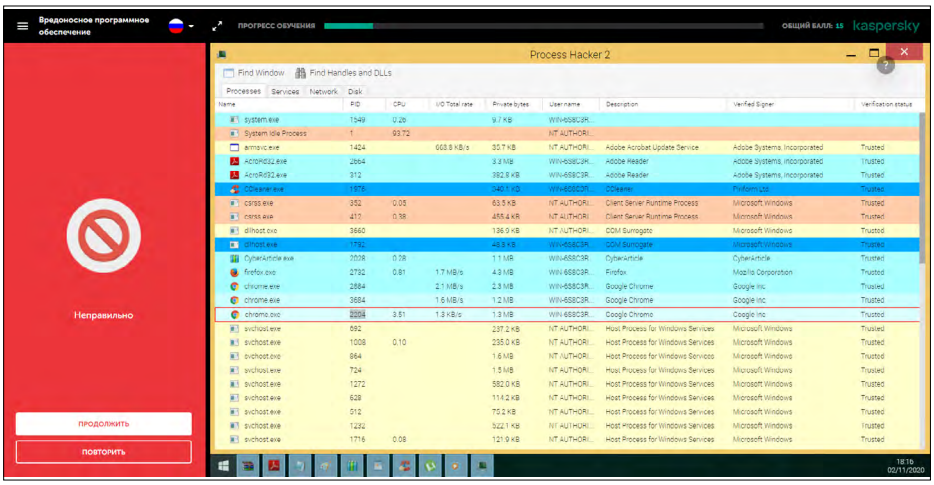
- Интерактивный формат: для участников моделируются реальные процессы, но без риска для безопасности компании
- Формирование не только знаний, но и навыков: большое внимание уделяется практике
- Интуитивный учебный процесс: удобная навигация и подсказки
- Охват основных вопросов и проблем кибербезопасности, с которыми IT-специалисты сталкиваются в своей работе
- Получение знаний онлайн: требуется только доступ к интернету или к корпоративной системе управления обучением (LMS), а также браузер Chrome

Как устроен процесс

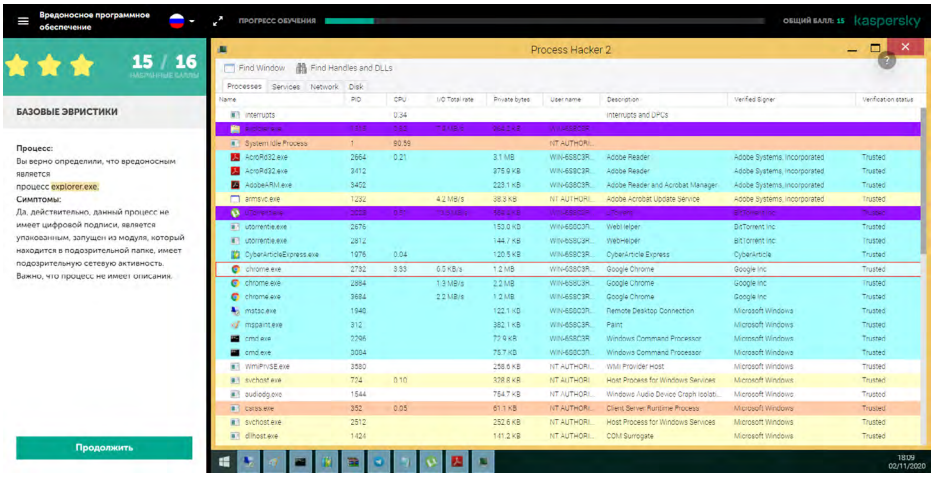
Каждый блок курса состоит из теоретической и практической части – моделирования реального процесса на основе теоретического материала.



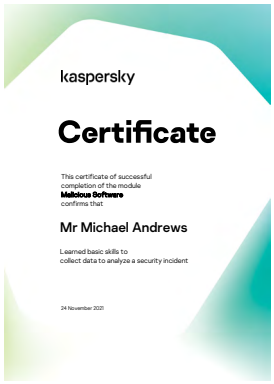
Если участнику не удается правильно выполнить задание, ему предлагают повторно пройти теоретическую часть.



Если задание выполнено успешно, участник переходит к следующему блоку с упражнением.



По завершению каждого модуля сотрудникам выдаются персональные сертификаты.


kaspersky

Certificate

This certificate of successful completion of the module **Malicious Software** confirms that

Mr Michael Andrews

Learned basic skills to collect data to analyze a security incident

24 November 2021

Кому будет полезно

Мы рекомендуем тренинг всем IT-специалистам в организации, в первую очередь работникам службы IT-поддержки и системным администраторам, но также он будет полезен и специалистам других отделов – в частности, всем, кто имеет права локального администратора на своей рабочей станции.

Результаты и тематика обучения

Название модуля	Основная целевая аудитория	Приобретенные знания	Формируемое отношение	Приобретенные навыки	Практические задания
Вредоносное программное обеспечение	Пользователи, обладающие правами администратора на рабочих станциях и (или) серверах	Методы и классификация вредоносного ПО Поведение и признаки, по которым можно обнаружить вредоносное ПО Основы эвристического анализа потенциально зараженной системы	Вредоносное ПО может существовать в любом компоненте компьютера Вредоносное ПО способно похищать данные многими способами, в том числе нестандартными Уведомление отдела ИБ обо всех подозрительных инцидентах также помогает решать проблемы и пользователя, и IT-департамента	Проверка наличия или отсутствия инцидентов, связанных с вредоносным ПО	Использование средств ProcessHacker для поиска подозрительных процессов на ПК и серверах
Потенциально нежелательные программы и файлы	Пользователи с правами на установку дополнительного ПО и пользователи, которые регулярно оценивают и открывают файлы, получаемые извне	Основы статического и динамического анализа образцов ПО и подозрительных документов	Документы (pdf, docx и др.) могут содержать эксплойты Неподписанные файлы могут содержать вредоносное или потенциально нежелательное ПО Все неподписанные файлы должны проходить проверку на наличие заражения Цифровая подпись не гарантирует, что у файла нет вредоносных функций	Работа с мониторами системных событий и песочницами Использование статистических сервисов по анализу файлов Удаление потенциально нежелательных программ	Статический и статистический (VirusTotal) анализ образцов ПО Использование procmon для выявления эксплойтов и вредоносного поведения ПО и сбора индикаторов компрометации Анализ файлов сиспользованием Cuckoo Sandbox Создание скриптов для удаления вредоносного ПО с помощью AVZ
Основы расследования инцидентов	IT-специалисты, задействованные в реагировании на инциденты безопасности или их расследовании под руководством отдела IT-безопасности	Процесс реагирования на инциденты Методы анализа журналов Особенности хранения цифровой информации	Если сотрудник подозревает инцидент кибербезопасности, необходимо немедленно сообщить об этом отделу ИБ и собрать цифровые улики Анализ необходимо проводить совместно с отделом ИБ и под их надзором	Сбор цифровых доказательств Анализ трафика netflow Хронологический анализ Анализ логов событий системы	Сбор энергозависимых и энергонезависимых данных (FTK-imager) Анализ журналов (логов) для поиска источника атаки и связанных с ней событий с помощью eventlogexplorer Анализ распространения атаки за счет анализа трафика netflow (ntop) Анализ диска с помощью Autopsy
Реагирование на фишинг и разведка в открытых источниках (OSINT)	IT-специалисты, задействованные в реагировании на инциденты безопасности или их расследовании	Современные методы фишинга Методы анализа заголовков электронных писем	Фишинг может быть очень искусно замаскирован. Фишинг можно выявить с помощью простых аналитических инструментов Фишинговые письма необходимо удалять из пользовательских почтовых ящиков	Анализ фишинговых писем и удаление замаскированных фишинговых писем из почтовых ящиков пользователей Анализ открытых источников с целью узнать, что злоумышленники знают о вашей компании	Exchange Mailbox Search и удаление фишинговых электронных писем Использование recon-ng для поиска информации в открытых источниках
Безопасность сервера	Администраторы сервера	Анализ сетевого окружения Усиление защиты сервера Анализ журналов PowerShell с целью обнаружения атак	Компрометация сетевого периметра – это один из основных векторов атак. Невозможно закрыть все уязвимости, однако, чтобы максимально усложнить атаку, необходимо уменьшить поверхность атаки. Даже если это не остановит злоумышленников, это даст вам время для обнаружения атаки.	Поиск уязвимых и нестандартных сетевых сервисов Настройка системы в соответствии с принципом «запрет по умолчанию» Поиск признаков атаки в журналах PowerShell	Использование Nmap для поиска уязвимых сетевых сервисов Настройка политик ограничения использования программ для управления программами и настройка брандмауэра Windows для контроля сети Анализ событий с помощью Event Log Explorer

Название модуля	Основная целевая аудитория	Приобретенные знания	Формируемое отношение	Приобретенные навыки	Практические задания
Безопасность Active Directory	Администраторы Active Directory	Использование API для проверки паролей по базе данных скомпрометированных паролей Настройка доменных политик в соответствии с рекомендациями Методы анализа безопасности доменов Active Directory	Установленные по умолчанию параметры конфигурации Active Directory не оптимальны с точки зрения безопасности Злоумышленники могут повысить свои привилегии разными способами Следует изучить рекомендации по безопасности и использовать инструменты, обеспечивающие лучшую видимость Active Directory	Безопасная проверка хэшей паролей по базе данных Поиск несоответствий между рекомендованными и фактическими доменными политиками Оценка уровня безопасности параметров Active Directory	Использование функции Have I Been Pwned? API для поиска по базе скомпрометированных паролей Использование анализатора политик для сравнения текущих доменных политик с рекомендованными Работа с отчетами Ping Castle

Связаться с нами

Демонстрацию, информацию о стоимости и доставке запрашивайте у менеджера или партнера «Лаборатории Касперского» в вашем регионе.

Kaspersky Security Awareness – системный подход к тренингам в сфере IT-безопасности

Ключевые особенности

Глубокие знания в области кибербезопасности
Более 20 лет опыта в этой сфере легли в основу наших курсов

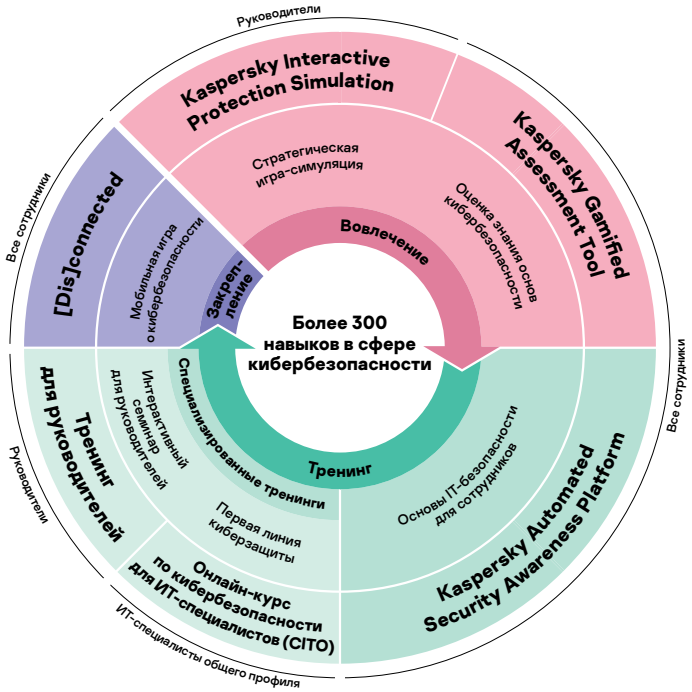
Навыки, которые меняют поведение сотрудников на всех уровнях организации
Игровой формат тренингов помогает заинтересовать и мотивировать сотрудников, а упражнения позволяют закреплять полученные навыки

Kaspersky Security Awareness предлагает ряд интересных и эффективных курсов для повышения осведомленности сотрудников и создания культуры кибербезопасности в организации. Поскольку для формирования устойчивых навыков безопасного поведения требуется время, наш подход подразумевает непрерывный и многокомпонентный цикл.

Разные форматы тренингов для разных уровней организации

Выберите один тренинг для решения конкретной задачи безопасности или приобретите пакет тренингов, который можно адаптировать под ваши потребности и приоритеты.

Подробная информация о пакетах тренингов на сайте: kaspersky.ru/awareness



www.kaspersky.ru

kaspersky АКТИВИРУЙ БУДУЩЕЕ