Обучение IT-специалистов навыкам поддержания кибербезопасности

Систематическое обучение сотрудников – важная часть обеспечения корпоративной безопасности. Большинство компаний внедряют обучение 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: обучение не затрагивает IT-профессионалов, 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.

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

Формат обучения

Обучение проходит онлайн: нужны только доступ в интернет и браузер Chrome. Все модули состоят из короткой теоретической части, практических советов и 7–10 упражнений: каждое позволяет отработать определенный практический навык и учит использовать инструменты и защитное ПО в повседневной работе.

Рекомендуемый темп: модуль в неделю, то есть около 45 минут. Таким образом, курс будет успешно завершен через 1,5 месяца, причем каждый сотрудник потратит на него 4–5 часов.

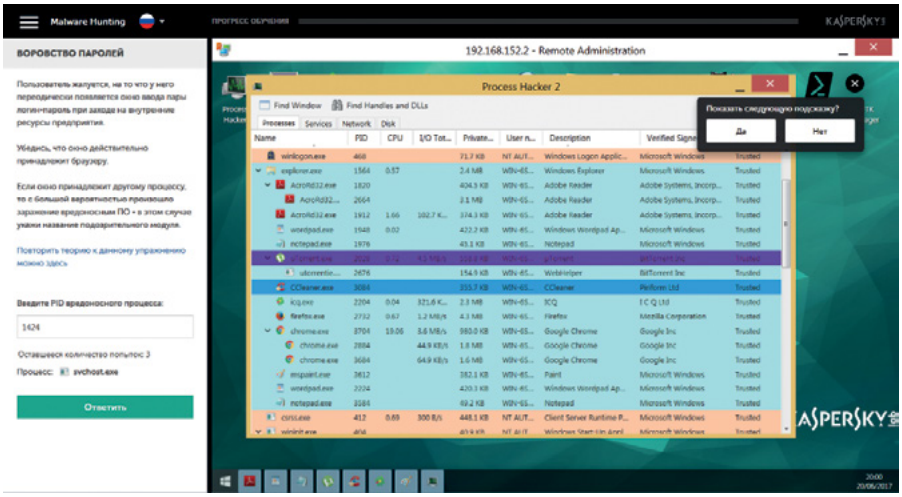
Мы рекомендуем обучение всем IT-специалистам в организации, в первую очередь работникам службы IT-поддержки и системным администраторам, но также он будет полезен и специалистам других отделов – в частности, всем, кто имеет права локального администратора на своей рабочей станции.

Первая линия кибероборонны

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

- Основные практические сведения о киберугрозах
- Вредоносное программное обеспечение
- Потенциально нежелательные программы и файлы
- Основы расследования инцидентов
- Реагирование на фишинг и разведка в открытых источниках
- Корпоративная безопасность: контроль уязвимостей и защита серверов

Этот курс дает IT-специалистам практические навыки по распознаванию возможной атаки при изучении безобидного на первый взгляд инцидента, а также навыки по сбору данных для передачи службе IT-безопасности. Также обучение мотивирует IT-специалистов искать и находить признаки кибератаки и помогает понять их задачи в качестве первой линии кибероборонны.



Результаты и тематика обучения

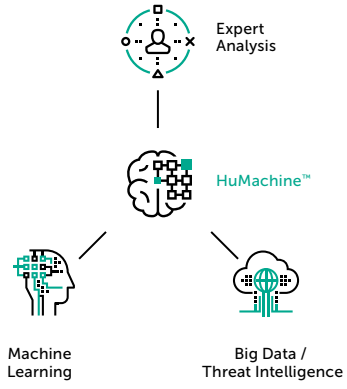
Название модуля	Основная целевая аудитория	Приобретенные знания	Формируемое отношение	Приобретенные навыки	Практические задания
Основные практические сведения о киберугрозах	Сотрудники, ответственные за получение, анализ и перенаправление IT-запросов (тикетов) от пользователей, в том числе в области безопасности	Типы и признаки киберугроз, методики и техники кибератак на предприятия	Атаки могут осуществляться с любого направления и в любой момент Стандартные процедуры по исполнению IT-запросов не всегда соответствуют стандартам техники кибербезопасности	Распознавание угроз по косвенным признакам	Использование средств ITIL наподобие Remedy для выявления признаков инцидента кибербезопасности
Вредоносное программное обеспечение	Пользователи, обладающие правами администратора на рабочих станциях и серверах	Классификация вредоносного ПО Поведение и признаки по которым можно обнаружить вредоносное и подозрительного 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 потенциальных инцидентах	Проверка наличия или отсутствия инцидентов, связанных с вредоносным ПО	Использование средств ProcessHacker, Autoruns, Fiddler, Gmer для обнаружения вредоносного ПО Создание индикаторов компрометации для поиска вредоносного ПО на других ПК
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	Документы (pdf, docx и др.) могут содержать эксплойты Неподписанные файлы могут содержать вредоносное ПО Цифровая подпись не гарантирует, что у файла нет вредоносных функций	Работа с мониторами событий (procmon) в системах и песочницах (cuckoo sandbox) Использование статистических сервисов по анализу файлов (VirusTotal) Удаление потенциально нежелательных программ и файлов (AVZ)	Статический (сигнатурный) и статистический (VirusTotal) анализ образцов ПО Использование procmon для выявления эксплойтов и вредоносного поведения ПО Проверка подозрительных исполняемых файлов на наличие вредоносного функционала

Название модуля	Основная целевая аудитория	Приобретенные знания	Формируемое отношение	Приобретенные навыки	Практические задания
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 свидетельства. Анализ необходимо проводить совместно с отделом ИБ и под их надзором	Локализация инцидента Сбор данных Сбор цифровых доказательств	Сбор данных разного типа с компьютеров Анализ журналов (логов) для поиска источника атаки и связанных с ней событий
Реагирование на фишинг и разведка в открытых источниках	Сотрудники, ответственные за получение, анализ и перенаправление IT-запросов (тикетов) от пользователей, в том числе в области безопасности Пользователи с правами на установку дополнительного ПО и пользователи, которые регулярно оценивают и открывают файлы, получаемые извне	Современные методы фишинга Методы обнаружения целенаправленного фишинга	Фишинг может быть очень искусно замаскирован Фишинг можно выявить с помощью простых аналитических инструментов Фишинговые письма необходимо удалять из пользовательских почтовых ящиков	Определение фишинговых писем Выявление инцидентов, связанных с фишингом Анализ открытых источников (OSINT)	Exchange Compliance Search и удаление фишинговых электронных писем Проверка подозрительных электронных писем с использованием открытых источников (поиск контрафактных данных)

Название модуля	Основная целевая аудитория	Приобретенные знания	Формируемое отношение	Приобретенные навыки	Практические задания
Корпоративная безопасность: контроль уязвимостей и защита серверов	IT-специалисты, задействованные в установке и администрировании внутренних или внешних серверов и систем	Методы оценки безопасности систем и серверов Многоуровневая безопасность Различное ПО для обеспечения безопасности	При отсутствии инструкций по настройке систем безопасности следует использовать многоуровневый подход Антивирус необходим всегда Атака должна быть невыгодной для злоумышленников: ее стоимость должна превышать ценность полученных данных	Проверка настроек безопасности при внедрении системы/сервера, полученных от коллег или поставщиков Проверка надежности паролей в системе Настройка мер безопасности для серверов Проверка уязвимостей и установка исправлений Управление установкой исправлений (патч-менеджмент)	Metasploit, hydra, ПО для конфигурации серверов, ПО для обеспечения безопасности, сканеры уязвимостей

Связаться с нами

По всем вопросам обращайтесь к вашему менеджеру «Лаборатории Касперского» или пишите на awareness@kaspersky.com



www.kaspersky.ru

#ИстиннаяБезопасность