kaspersky

Средний уровень

Реагирование на инциденты в Windows

Пройдите все этапы реагирования на инцидент на примере реального случая с программой-вымогателем

Благодаря этому тренингу вы сможете:

- Изучить способы выявления киберинцидентов и реагирования на них
- Отличать APT-угрозы от других типов угроз
- Проводить анализ пораженных машин в режиме реального времени
- Повысить качество создаваемых индикаторов компрометации (IoC)
- Изучить последовательность и содержание этапов реагирования на инциденты
- Изучить различные методы совершения атак и анатомию целевых атак на примере цепочки поражения
- Проводить анализ log-файлов с помощью регулярных выражений и ELK
- Освоить навыки криминалистического анализа сетевого трафика и памяти

Язык курса - Русский, Английский

Требования

- Базовые знания и общий опыт устранения неполадок в ОС Windows, знакомство с командами ОС Linux.

Для кого

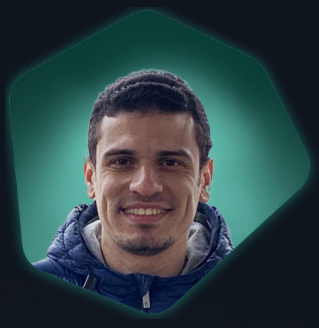
Организации, которые стремятся повысить квалификацию своих команд:

- SOC-центры
- Группы реагирования на инциденты
- Группы исследования угроз

Отдельные эксперты, которые хотят расширить свои компетенции в ИБ:

- Специалисты по реагированию на инциденты
- SOC-аналитики
- Исследователи киберугроз

Эксперты



Айман Шаабан

Руководитель группы цифровой криминалистики и реагирования на инциденты “Лаборатории Касперского”

Кай Шурихт

Эксперт кибербезопасности

Программа курса

1 Введение

- Триада CIA
- Ландшафт киберугроз
- APT-атаки и модель цепочки поражения
- Основные термины и определения

2 Процесс реагирования на инциденты

- Шесть этапов процесса реагирования на инциденты
- Разработка плана реагирования на инциденты

3 Обнаружение инцидентов: сетевой и системный уровни

- Обнаружение инцидента и его проверка
- Проверка и анализ инцидентов на атакованных машинах в режиме реального времени (с использованием различных подходов: IRCD и PowerShell)

4 Сбор улик

- Сбор цифровых улик с соблюдением требований криминалистики и сохранением их целостности
- Разница между созданием полного криминалистического образа и выборочным сбором данных
- Выборочный сбор данных с помощью FTK-Imager и Velociraptor

5 Анализ памяти

- Анализ памяти с помощью платформы Volatility
- Полный криминалистический анализ памяти с целью извлечения важной для расследования информации

6 Анализ лог-файлов

- Стек ELK для анализа лог-файлов
- Анализ лог-файлов с помощью командной строки Linux, программы LogParser и инструмента Windows PowerShell

7 Анализ сети

- Создание дампа сетевого трафика для анализа
- Создание правил Suricata для обнаружения угроз на уровне сети
- Анализ сети с помощью Wireshark

8 Аналитика киберугроз (CTI)

- Индикатор компрометации (IOC)
- Роль поиска IOC в процессе реагирования на инциденты
- Цикл поиска IOC
- Создание правил YARA для обнаружения вредоносных файлов в рамках практического примера

Связаться с нами:

support@kaspersky.happydesk.ru

www.kaspersky.ru