Компьютерная криминалистика

Цель программы — сформировать у слушателей целостное представление о криминалистическом анализе данных, а также научить техникам и инструментам, необходимым для проведения криминалистических исследований.

Выпускники курса получают свидетельство о повышении квалификации государственного образца, именной сертификат ООО «Ф.А.К.К.Т.».

Целевая аудитория:

- руководители и специалисты отделов информационной безопасности;
- команды специалистов по реагированию на инциденты информационной безопасности;
- руководители и специалисты центров по реагированию (CERT);
- специалисты по тестам на проникновение, компьютерные криминалисты и эксперты;
- технические специалисты всех наименований и категорий, обеспечивающие кибербезопасность.

Форма обучения – очная (дневная).
Стоимость обучения одного слушателя – 3500 рублей.

Продолжительность программы – 40 академических часов.

Учебный план курса

№ п/п	Название тем курса
	Первичное реагирование
1.	Обзор ключевых трендов киберпреступлений
2.	Введение в криминалистику. Процесс сбора первоначальных данных
3.	Типы криминалистических копий, способы создания копий диска. Сбор доказательной базы и ее оформление/хранение
4.	Основы проведения криминалистического исследования. Базовые инструменты для анализа
5.	Анализ атак
6.	Маппинг данных из отчета на матрицу MITRE ATT&CK
	Компьютерная криминалистика систем под управлением ОС Windows
7.	Подготовка источников доказательств. Особенности файловой системы NTFS
8.	Восстановление данных. Сбор информации о системе. Просмотр таймлайна. Первичный анализ основных источников данных
9.	Поиск следов первичной компрометации. Анализ RDP-подключений, способов фишинга, просмотр использования USB-устройств. Изучение следов открытия файлов
10.	Анализ следов запуска на скомпрометированном хосте с помощью ключа UserAssist. Исследование prefetch-файлов, ShimCache, MUICache и AmCache

11.	Анализ следов закрепления в системе с помощью ключей запуска и планировщика заданий. Изучение WMI Event Subscription
12.	Исследование следов закрепления по сети. Изучение журналов событий, реестра, следов работы psexec
13.	Практические занятия с исследованием скомпрометированного хоста
	Криминалистика оперативной памяти
14.	Принцип работы оперативной памяти, межпроцессный обмен данными и внедрение вредоносного кода в процессы
15.	Live-анализ оперативной памяти для выявления признаков компрометации системы
16.	Создание дампов оперативной памяти и специфика их анализа посредством volatility, Rekall, Redline
17.	Исследование файлов гибернации и подкачки на предмет поиска криминалистических артефактов
18.	Алгоритм выявления аномалий и вредоносной активности в оперативной памяти
19.	Практические занятия на восстановление хронологии атак на основе дампов оперативной памяти
	Сетевая криминалистика
20.	Общие сведения о сетях и сетевом взаимодействии
21.	Основные принципы проведения сетевой криминалистики. Регламент действий сотрудников с целью получения максимально подробной информации для проведения анализа
22.	Типовые источники данных для проведения сетевой криминалистики и их исследование
23.	Особенности инструментария для создания дампа сетевого трафика
24.	Анализ трафика с помощью ПО Wireshark, Sguil, Xplico, Squer, SecurityOnion и др.
25.	OSINT
26.	Практические занятия по анализу вредоносного трафика, зашифрованного трафика и выявление аномальной активности
	Итоговое исследование
27.	Криминалистическое исследование дампа оперативной памяти
28.	Криминалистическое исследование триажа скомпрометированного хоста
29.	Разбор результатов самостоятельной работы