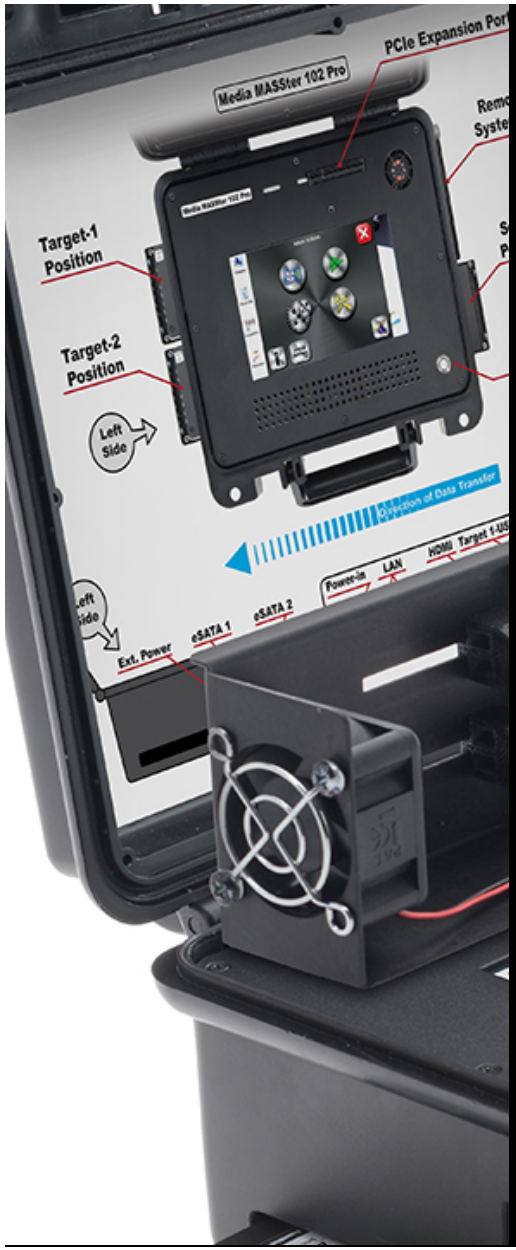
CROSSTECH
SOLUTIONS GROUP

Криминалистика как бизнес процесс компании

Ильяс Киреев



CROSSTECH SOLUTIONS GROUP

Компьютерная криминалистика

Источник: https://ics-iq.com/media-masster-102-pro-forensic/

CROSSTECH
SOLUTIONS GROUP

Криминалистика

Классификация

- **Computer forensics**
- **Network forensics**
- **Forensic data analysis**
- **Mobile device forensics**
- **Hardware forensic**

Инцидент менеджмент

Выявление

- Активы
- События ИБ
- Инциденты ИБ
- Анализ
- Классификация

Реагирование

- Ответственные
- ГРИБ
- Контроль

Расследование

- Источники
- Причины
- Следствие

Пост анализ

- Первичный сбор
- Анализ цифровых улик
- Создание отчетов

CROSSTECH
SOLUTIONS GROUP

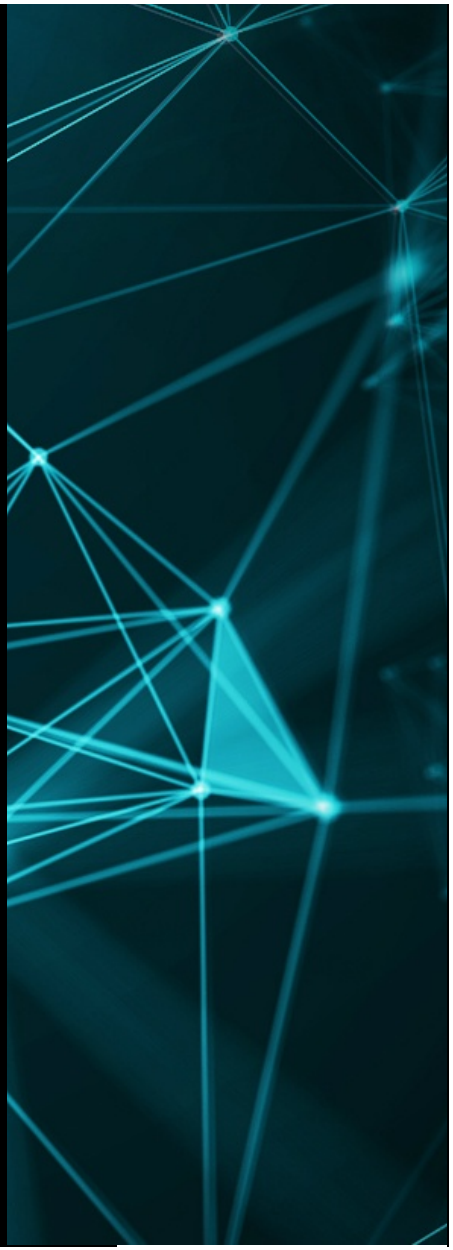
Пост анализ

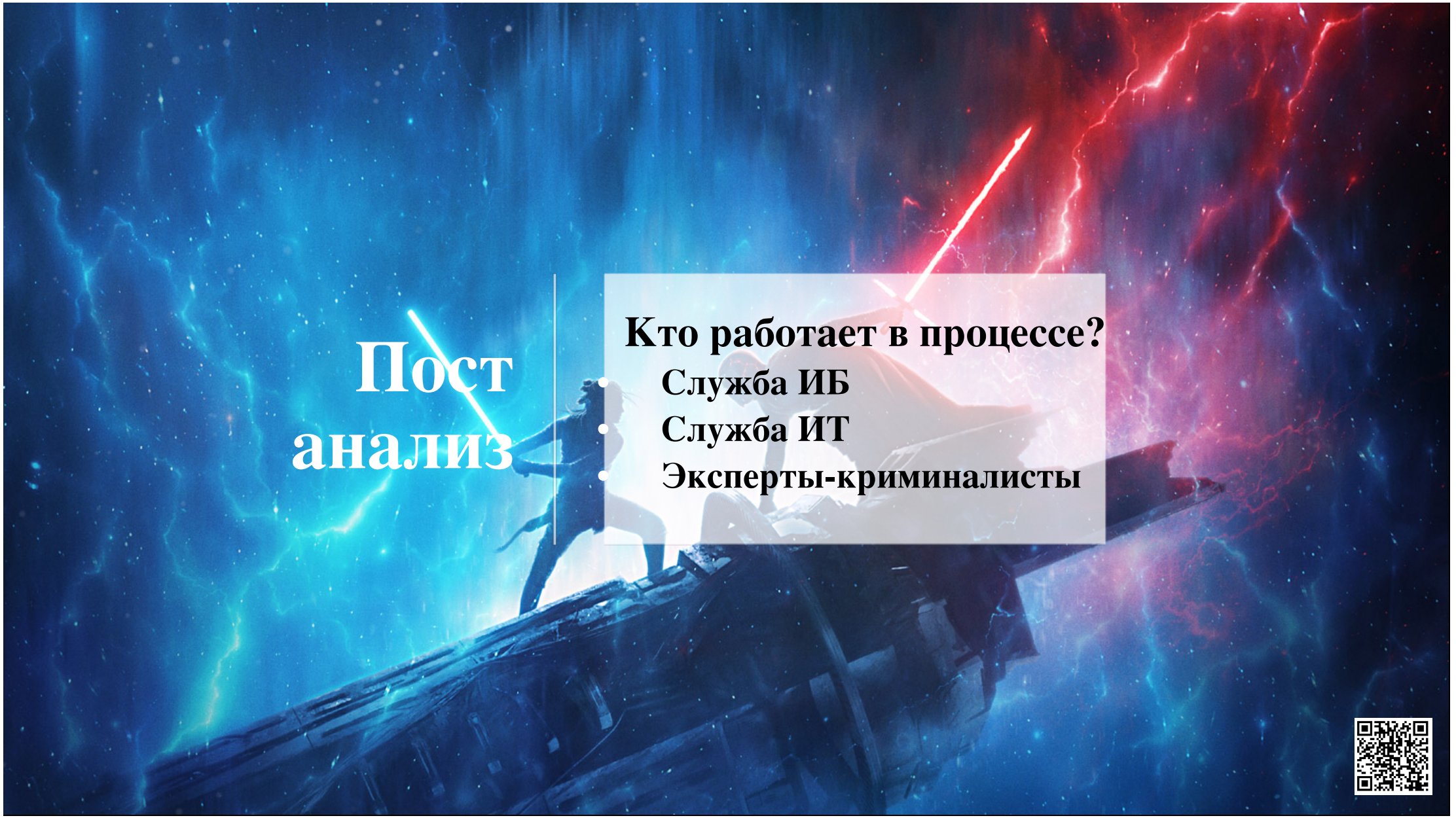
Детальные компьютерные расследования инцидентов информационной безопасности

CROSSTECH
SOLUTIONS GROUP

Процессы

- Сбор
- Анализ
- Рассмотрение
- Управление



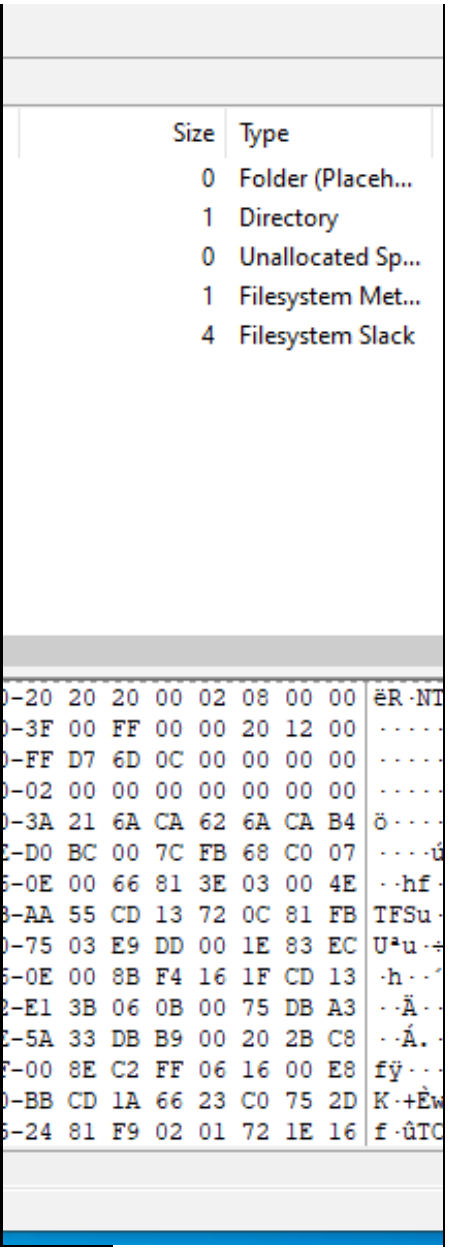

Пост
анализ
Кто работает в процессе?
Служба ИБ
Служба ИТ
Эксперты-криминалисты

CROSSTECH
SOLUTIONS GROUP

ACCESSDATA

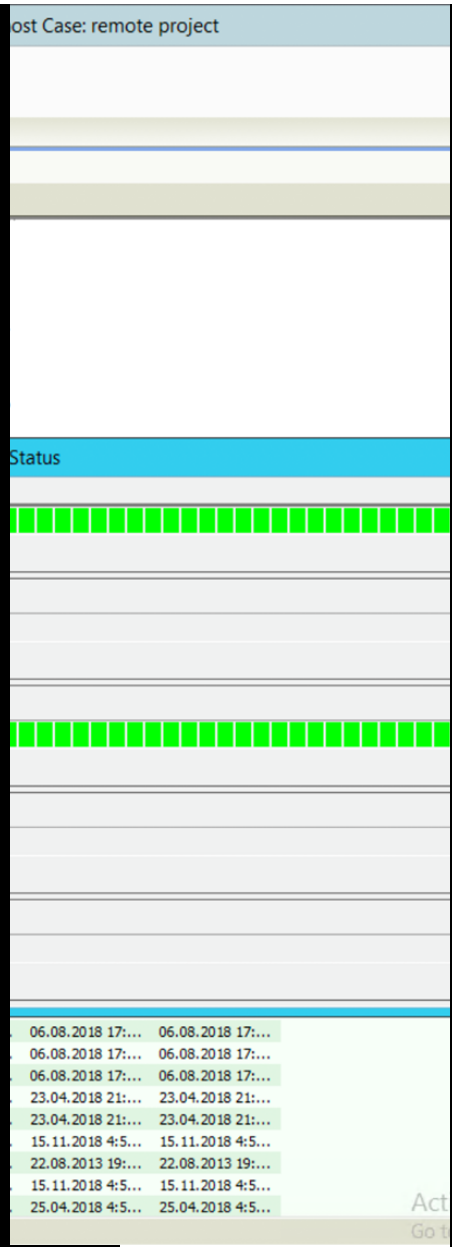
Скачать бесплатно

https://accessdata.com/product-download/ftk-imager-version-4-3-0



CROSSTECH
SOLUTIONS GROUP

Централизованный удаленный сбор



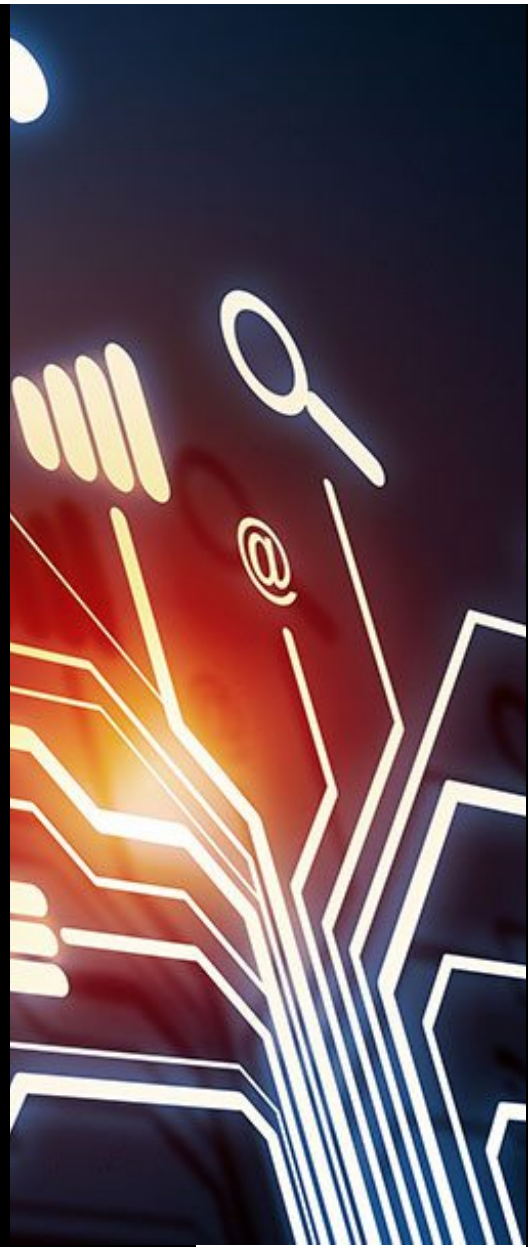
CROSSTECH
SOLUTIONS GROUP

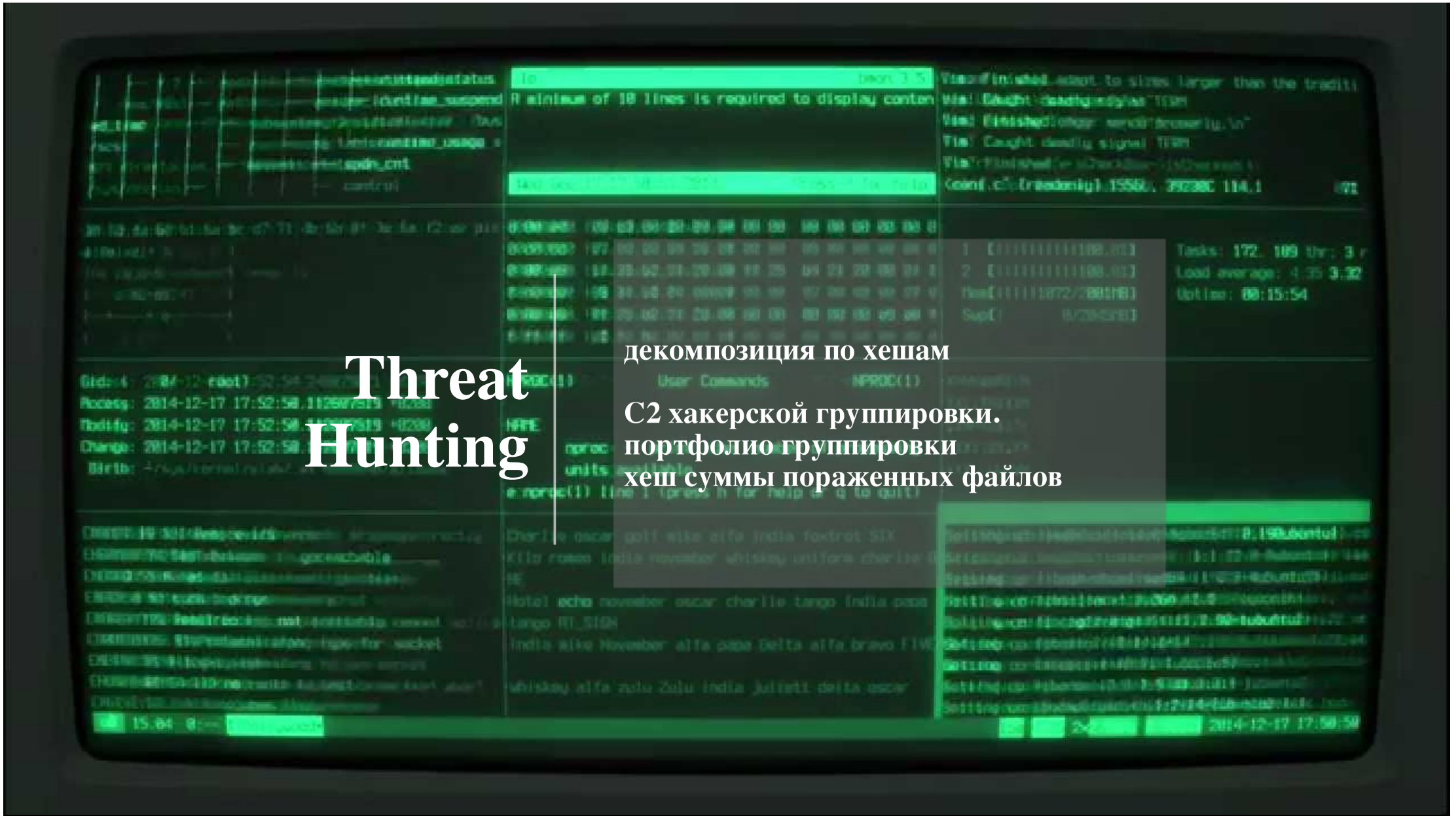
Объекты сбора и анализа

CROSSTECH
SOLUTIONS GROUP

- почтовые сервера
- базы данных
- файловые хранилища
- криминалистический образ

eDiscovery




Threat Hunting
декомпозиция по хешам
C2 хакерской группировки.
портфолио группировки
хеш суммы пораженных файлов

IOCs

MD5	SHA-1	SHA-256
SkinnyD		
ec2377cbd3065b4d751a791a22bd302c	cdd78ccd274705f6c94b6640c968e90972597865	1d59968304
3fff50f9ea582848b8a5db05c88f526e	ea11d0d950481676282cee20c5eb24fc71878bcc	b5227a1218
55186de70b2d5587625749a12df8b607	858d866c5faa965fa9fbe41c8484a88fe0c612eb	d81ba465fe
Бэкдор xDll		
9f01cb61f342f599a013c3e19d359ab4	b63bfdfb7f267e9fbf1c19be65093d857696f3b0	169c24f0ad
a2d552ed07ad15427f36d23da0f3a5d3	1858a80c8cff38d7871286a437c502233e027ab0	59759bbdfc
60ddb540da1aefee1e14f12578eafda8	8d16bc28cef6760ecf69543a14d29ba041307957	87a57f5bb9
7a4c8e876af7d30206b851c01dbda734	4cff1af90c69cc123ecafe8081e3c486a890d500	06d20fb589
3d760b6fc84571c928bed835863fc302	adcf9ade7a4dc14b7bf656e86ea15766b843e3b6	8ac21275d0

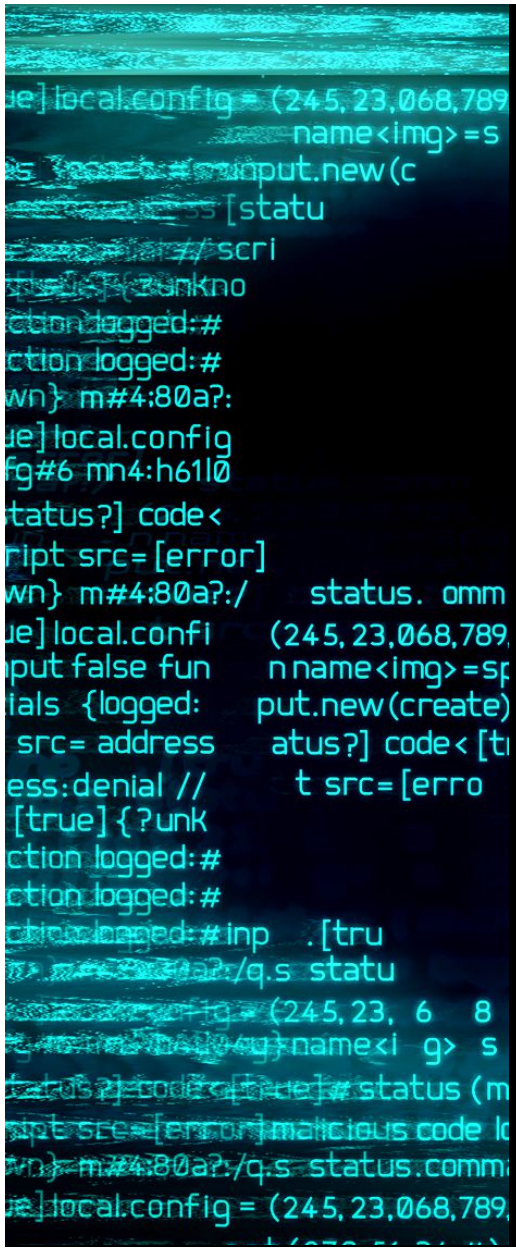
Добавление кейса и задачи на сканирование шары по хешу

Поиск по индексу целевого хеша и название файла

Добавление списка хешей IoC в формате CSV

Настройка профиля KFF

Настройка планировщика задач поиска



CROSSTECH
SOLUTIONS GROUP

eDiscovery processing

Вирусное заражение

CROSSTECH
SOLUTIONS GROUP

Автоматизация инцидент менеджмента

- Улучшает реакцию команды SOC до 40 минут
- Исключает ошибки человека
- Автоматизирует сбор цифровых артефактов
- Изоляция хоста на стадии закрепления
- Интеграция с TI платформами

CROSSTECH
SOLUTIONS GROUP

Вопросы?

CROSSTECH
SOLUTIONS GROUP