Cross Technologies

Шамовка Андрей
Руководитель службы поддержки продуктов

ПРЕДПОСЫЛКИ

Глобальная цифровизация, растущие объемы данных, множество форматов:

1996 – 10 MB
1999 – IBM the Microdrive 170 MB и 340 MB
2002 – 137 GB addressing space barrier broken
2005 – 500 GB hard drive
2007 – 1 terabyte hard drive
2009 – 2 terabyte hard drive
2011 – 4 terabyte hard drive
2013 – 5 terabyte hard drive
2015 – 10 terabyte hard drive
2018 - 16TB Samsung, 60 terabyte SSD Seagate

Cross Technologies

ACCESSDATA®

ЧАСТНАЯ ПРОБЛЕМАТИКА

Инциденты требующие расследования внутри компании

Задержки по разбору инцидентов, криминалистическому анализу, в случае привлечения к расследованию сторонних подрядчиков

Связанные с привлечением сторонних подрядчиков финансовые издержки

Сокращение времени реагирования на инцидент и его расследования

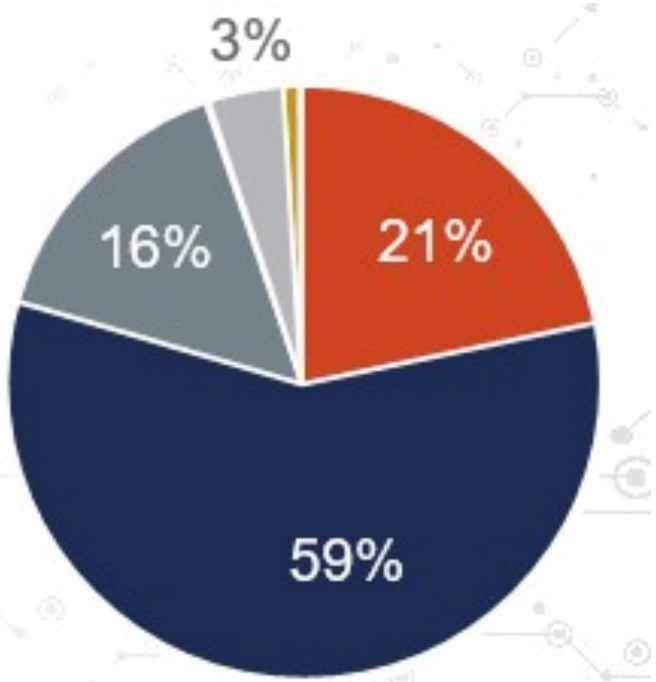
Cross Technologies

ACCESSDATA®

ЧАСТНАЯ ПРОБЛЕМАТИКА

Уровень важности сотрудничества между HR, IT и специалистами по криминалистике для успеха расследования инцидентов

- Критичный
- Высокий
- Средний
- Низкий
- Нулевой



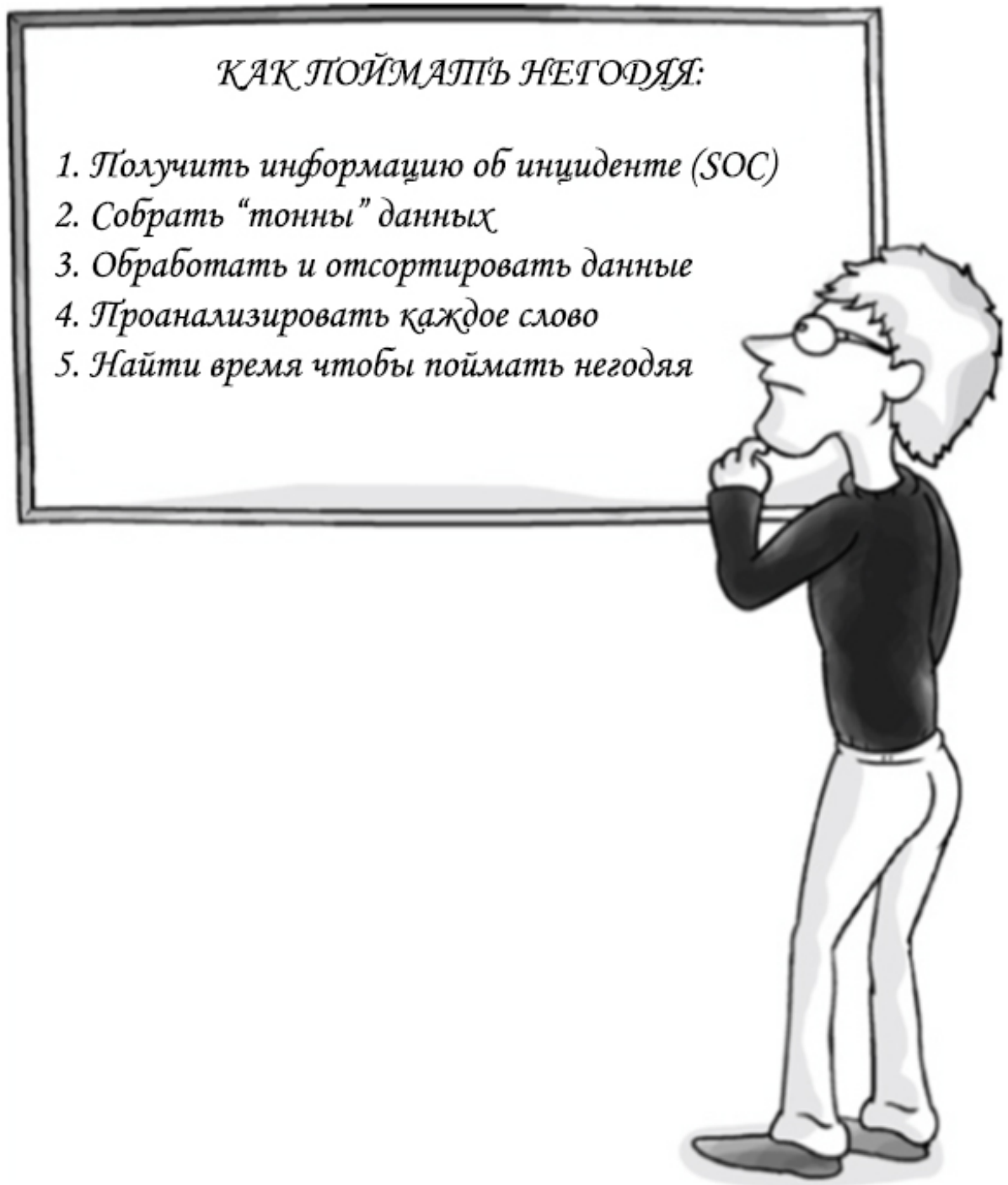
Cross Technologies

ACCESSDATA®

ОБЩАЯ ПРОБЛЕМАТИКА

Cross Technologies

ACCESSDATA®


КАК ПОЙМАТЬ НЕГОДЯЯ:
1. Получить информацию об инциденте (SOC)
2. Собрать “тонны” данных
3. Обработать и отсортировать данные
4. Проанализировать каждое слово
5. Найти время чтобы поймать негодяя

КОНЦЕПЦИЯ

Cross Technologies

ACCESSDATA®

ПОДХОД

- Удаленное управление, скрытые расследования
- Проведение пост-анализа инцидента в конечной точке
- Все необходимые инструменты в одном продукте

Cross Technologies

ACCESSDATA®

РЕШЕНИЯ

Каждая компания должна **собирать данные в криминалистически (юридически) значимой форме**.

Какое решение вам требуется – зависит от того, как вы планируете собирать и анализировать информацию.

FTK®

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ

- 1:1 расследования
- Ядро AccessData
- Быстрая обработка данных
- Интеграция с Belkasoft

AD Enterprise

РАССЛЕДОВАНИЯ В СЕТИ & ПОСТ-АНАЛИЗ ИНЦИДЕНТОВ

Корпоративные расследования

Предварительный просмотр данных в конечной точке в реальном времени

Анализ оперативной памяти Агентская инфраструктура

Удаленная работа, скрытые расследования

Восстановление удаленных файлов и т.д..

AD eDiscovery®

РЕГУЛЯРНЫЙ ЗАЩИЩЕННЫЙ СБОР ДАННЫХ

- Для крупномасштабных расследований
- Сбор данных через коннекторы к наиболее используемым хранилищам
- Встраивание в EDRM
- Визуализация и аналитики для интерпретации данных
- Интеграция с Brainspace

QUIN-C

НОВОЕ ПОКОЛЕНИЕ КРИМИНАЛИСТИКИ

- Повышение эффективности и пропускной способности
- Поиск и анализ ключевых данных и получение комплексных результатов
- Меньшее время расследования

Cross Technologies

ACCESSDATA®

ПРЕИМУЩЕСТВА

Never touch your data again!

Отсутствие влияния на бизнес-процессы (удаленный сбор, разделение задач: безопасности свое – аналитикам и юристам свое)

Снижение рисков

Снижение издержек на сбор и анализ доказательств

Cross Technologies

ACCESSDATA®

BEST PRACTICE

Автоматизация процесса сбора данных – скорость сбора, корректность, отсутствие зависимости от квалификации IT-специалиста

Унификация форматов и процессов сбора, хранения и обработки Данных

Подтвержденная целостность собранных данных (включая трекинг процесса сбора)

Придание юридической значимости собранным доказательствам
Возможность использования следственными органами инструментов, которые работают с форматами AD1, EO1

БОЛЕЕ 130000 КЛИЕНТОВ ПО ВСЕМУ МИРУ

Cross Technologies

ACCESSDATA®

БЛАГОДАРИМ ЗА ВНИМАНИЕ!