ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ:

где начинается

Оксиджен
софтвер

ОЛЬГА ГУТМАН

Генеральный директор
ООО «Оксиджен Софтвер»

Оксиджен
софтвер

22 ГОДА

НА РЫНКЕ ЦИФРОВОЙ КРИМИНАЛИСТИКИ
И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

DLP

SIEM

SOAR

DFIR

и другие

DLP

SIEM

SOAR

DFIR

DATA LEAK PREVENTION

Системы предотвращения утечек информации

DLP-системы обеспечивают возможность **блокировать несанкционированную обработку информации**, позволяют значительно **снизить риск утечки информации** и, как следствие, **уменьшить ущерб** от такого инцидента.

DLP-системы строятся на анализе потоков данных, пересекающих периметр информационной системы компании. При обнаружении в этом потоке конфиденциальной информации срабатывает триггер и передача сообщения блокируется.

DLP

SIEM

SOAR

DFIR

SECURITY INFORMATION AND EVENT MANAGEMENT

Системы управления событиями и информацией о безопасности

SIEM-системы собирают и обрабатывают данные, а также оповещают оператора о возможной опасности.

В задачи SIEM-систем входит:

- В реальном времени отслеживать сигналы тревоги, поступающие от сетевых устройств и приложений.
- Обрабатывать полученные данные и находить взаимосвязи между ними.
- Выявлять отклонения от нормального поведения контролируемых систем.
- Оповещать операторов об обнаруженных инцидентах.

DLP

SIEM

SOAR

DFIR

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE

Системы для координации и управления безопасностью

Продукты класса **SOAR объединяют защитные решения в единую систему**, избавляя специалистов по безопасности от необходимости управлять каждым из них в отдельности.

В то время как SIEM-решения нацелены на сбор информации и ручное управление инцидентами, **SOAR-системы рассчитаны на автоматизацию** и оркестровку работы нескольких различных систем информационной безопасности, в частности, на этапе реагирования.

DLP

SIEM

SOAR

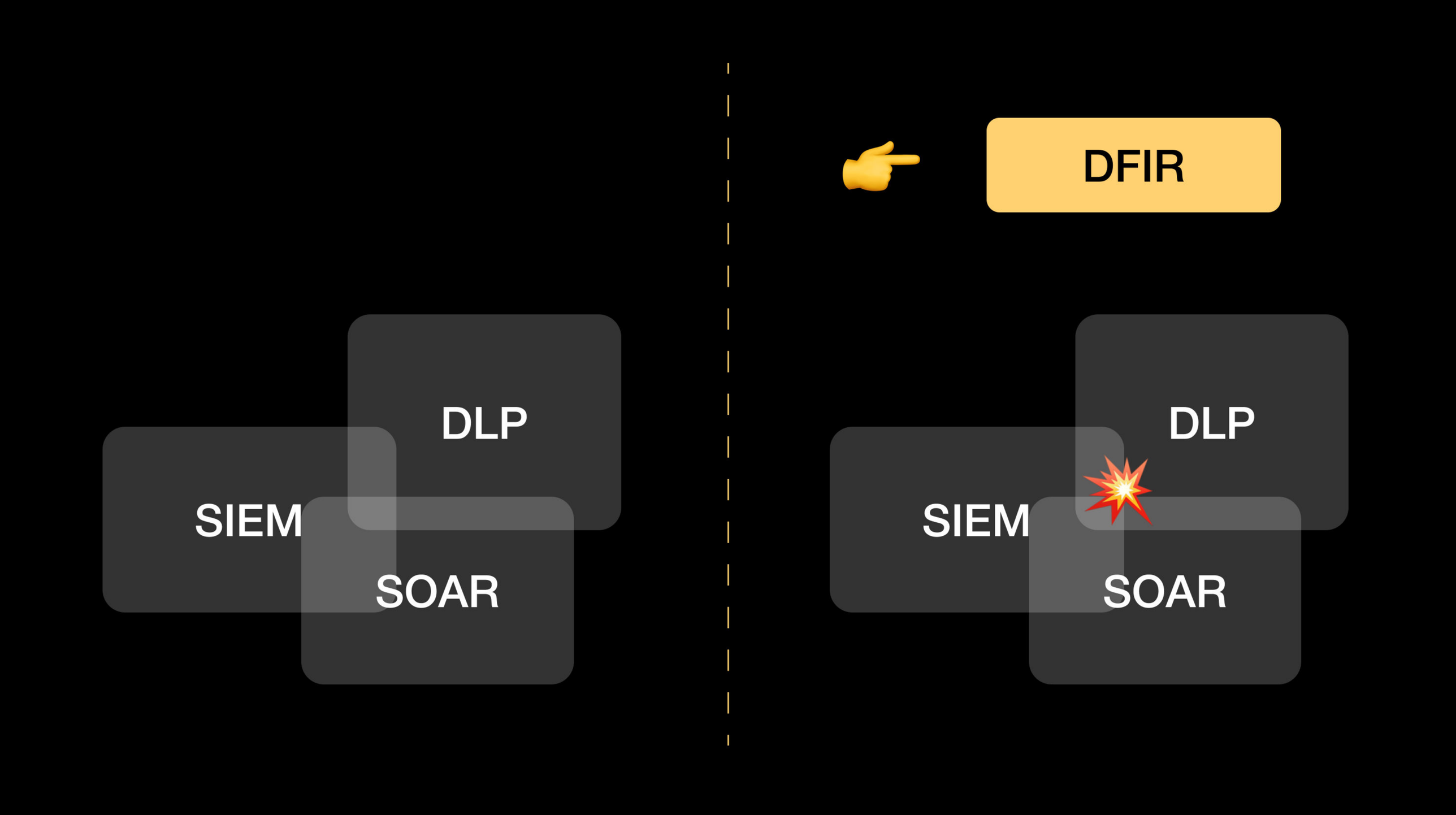
DFIR

DIGITAL FORENSICS AND INCIDENT RESPONSE

Расследование инцидентов в сфере информационной безопасности

Цель DFIR — создать полную, прозрачную и достоверную картину инцидента и ответить на такие вопросы, как:

- Кто стал «нулевым пациентом»?
- Каковы последствия и полный масштаб атаки?
- Какие шаги предприняли злоумышленники, находясь в периметре?
- Как нам реагировать на инцидент и нивелировать последствия?


DLP
SIEM
SOAR
DFIR
DLP
SIEM
SOAR

ПРОГРАММНОЕ
ОБЕСПЕЧЕНИЕ КЛАССА

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

DFIR

необходим тем, кто хочет защититься от:

- шифровальщиков
- утечек конфиденциальной информации
- противоправных инсайдерских действий
- атак вредоносного ПО
- промышленного шпионажа и т.д.

DFIR

позволяет:

- найти виновного
- найти уязвимость, которая позволила инциденту произойти
- определить масштаб инцидента
- получить информацию для предотвращения подобных инцидентов в будущем

DFIR

- извлекает данные из устройств, в т.ч. удаленные данные
- анализирует извлеченные данные
- позволяет восстановить хронологию событий

DFIR

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ТИПЫ КЕЙСОВ

- ВРЕДОНОСНОЕ ПО
- ШИФРОВАЛЬЩИКИ
- ФИШИНГ
- ИНСАЙДЕРСТВО
- НЕЦЕЛЕВОЕ ИСПОЛЬЗОВАНИЕ АКТИВОВ
- НАРУШЕНИЕ ВНУТРЕННЕЙ ПОЛИТИКИ
- МОШЕННИЧЕСТВО
- ПРОГРАММЫ-ВЫМОГАТЕЛИ
- УВОЛЬНЕНИЕ СОТРУДНИКА
- ЗАПРЕЩЕННЫЕ ПРИЛОЖЕНИЯ
- ХАРАССМЕНТ

и другое

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ИНСАЙДЕРСТВО

- Потеря клиентов на финальном этапе переговоров
- Конкурент предлагает клиентам более выгодные условия
- Предположительный “слив” информации

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

РЕШЕНИЕ КЕЙСА

- Поиск и сбор данных
- Идентификация подозреваемых
- Анализ рабочих станций подозреваемых
- Определение методов организации утечки
- Определение реального масштаба инцидента
- Разработка мер по устранению последствий внутри сети и предотвращению схожих инцидентов

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ЗАДАЧИ

ПРОВЕДЕНИЕ РАССЛЕДОВАНИЙ

ПОИСК ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ НА КОНЕЧНЫХ ТОЧКАХ СЕТИ

ОПТИМИЗАЦИЯ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ПРОВЕДЕНИЕ РАССЛЕДОВАНИЙ

- Выявление источников утечки конфиденциальных данных
- Отслеживание последовательности действий вируса на рабочей станции
- Обнаружение попыток несанкционированного доступа
- Определение пути движения документов внутри компании
- Выявление неправомерных действий сотрудников

и другое

DFIR

ПОИСК ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ НА КОНЕЧНЫХ ТОЧКАХ СЕТИ ОРГАНИЗАЦИИ, НАПРИМЕР:

- Обнаружениие внесения несанкционированных изменений в бухгалтерские документы и идентификация их автора
- Выявление факта подмены документов
- Подробное содержание email’ов и переписки в мессенджерах
- Скачивание данных на флешку
- Неправомерный доступ к грифованным документам
- Переход по неверифицированным ссылкам
- Скачивание несанкционированных файлов

и другое

DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR
DFIR

ОПТИМИЗАЦИЯ ПРОЦЕССА РЕАГИРОВАНИЯ НА ИНЦИДЕНТ:

- Извлечение данных из устройств и сервисов
- Анализ извлеченной информации
- Демонстрация коммуникаций владельцев устройств
- Выстраивание хронологии инцидента
- Поиск информации по извлеченным данным
- Хранение всех данных в одном месте

и другое

R DFIR **DFIR** DFIR DFIR DFIR DFIR DFIR DFIR DFIR DFIR D

R DFIR **DFIR** DFIR DFIR DFIR DFIR DFIR DFIR DFIR DFIR D

ВКЛЮЧЕНЫ В РЕЕСТР РОССИЙСКОГО ПО

MK ENTERPRISE

АНАЛИТИЧЕСКИЙ ЦЕНТР

MK ENTERPRISE

- Дистанционное исследование рабочих станций на Windows, MacOS, Linux
- Исследование группы рабочих станций Windows
- Извлечение данных из устройств на базе Android и iOS
- Получение доступа к информации в облачных хранилищах
- Анализ коммуникаций владельца устройства или учетной записи
- Построение полной хронологии инцидента
- Изучение полной файловой базы объекта исследования
- Поиск данных внутри извлечения по заданным параметрам

и многое другое

АНАЛИТИЧЕСКИЙ ЦЕНТР

АНАЛИТИЧЕСКИЙ
ЦЕНТР

- Серверное хранение базы извлечений с гибкой настройкой ролей и прав доступа
- Одновременный доступ к полной базе загруженных извлечений для всех сотрудников
- Анализ больших объемов данных с использованием передовых аналитических инструментов и фильтров
- Поиск данных по всей базе
- Перекрестный анализ данных между несколькими инцидентами
- Экспорт полученных результатов в отчеты разных форматов

и многое другое

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

СПАСИБО

КОНТАКТЫ:

+7 (495) 909-92-78

sales@oxygensoftware.ru

oxygensoftware.ru