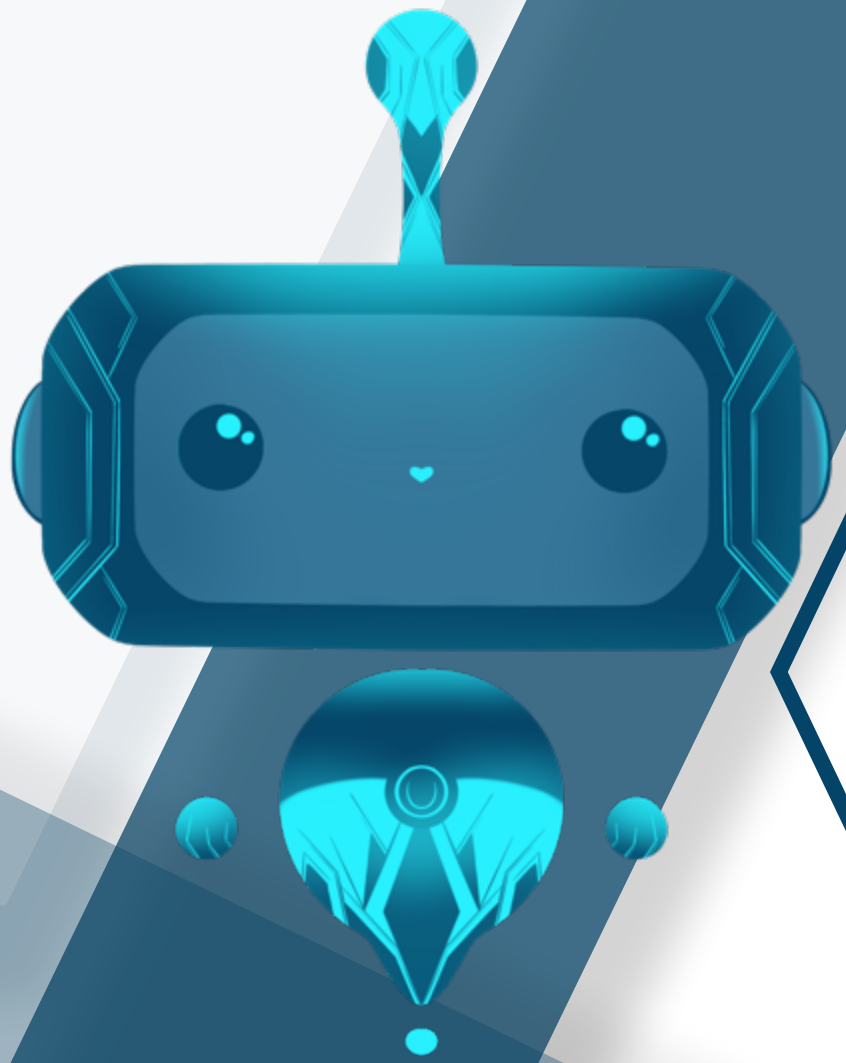


reTributor

Да, даже фото экрана :)

Немного о

20+ сотрудников, в т.ч. сертифицированных ИБ-экспертов с опытом работы CISO

2017 с 2017 г. занимается заказной разработкой программного обеспечения и комплексной автоматизацией деятельности клиентов

20 реализовано более 20 проектов для госорганов, транспортных и финансовых компаний

Собственная разработка:

- reTributor – маркировка документов, маркировка интерфейсов
- reTributor – messenger DLP
- reTributor Voice DLP – контроль голосовых каналов

Наши решения

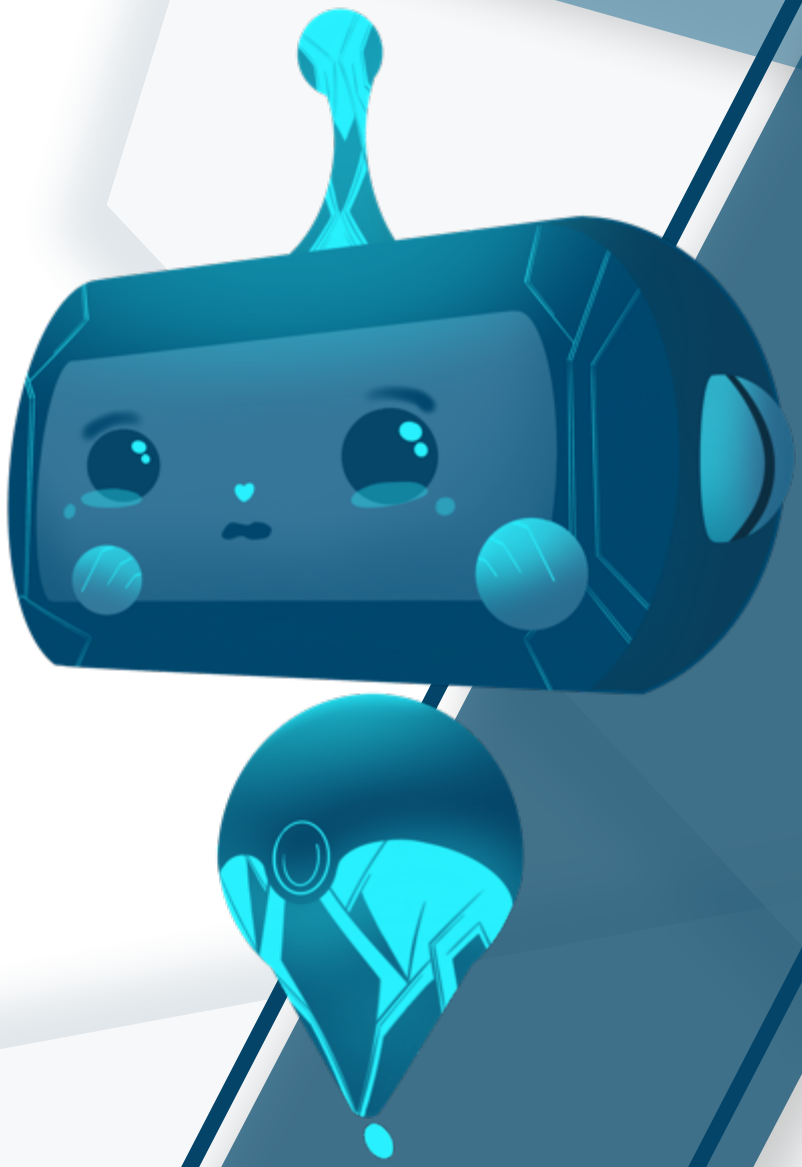
- reTributor – защита документов от утечек и выявление злоумышленников

  Автоматизированная идентификация источника утечки документов через:
  - распечатку
  - фото документа/экрана
  - захват экрана

- reTributor Voice DLP – контроль распространения конфиденциальной информации в голосовых каналах

  - речь в телефонных переговорах и звуковых сообщениях корпоративной связи
  - речь в записях онлайн конференций, данных систем видео-аудио-наблюдения
  - речь в записях из клиентских залов обслуживания

Утечки



Что может утечь?

Финансовая отчетность

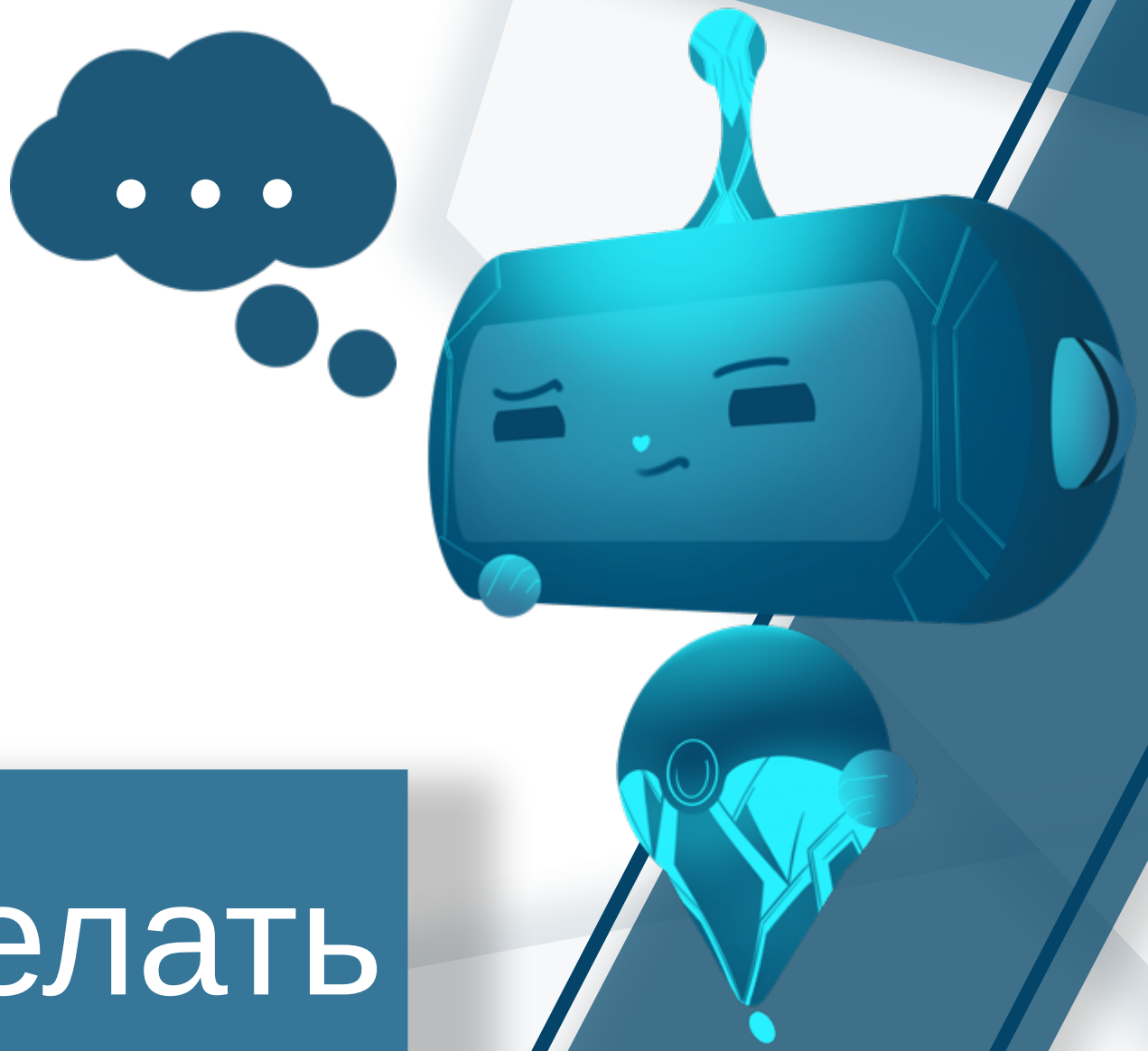
Клиентская база

Данные о закупках

Интеллектуальная собственность

ДСП информация

Персональные данные



Что с ними делать

Инструменты

Контроль доступа

Ограничивать и контролировать доступ к конфиденциальной информации

IAM
ECM / СЭД

Перехват и блокировка

Проводить автоматический анализ исходящих коммуникаций

DLP

ПРОБЛЕМА

Идентификация нарушителя

Если произошла утечка, необходимо максимально быстро и точно определить её источник

Каналы

ПРОБЛЕМА

- Почта
- Вывод на печать
- Интернет
- Мессенджеры
- Флешка
- Распечатка
- Фото
- Захват экрана

Чем мы можем помочь

Продукт 1

reTributor маркировка документов

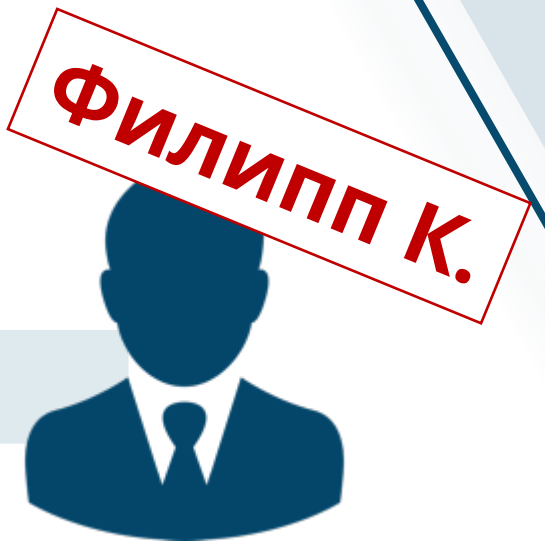
Однозначная автоматизированная идентификация источника утечки

Жизненный цикл документа

3 простых шага к расследованию

Какие документы
в утечке

Проверить в
системе



**Однозначный
результат**

Принцип работы

Отчет о кибератаках, характеризующих 2023 год, включая некоторые цифры и статистику.

1. Искусственный интеллект и Машинное обучение:
В течение года было выявлено более 30% увеличение кибератак, в которых применялись технологии искусственного интеллекта и машинного обучения. Это число представляет собой значительный рост по сравнению с предыдущими годами.

2. Кибератаки на критическую инфраструктуру:
Количество атак на критическую инфраструктуру возросло на 45% по сравнению с предыдущим годом. Было зафиксировано более 150 инцидентов, затрагивающих энергосистемы, транспортные сети и другие важные объекты.

3. Атаки на поставщиков:
Увеличение атак на поставщиков составило 25%. Это включает в себя как прямые атаки на поставщиков услуг, так и атаки на их системы, направленные на компрометацию цепочки поставок.

4. Угрозы "нулевого дня" и эксплоиты:
Атаки с использованием угроз "нулевого дня" увеличились на 20%. Злоумышленники успешно использовали ранее неизвестные уязвимости для компрометации систем и данных.

5. DDoS-атаки:
Было зафиксировано более 500 DDoS-атак, что представляет собой увеличение на 30%. Атаки стали более мощными и длительными, что требует повышенного внимания к защите от этого типа угроз.

Вносятся незаметные изменения в тексте, уникальные для каждого пользователя

Автоматически определяется пользователь, которому принадлежит копия документа

Отчет о кибератаках, характеризующих 2023 год, включая некоторые цифры и статистику.

1. Искусственный интеллект и Машинное обучение:
В течение года было выявлено более 30% увеличение кибератак, в которых применялись технологии искусственного интеллекта и машинного обучения. Это число представляет собой значительный рост по сравнению с предыдущими годами.

2. Кибератаки на критическую инфраструктуру:
Количество атак на критическую инфраструктуру возросло на 45% по сравнению с предыдущим годом. Было зафиксировано более 150 инцидентов, затрагивающих энергосистемы, транспортные сети и другие важные объекты.

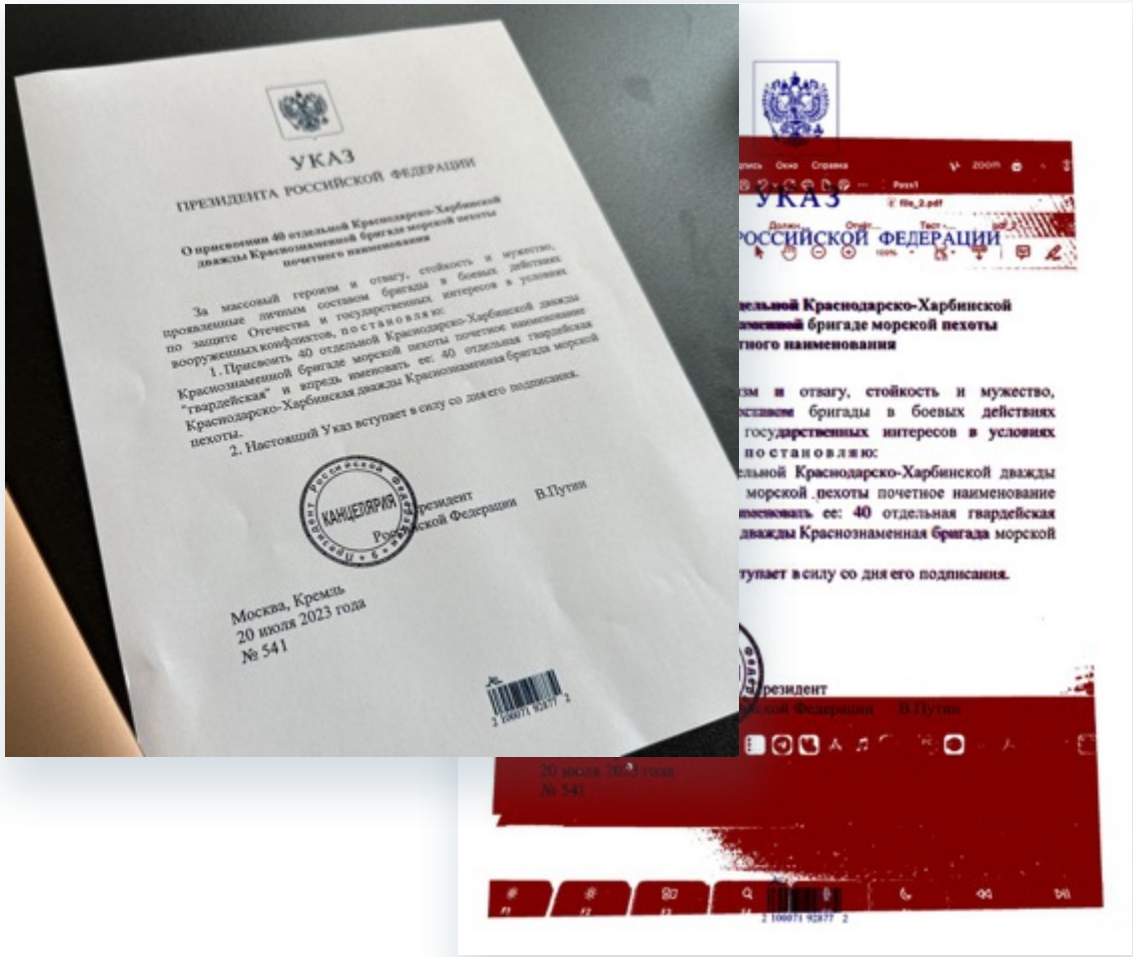
3. Атаки на поставщиков:
Увеличение атак на поставщиков составило 25%. Это включает в себя как прямые атаки на поставщиков услуг, так и атаки на их системы, направленные на компрометацию цепочки поставок.

4. Угрозы "нулевого дня" и эксплоиты:
Атаки с использованием угроз "нулевого дня" увеличились на 20%. Злоумышленники успешно использовали ранее неизвестные уязвимости для компрометации систем и данных.

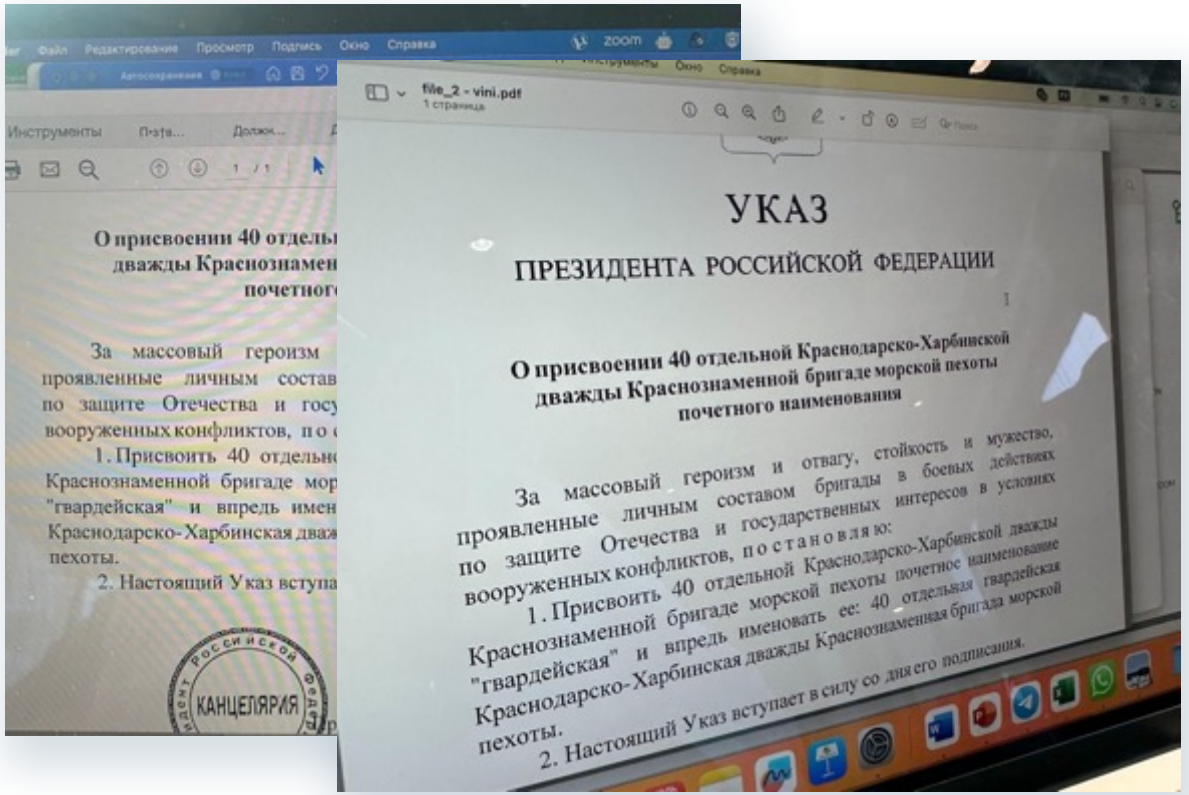
5. DDoS-атаки:
Было зафиксировано более 500 DDoS-атак, что представляет собой увеличение на 30%. Атаки стали более мощными и длительными, что требует повышенного внимания к защите от этого типа угроз.

Принцип работы

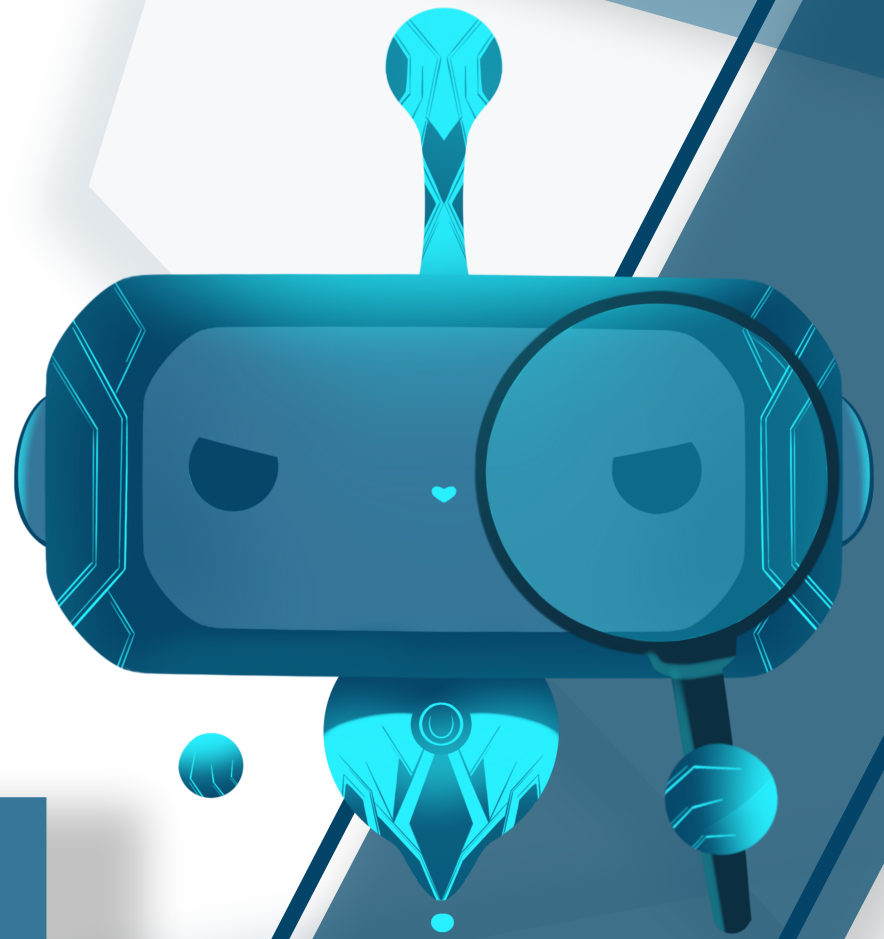
Нечеткая фотография документа



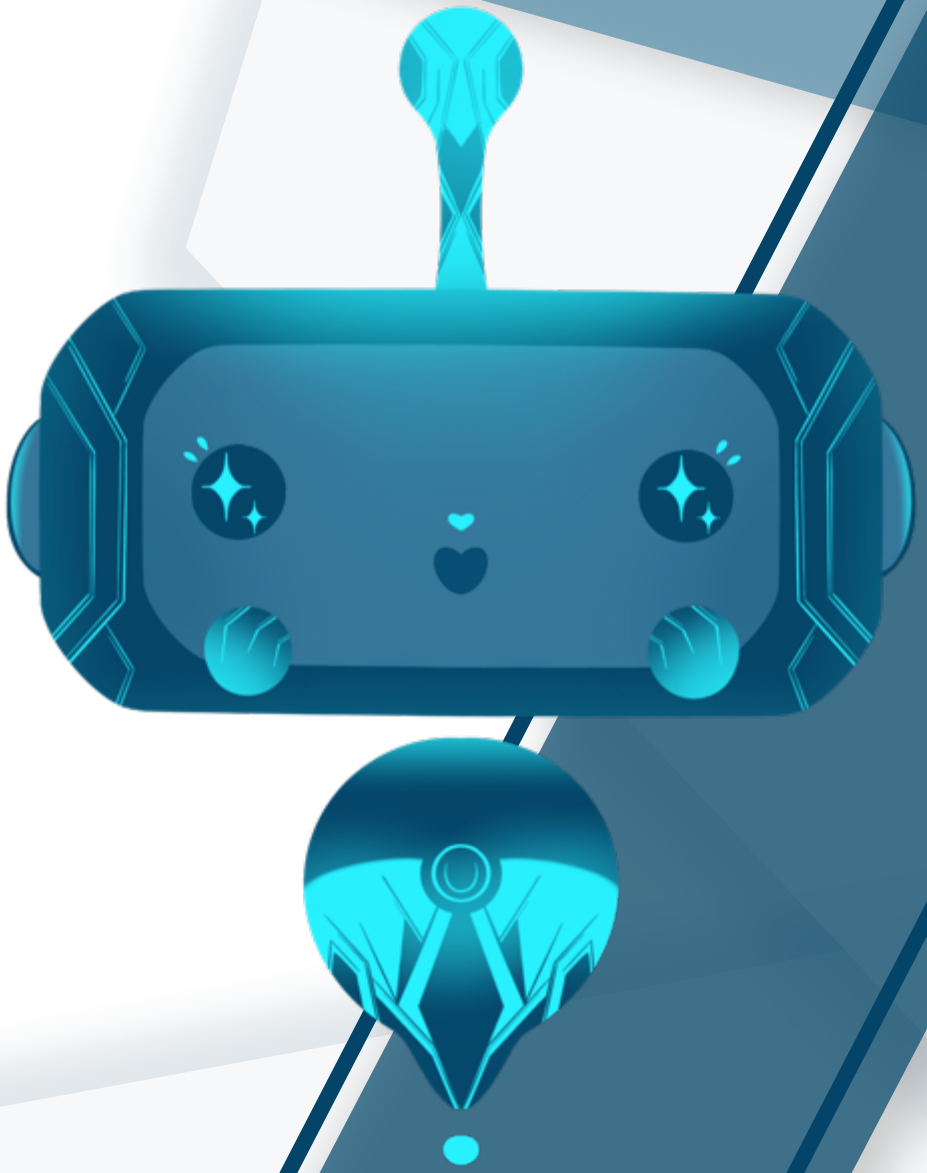
Фотография экрана с искажениями



Демонстрация



В итоге



Расследуйте сразу

Было

Опасно

Некоторые каналы полностью открыты

Не понятно

Как определить источник, если произойдет утечка

Долго

Расследование утечки было нелинейным и требовало много ресурсов

Страшно

Что когда произойдёт утечка, будет невозможно её расследовать

Стало

Прозрачно

Определить источник даже на сложных каналах

Точно

Однозначная идентификация источника

Быстро

Процесс занимает несколько минут и 3 простых шага

Спокойно

Даже если утечка произойдёт, вы будете знать кто это сделал - и предотвратить их в будущем

Продукт 3

reTributor Voice DLP

Контроль распространения конфиденциальной информации в голосовых каналах

Каналы утечки информации с высоким риском

Необходимость в контроле:

- Телефонных переговоров и звуковых сообщений корпоративной связи
- Записей онлайн конференций, данных систем видео-аудио-наблюдения
- Записей из клиентских залов обслуживания

Существующие инструменты защиты

Внутренний контроль

1. Настройка политик на создание, передачу и хранение звукозаписей

2. Повышение осведомленности сотрудников о недопустимости распространения конфиденциальной информации

3. Ручная проверка и прослушка данных

Решения на рынке

1. Облачные сервисы транскрибации речи в текст

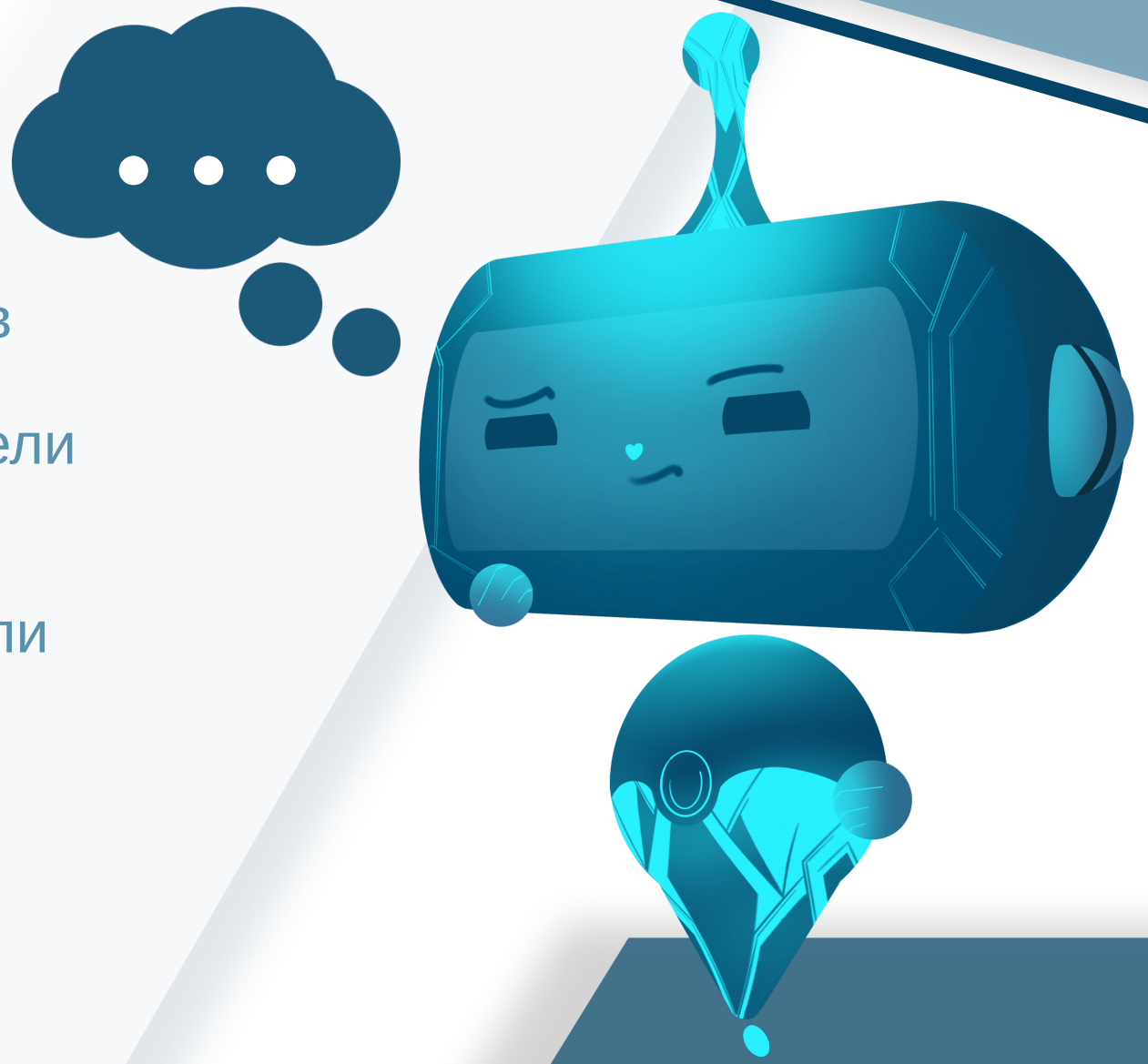
Эффективность расследований

2. Системы управления контроля доступом

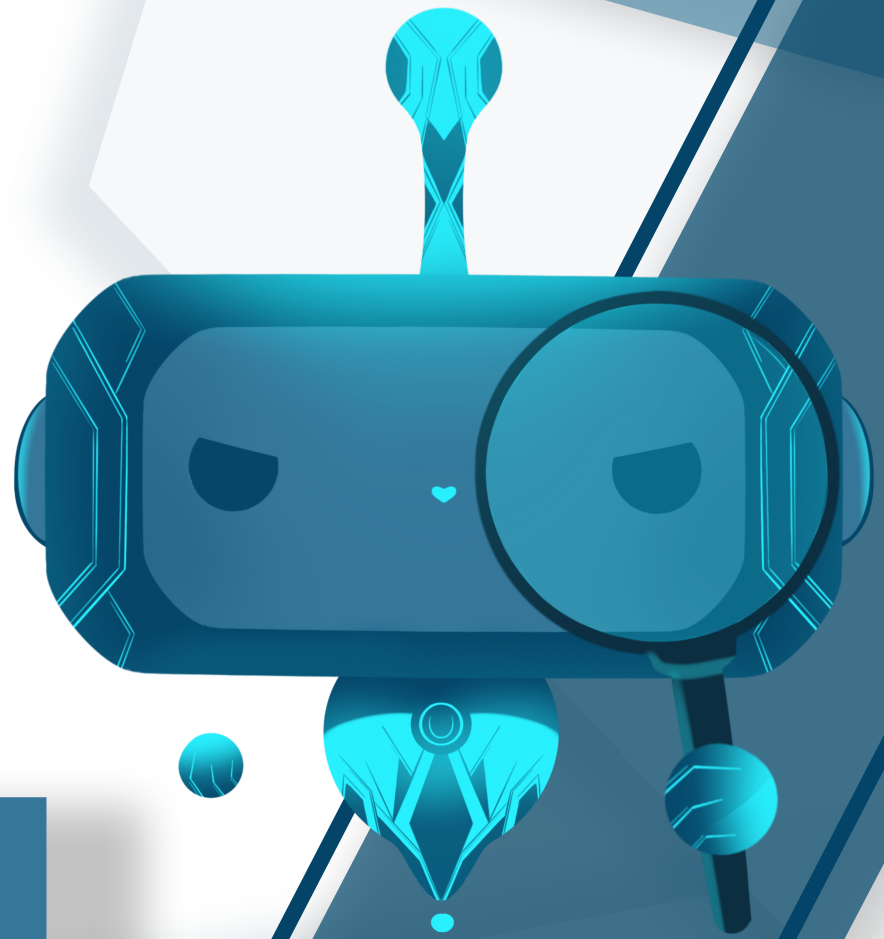
3. Системы записи телефонных звонков

Минусы облачных решений транскрибации речи

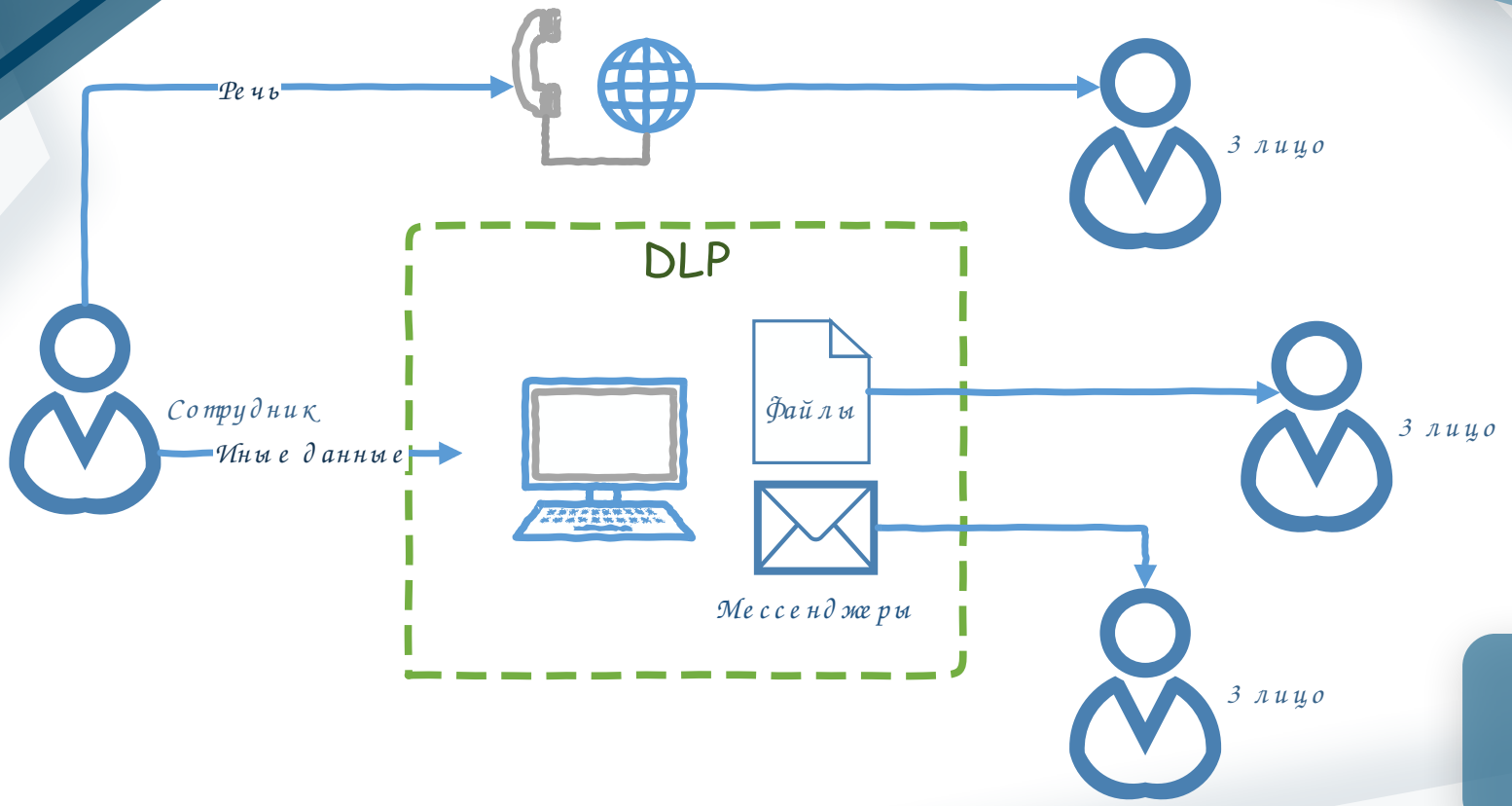
- Высокая доля ручной компоненты при обработке потенциальных инцидентов
- Невозможность реагирования по модели угроз и политики заказчика
- Несовместимость с DLP системами или ограниченность функционала
- Условия тарификации

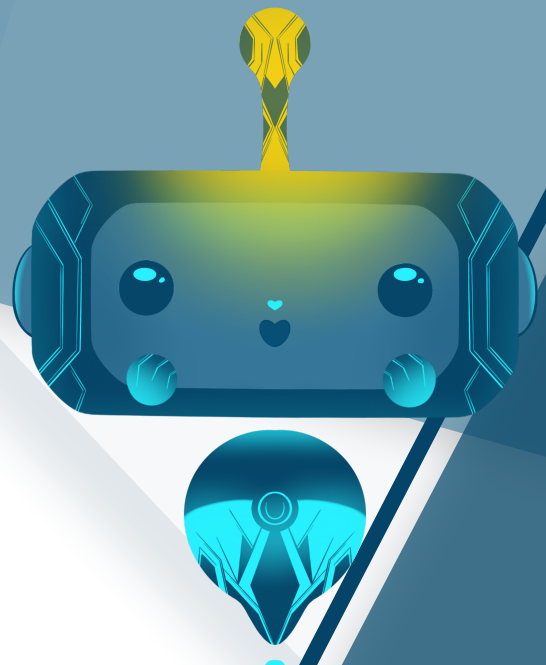


Демонстрация



Общая схема



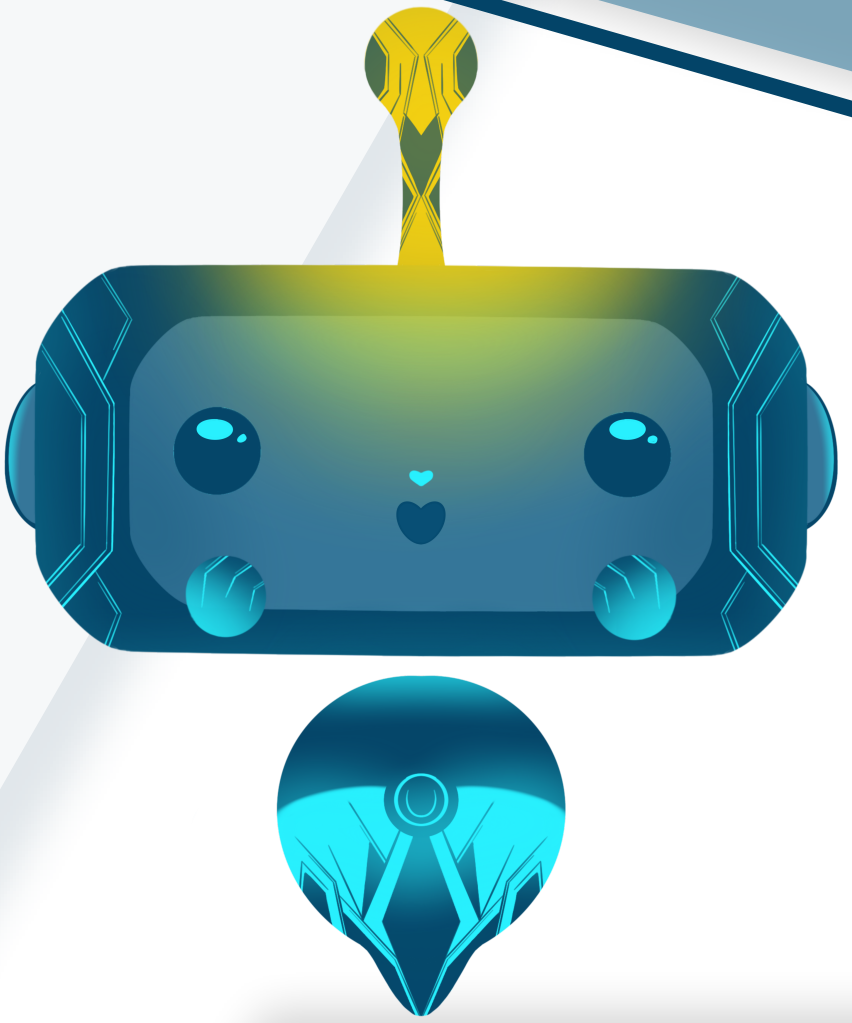


+

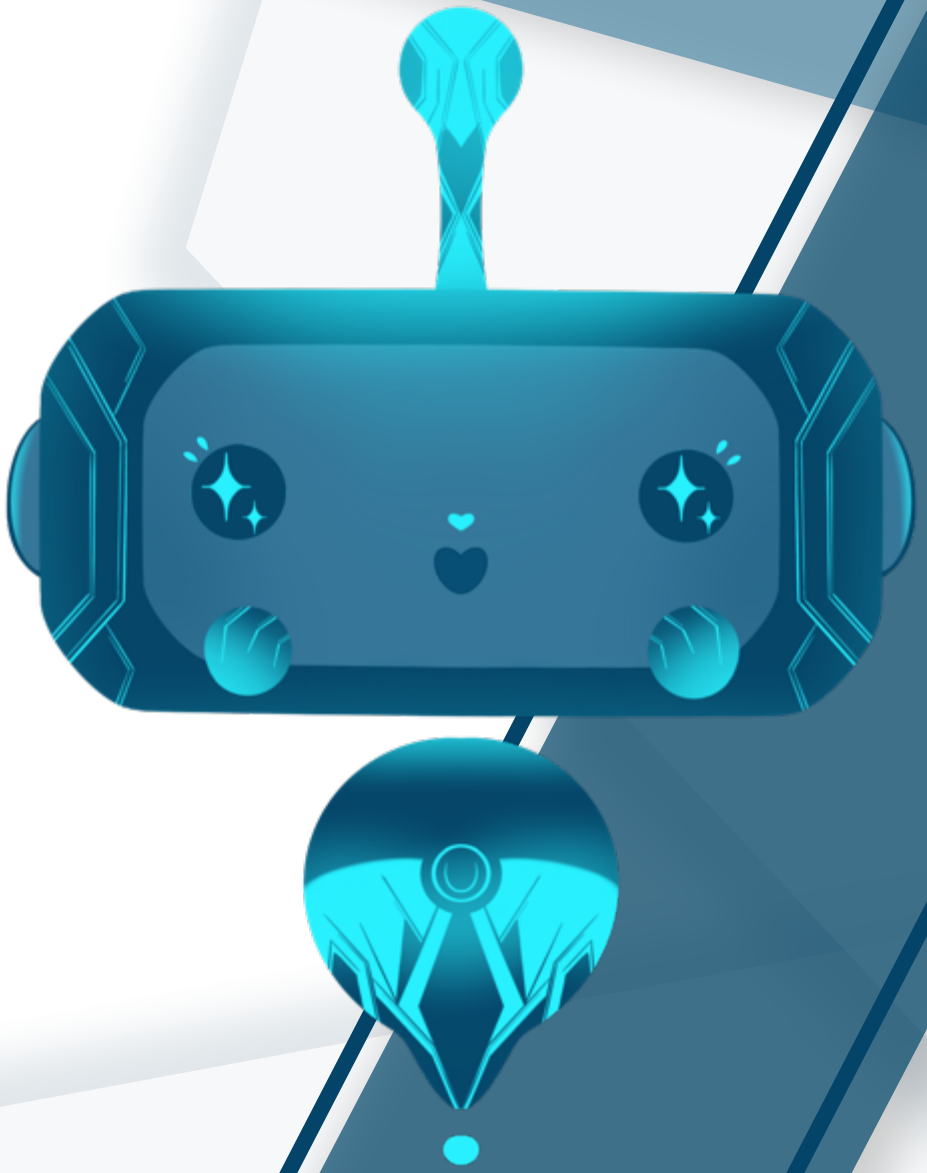
Система может работать в режиме «Stand-alone» без использования DLP

Преимущества

- Полная автоматизации процесса обработки потенциальных инцидентов
- Возможность адаптации под модель угроз и политики Заказчика
- Бесшовная интеграция с DLP-системой
- Сопоставимая стоимость с предложениями на рынке



В итоге



reTributor Voice DLP

ДО

Сизифов труд

Ручная проверка каждого файла

Непонятно

ак определить источник, если произойдет утечка

Долго

Расследование утечки нелинейно и требует много ресурсов (70% записи - тишина)

Страшно

Невозможность расследования утечки в случае инцидента

ПОСЛЕ

Автоматизация

Инциденты выявляются по настроенным политикам

Точно

Однозначная идентификация источника

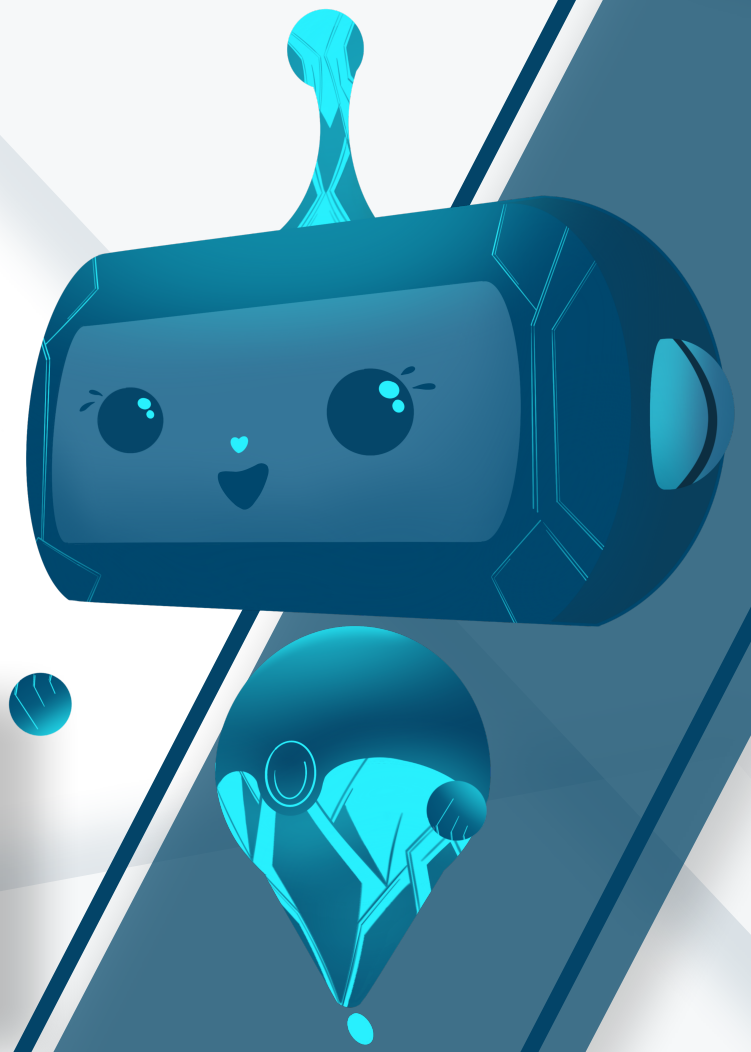
Быстро

Процесс полностью автоматизирован и доступен в режиме реального времени

Спокойно

Точность идентификации источника работает в дальнейшем как превентивная мера

Вопросы?



Татьяна Самойленко

Директор по продажам

https://retributor.ru

ts@afi-d.ru

+7 982 390 83 10

Подключайтесь