ЦЕНТРАЛИЗОВАННАЯ ЗАЩИТА БАЗ ДАННЫХ

Горлянский Дмитрий

Москва
17 февраля 2021 г.

ПРОБЛЕМЫ ДЕТЕКТИРОВАНИЯ УТЕЧЕК НА ПЕРИМЕТРЕ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

- Большое количество каналов передачи данных
- Неконтролируемые каналы
- Формализация данных
- Формализация утечки

КОНТРОЛЬ ДОСТУПА ВМЕСТО РАСПРОСТРАНЕНИЯ

ГАРДА БД

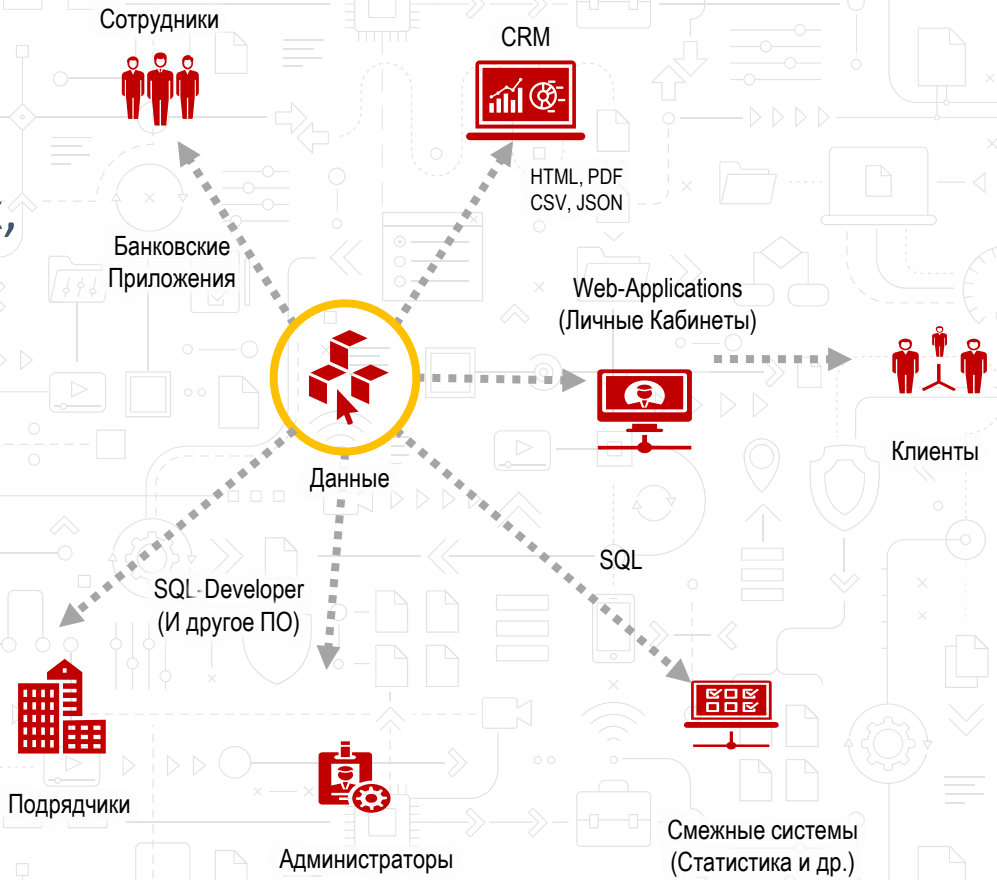
ГАРДА ТЕХНОЛОГИИ

Данные хранятся централизовано.

Прежде чем осуществить утечку данных, злоумышленник должен их получить.

Преимущества подхода:

- Независимость от каналов доступа
- Единое представление данных
- Структурированность данных и их формальное описание



АУДИТ ДОСТУПА СРЕДСТВАМИ СУБД

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

Аудит доступа к данным в СУБД
входит во все мировые стандарты безопасности.

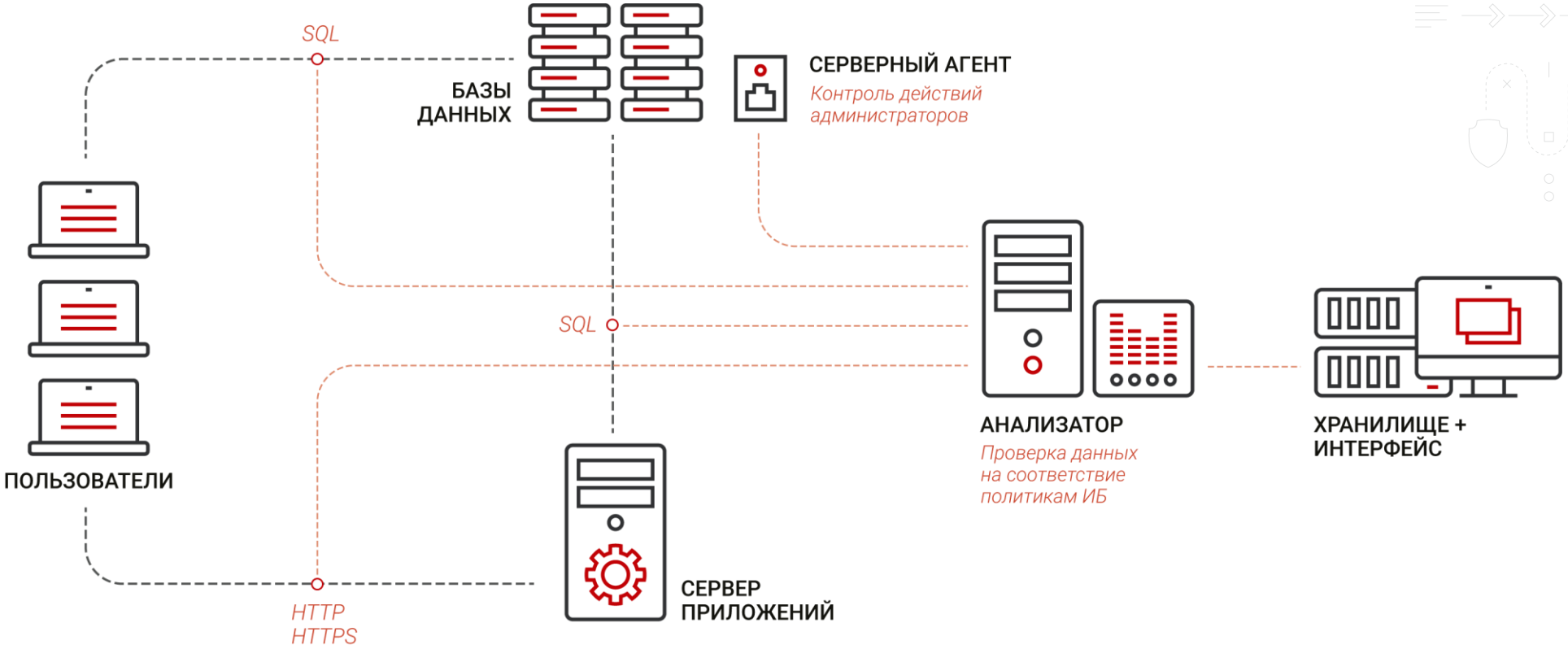
Недостатки аудита средствами СУБД:

- Нагрузка на аппаратную часть
- Сложность настройки
- Возможность отключения
- Сложность анализа

МОНИТОРИНГ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ



Опционально:
Агенты для контроля локальных подключений

ВОЗМОЖНОСТИ DAM/DBF СИСТЕМ

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

1. Анализ трафика
Анализ сетевого и локального трафика и проверка на легитимность запросов пользователей и ответов БД.

3. Поиск баз
Обнаружение всех активных СУБД, выявление фактов их перемещения/изменения. Контроль за созданием новых ИС/АС

5. Аналитика/Отчеты + UBA
Выявление нарушения политик безопасности
Отклонения от модели типичного поведения пользователей.

2. Долгосрочное хранение информации
Обработка данных (например, проверка на регулярные выражения) и сохранение всех запросов и ответов для ретроспективного анализа.

4. Сканирование баз
Классификация СУБД
Выявление уязвимостей СУБД (неоптимальных настроек)
Построение матриц доступа к СУБД

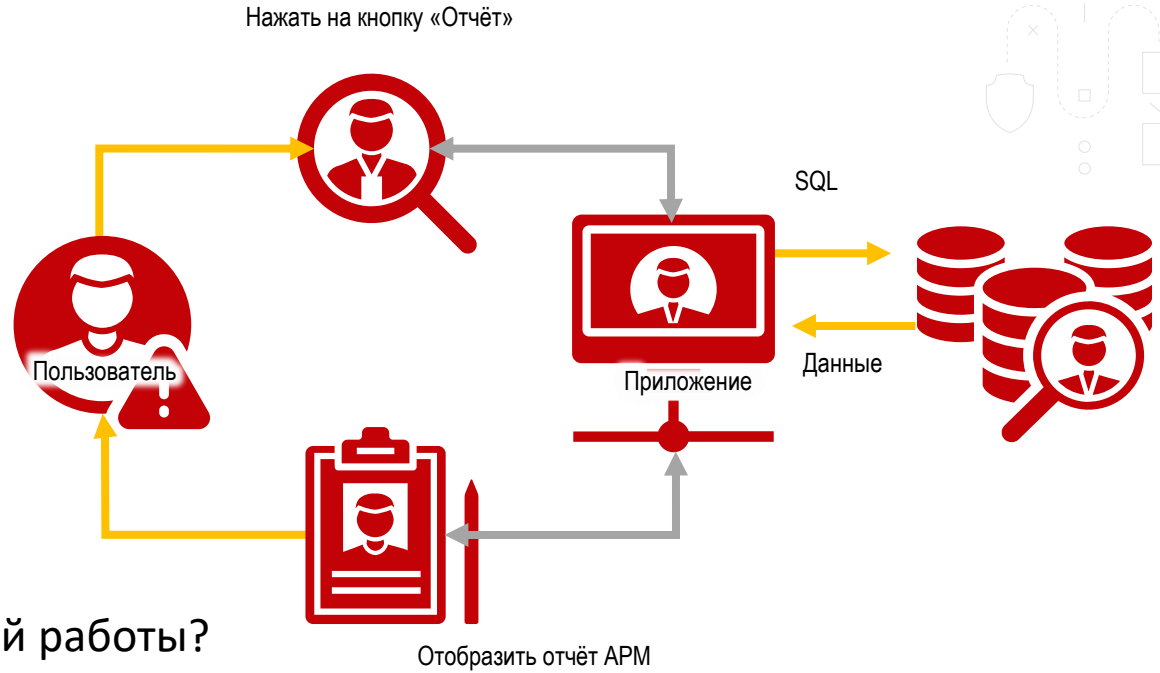
6. Система оповещения.
Дашборды,
уведомления о событиях по e-mail,
передача данных во внешние SIEM-системы

ПРИВЯЗКА ПОЛИТИК К БИЗНЕС-ПРОЦЕССАМ

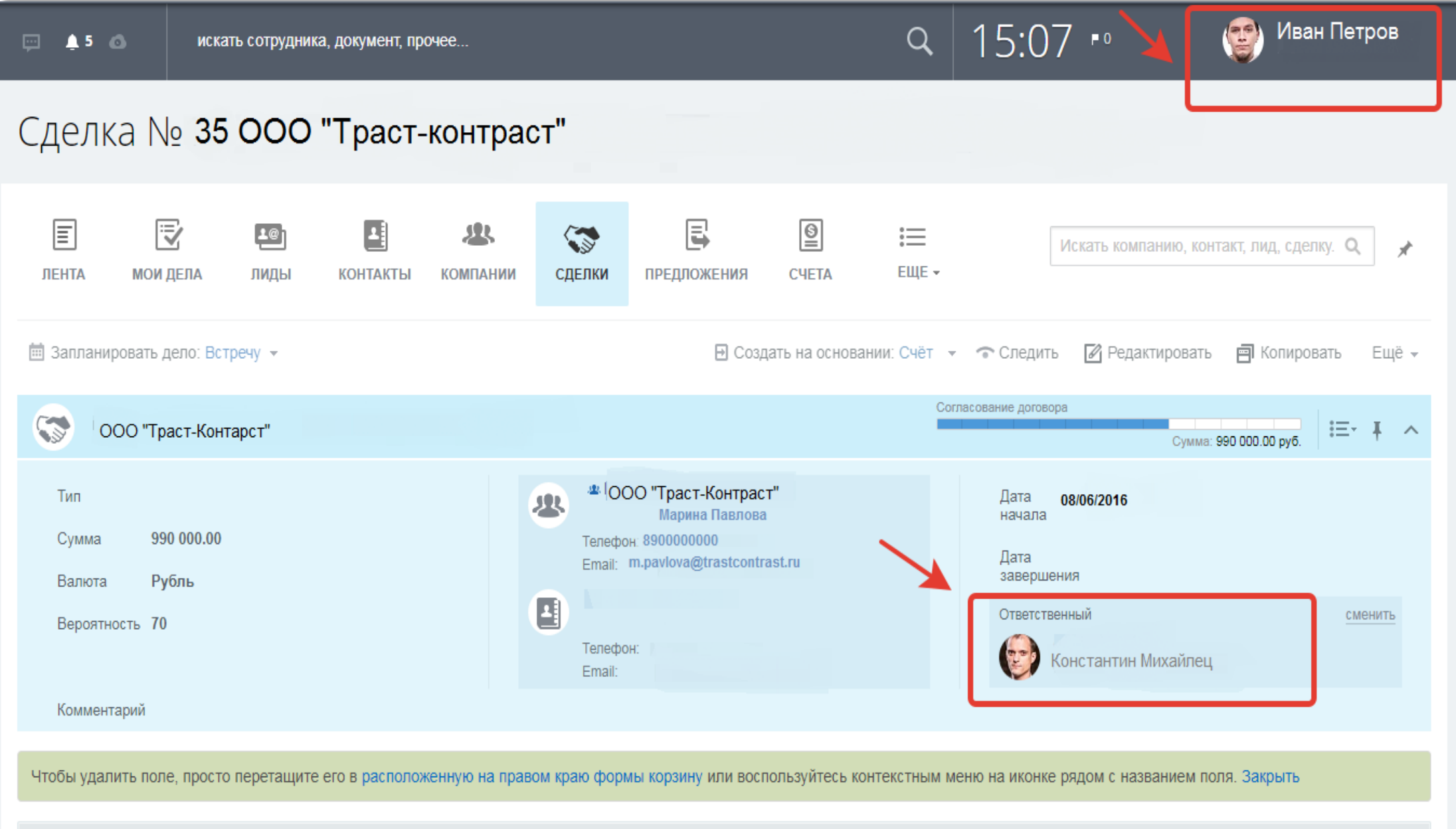
ГАРДА БД
ГАРДА ТЕХНОЛОГИИ

Политики можно настроить в соответствии с типовыми действиями пользователя:

- Аудит действий
- Возможность выявлять нарушения



Вопрос:
Как отличить утечку данных от штатной работы?


искать сотрудника, документ, прочее...
15:07
Иван Петров
Сделка № 35 ООО "Траст-контраст"
ЛЕНТА
МОИ ДЕЛА
ЛИДЫ
КОНТАКТЫ
КОМПАНИИ
СДЕЛКИ
ПРЕДЛОЖЕНИЯ
СЧЕТА
ЕЩЕ
Искать компанию, контакт, лид, сделку.
Запланировать дело: Встречу
Создать на основании: Счёт
Следить
Редактировать
Копировать
Ещё
ООО "Траст-Контарст"
Согласование договора
Сумма: 990 000.00 руб.
Тип
Сумма 990 000.00
Валюта Рубль
Вероятность 70
Комментарий
ООО "Траст-Контраст"
Марина Павлова
Телефон: 8900000000
Email: m.pavlova@trastcontrast.ru
Телефон:
Email:
Дата начала 08/06/2016
Дата завершения
Ответственный
сменить
Константин Михайлец
Чтобы удалить поле, просто перетащите его в расположенную на правом краю формы корзину или воспользуйтесь контекстным меню на иконке рядом с названием поля. Закрыть

ЗАЧЕМ UBA?

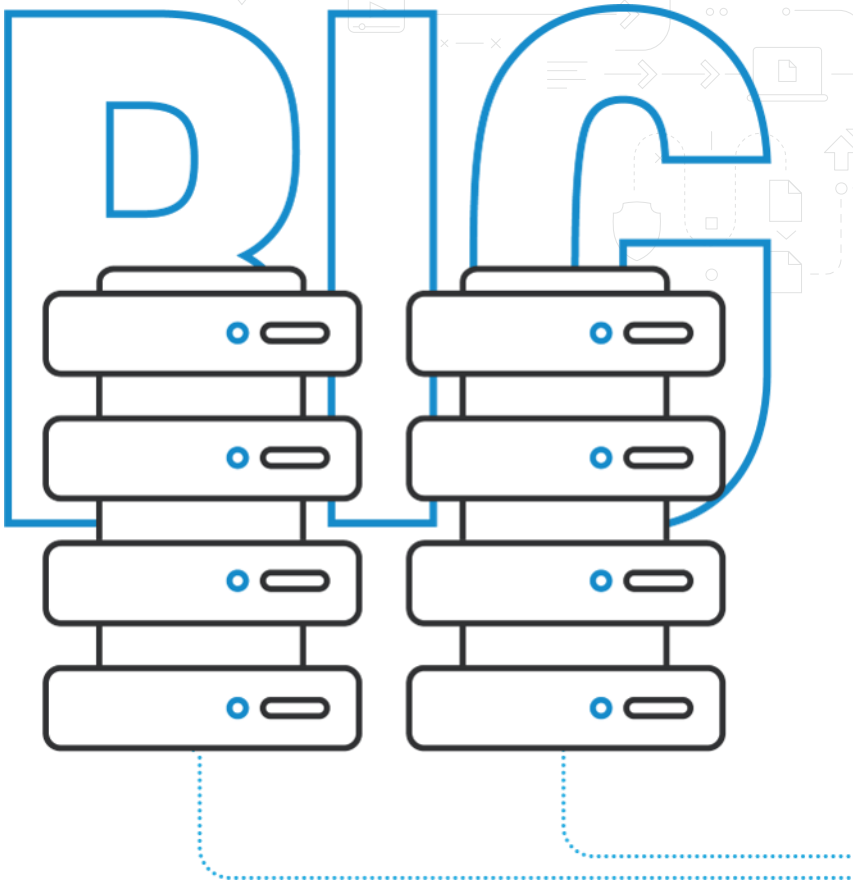
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

USER AND ENTITY BEHAVIOR ANALYTICS (UEBA) - ПОВЕДЕНЧЕСКАЯ АНАЛИТИКА ПОЛЬЗОВАТЕЛЕЙ И СУЩНОСТЕЙ

UBA как модуль существующих ИБ-систем.

Оперирует активностью пользователей/сущностей внутри/снаружи компании, и информацией, к которой происходит обращение.



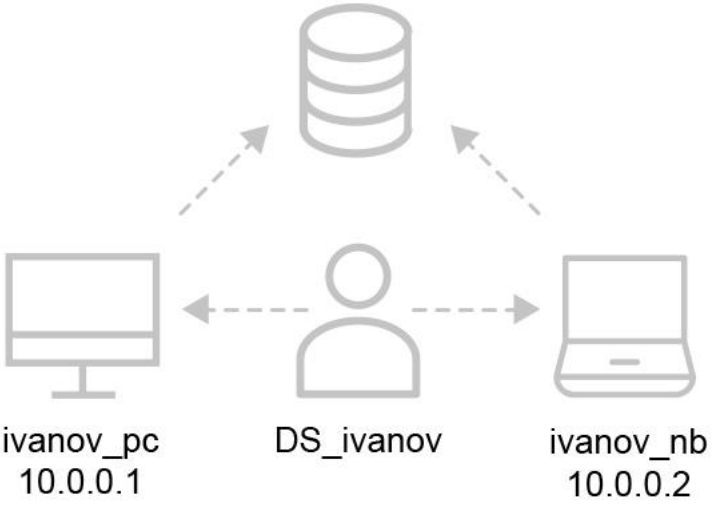
ВЫЯВЛЯЕТ ОТКЛОНЕНИЯ

- Определяет сущность (пользователь/хост/приложение)
- Формирует модель (портрет поведения)
- Внутри использует принципы машинного обучения

КЕЙС 1. СКОМПРОМЕТИРОВАННЫЕ УЧЕТНЫЕ ЗАПИСИ

Компрометация— факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

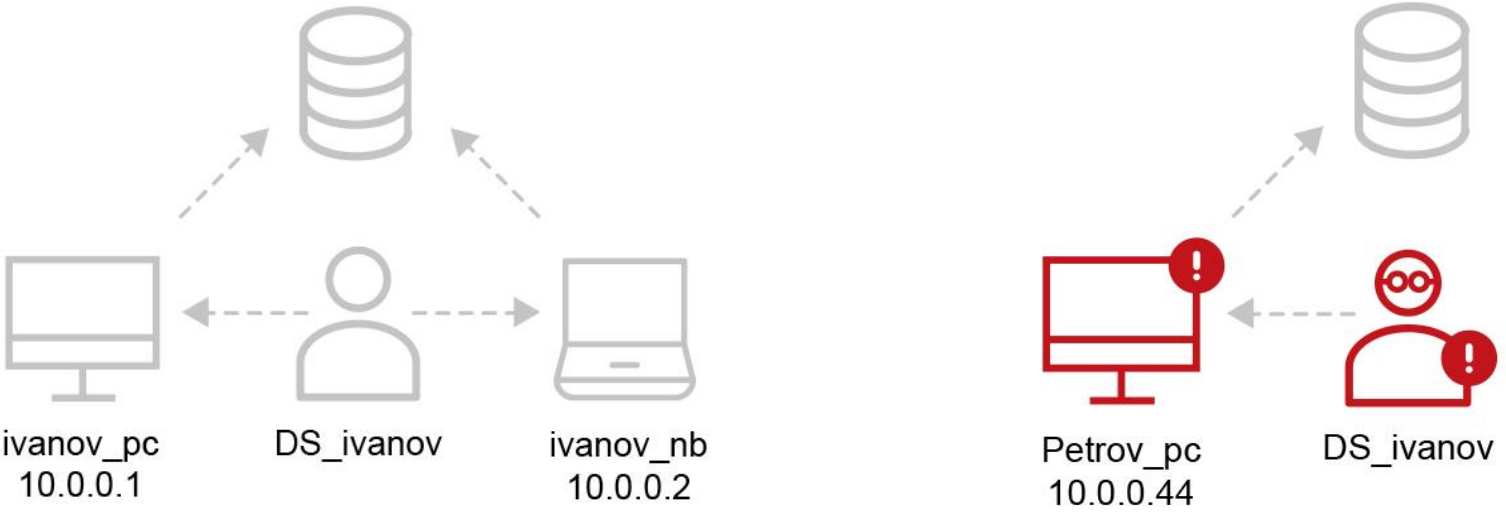
Профиль - это учетная запись, IP-адрес, имя компьютера, доменная УЗ и т. д.



КЕЙС 1. СКОМПРОМЕТИРОВАННЫЕ УЧЕТНЫЕ ЗАПИСИ

Компрометация— факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Профиль - это учетная запись, IP-адрес, имя компьютера, доменная УЗ и т. д.



КЕЙС 2. ДОСТУП К ЧУЖОЙ/ИЗБЫТОЧНОЙ ИНФОРМАЦИИ

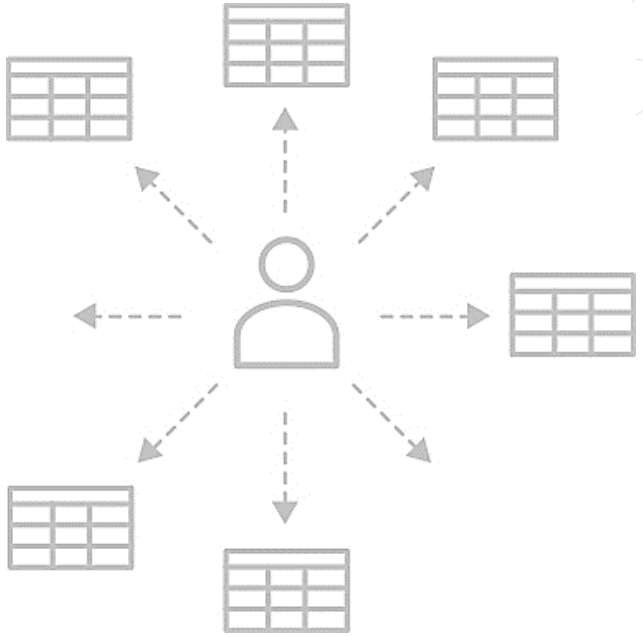
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

ДОСТУП К НОВЫМ ДАННЫМ

В профиль включена статистика и список используемых пользователем таблиц и полей.

Инцидент – факт обращения к ранее неиспользуемым объектам ИС\АС.



КЕЙС 2. ДОСТУП К ЧУЖОЙ/ИЗБЫТОЧНОЙ ИНФОРМАЦИИ

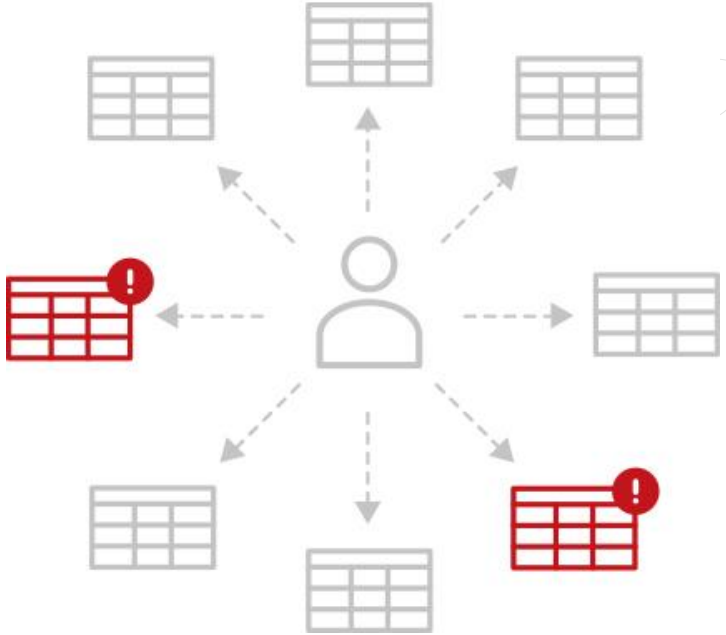
ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

ДОСТУП К НОВЫМ ДАННЫМ

В профиль включена статистика и список используемых пользователем таблиц и полей.

Инцидент – факт обращения к ранее неиспользуемым объектам ИС\АС.

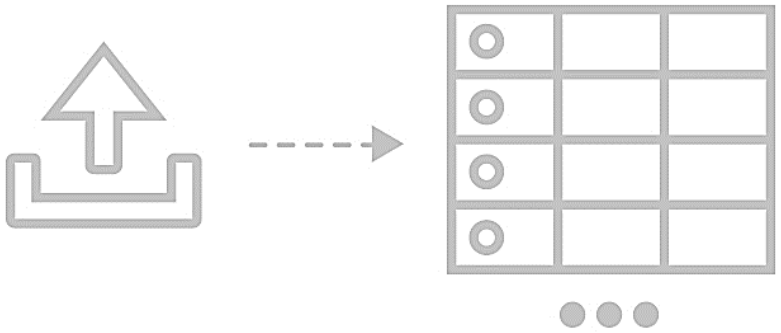


Решение проблемы:
Выявление отклонений от автоматически сформированной модели поведения пользователя.

КЕЙС 3. КОЛИЧЕСТВЕННАЯ АНАЛИТИКА

БОЛЬШИЕ ВЫГРУЗКИ

Позволяет выявлять инциденты, как цепочку событий



Выгрузка одним запросом

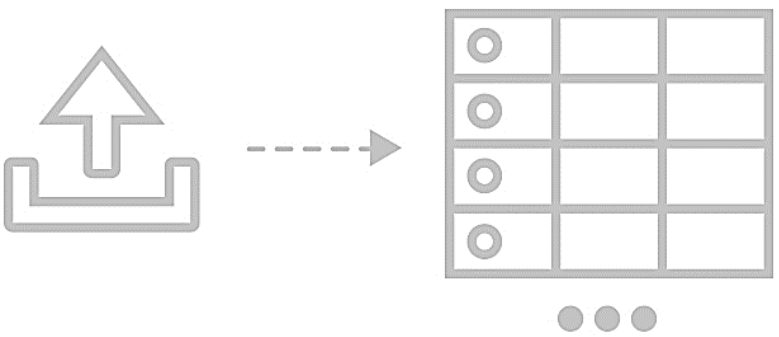
КЕЙС 3. КОЛИЧЕСТВЕННАЯ АНАЛИТИКА

ГАРДА БД

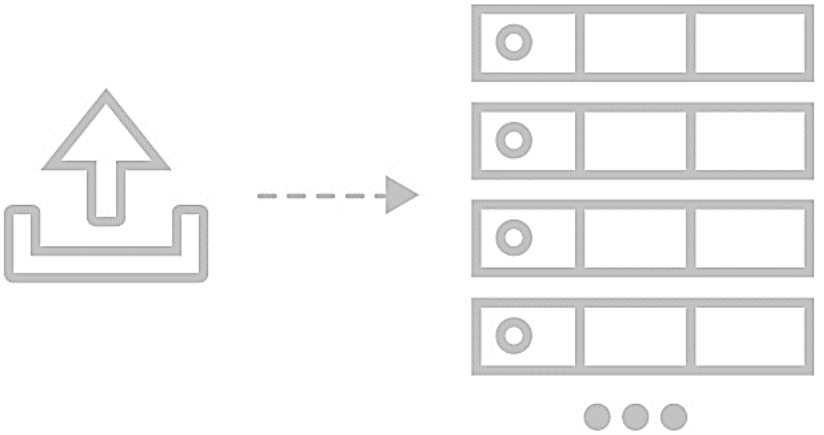
ГАРДА ТЕХНОЛОГИИ

БОЛЬШИЕ ВЫГРУЗКИ

Позволяет выявлять инциденты, как цепочку событий



Выгрузка одним запросом



Выгрузка по частям

ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ !