ГАРДА БД

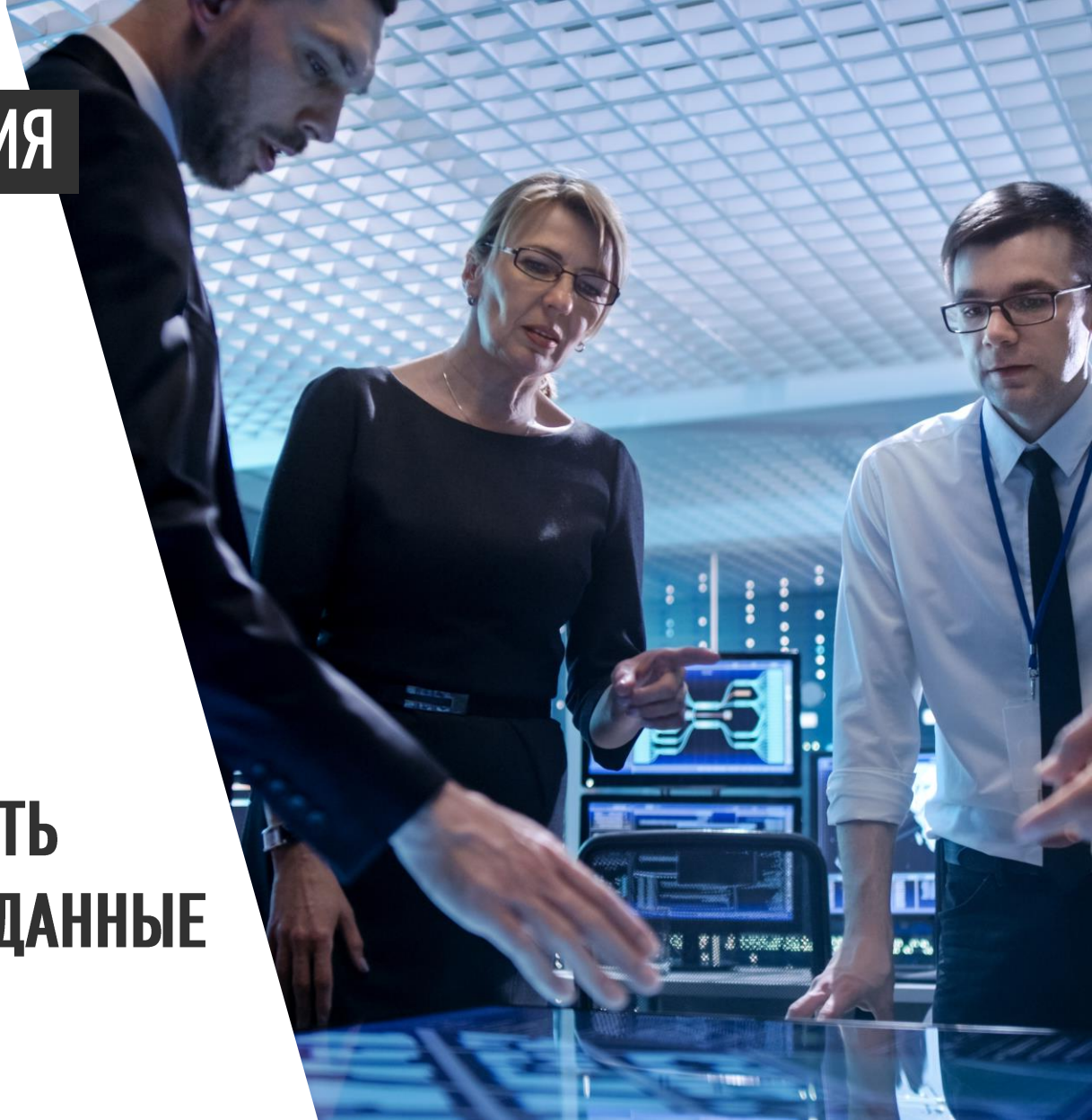
ГАРДА ТЕХНОЛОГИИ

ЦЕНТРАЛИЗОВАННАЯ ЗАЩИТА БАЗ ДАННЫХ В СУБД

Дмитрий Горлянский

Руководитель направления технического сопровождения продаж

ПРОБЛЕМЫ ДЕТЕКТИРОВАНИЯ УТЕЧЕК НА ПЕРИМЕТРЕ



ТРУДНО ОХВАТИТЬ ВСЕ КАНАЛЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

СЛОЖНО ФОРМАЛИЗОВАТЬ И ИДЕНТИФИЦИРОВАТЬ ДАННЫЕ

значительной мере определяется уровнем текущей потребности в инвестиционных ресурсах, готовностью организации к реализации отдельных инвестиционных проектов, обеспечивающих обновление операционных внеоборотных активов.¶

Учет перечисленных факторов позволяет организации выбрать соответствующие методы амортизации отдельных групп операционных внеоборотных активов, в наибольшей степени отражающие специфику их

А ЧТО ЭТО У НАС ЗДЕСЬ?..

ационном процессе.¶

950 000 000	**61,54%**
584 630 000	**50%**
292 315 000	**57,14%**
167 028 791	**100%**
167 028 791	**50%**
83 514 396	**60%**
50 108 637	**33,33%**

В современной отечественной практике различают два основных метода амортизации внеоборотных активов:¶

метод прямолинейной (линейной) амортизации - основан на прямолинейно пропорциональном способе начисления износа амортизируемых активов (основных средств,

КОНТРОЛЬ ДОСТУПА ВМЕСТО РАСПРОСТРАНЕНИЯ

ГАРДА БД

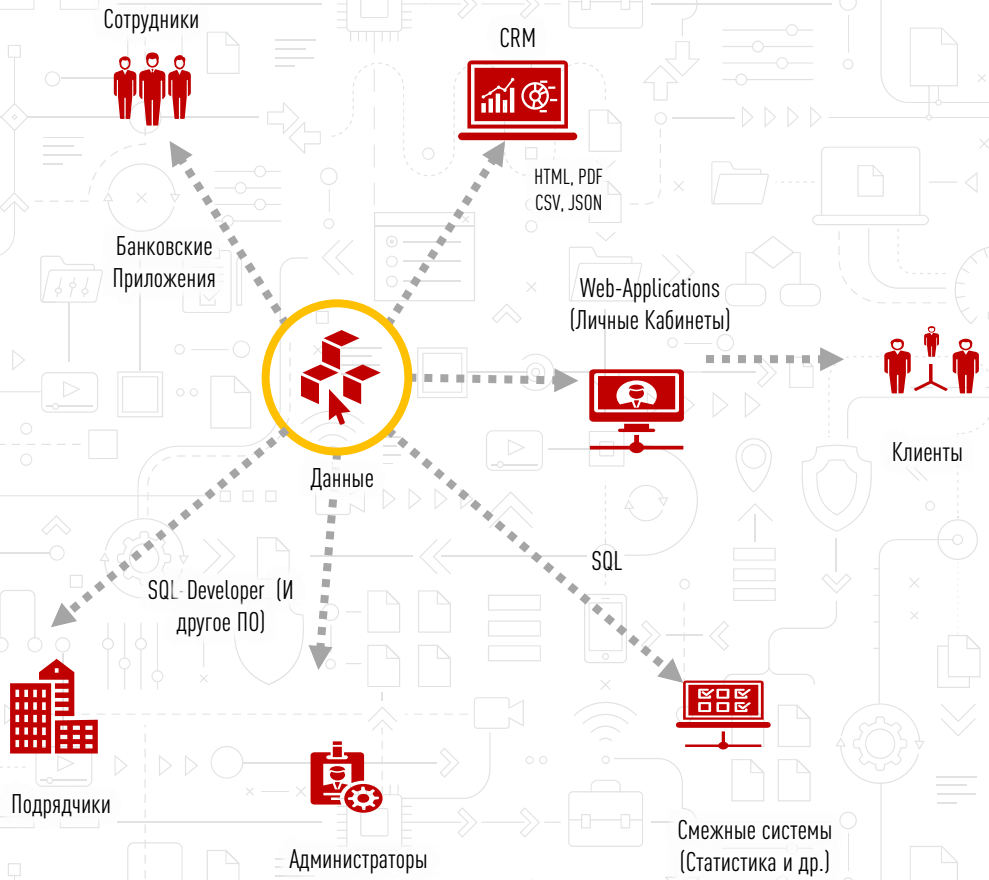
ГАРДА ТЕХНОЛОГИИ

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.

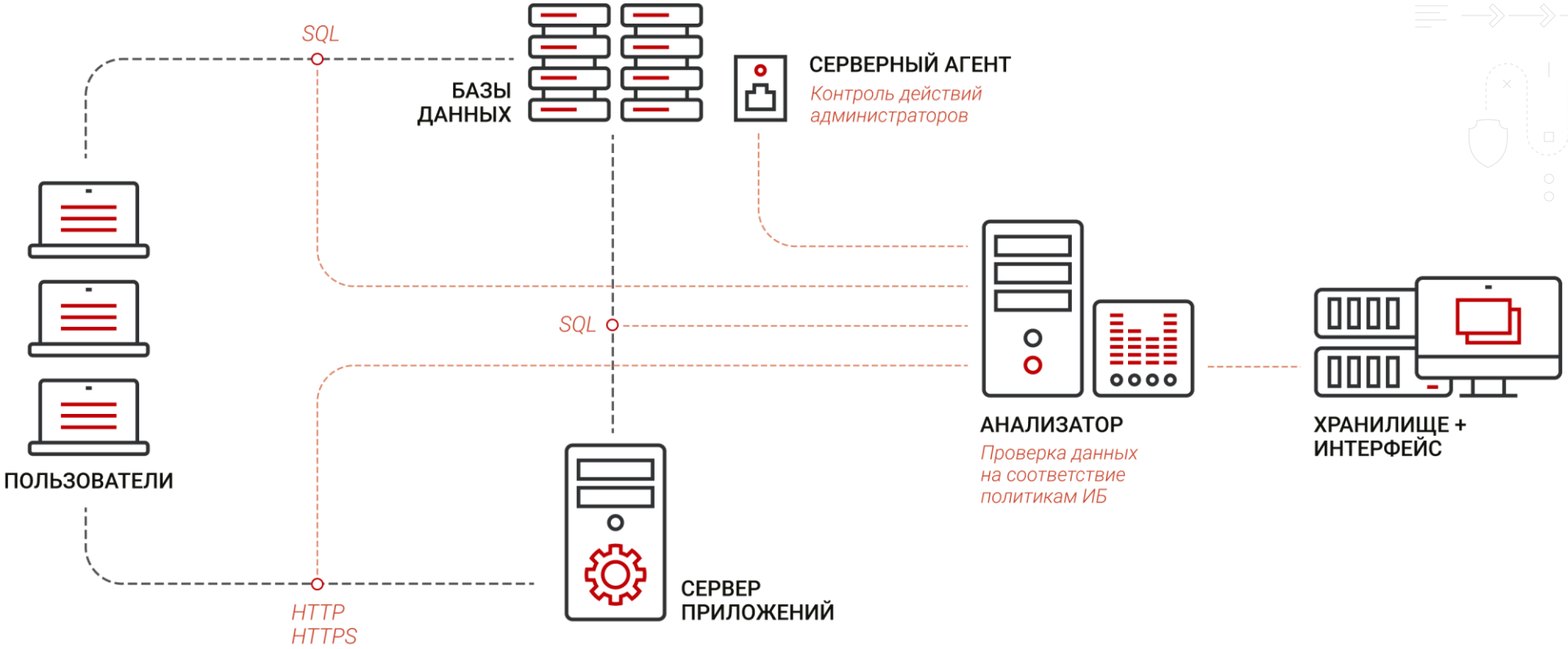
НЕДОСТАТКИ АУДИТА СРЕДСТВАМИ СУБД:

- 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.

2. Долгосрочное хранение информации

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

3. Поиск баз

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

4. Сканирование баз

Классификация СУБД

Выявление уязвимостей СУБД (неоптимальных настроек)

Построение матриц доступа к СУБД

5. Аналитика/Отчеты + UBA

Выявление нарушения политик безопасности

Отклонения от модели типичного поведения пользователей.

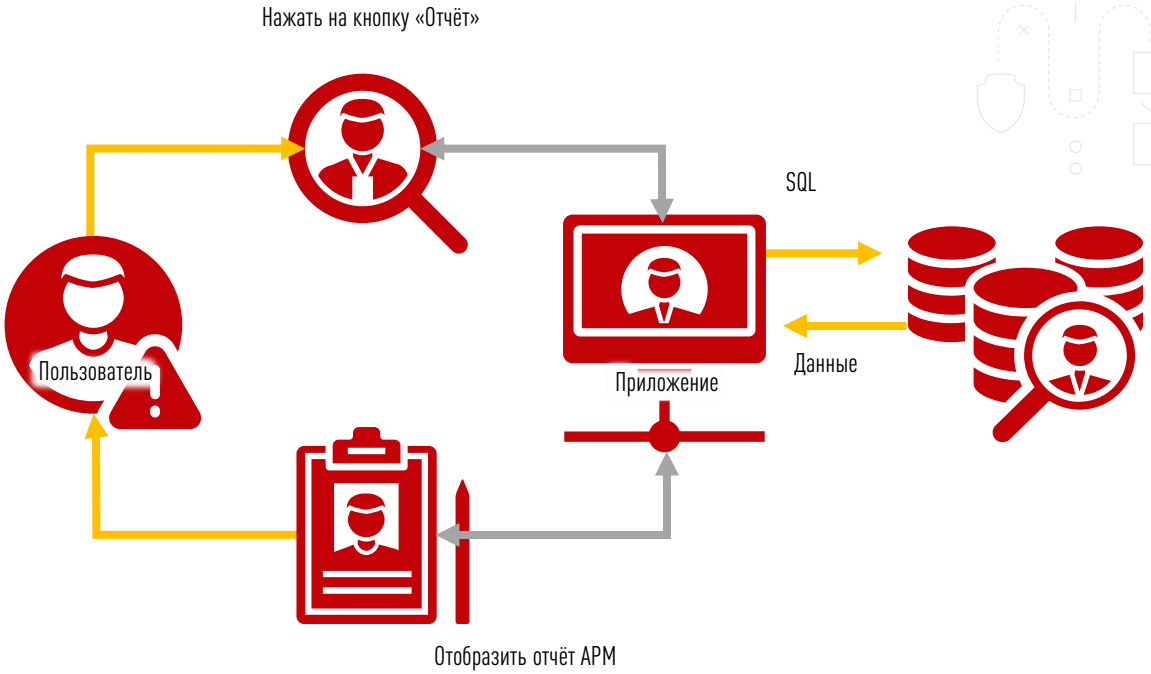
6. Система оповещения.

Дашборды, уведомления о событиях по e-mail, передача данных во внешние SIEM-системы

ПРИВЯЗКА ПОЛИТИК К БИЗНЕС-ПРОЦЕССАМ

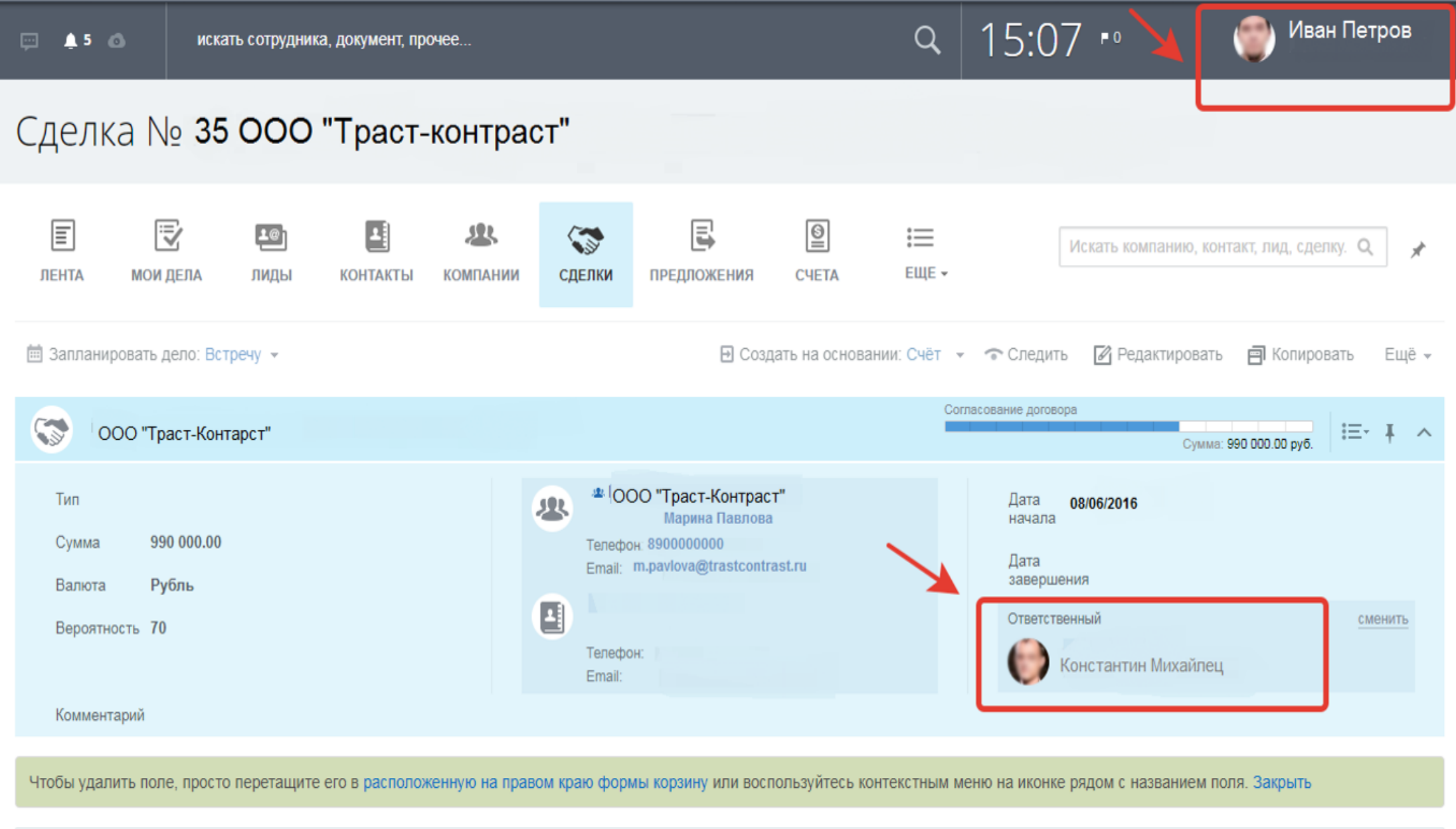
ПОЛИТИКИ МОЖНО НАСТРОИТЬ В СООТВЕТСТВИИ С ТИПОВЫМИ ДЕЙСТВИЯМИ ПОЛЬЗОВАТЕЛЯ:

- Аудит действий
- Возможность выявлять нарушения



ВОПРОС:

Как отличить утечку данных от штатной работы?


5
искать сотрудника, документ, прочее...
15:07
0
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?

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.

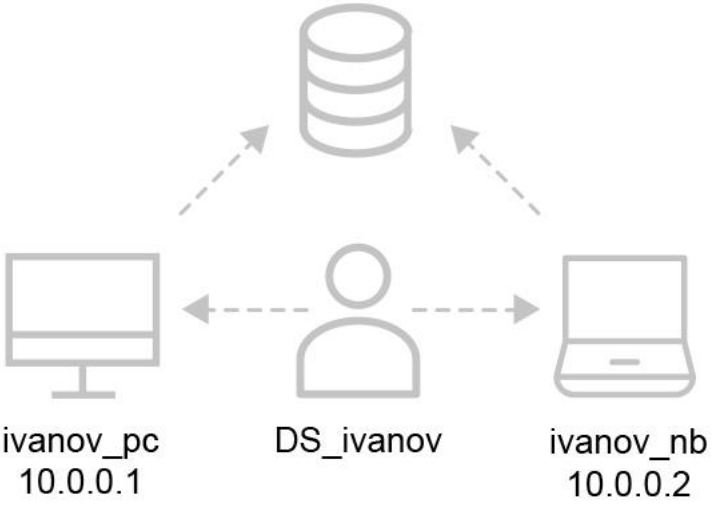
ВЫЯВЛЯЕТ ОТКЛОНЕНИЯ

- 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.

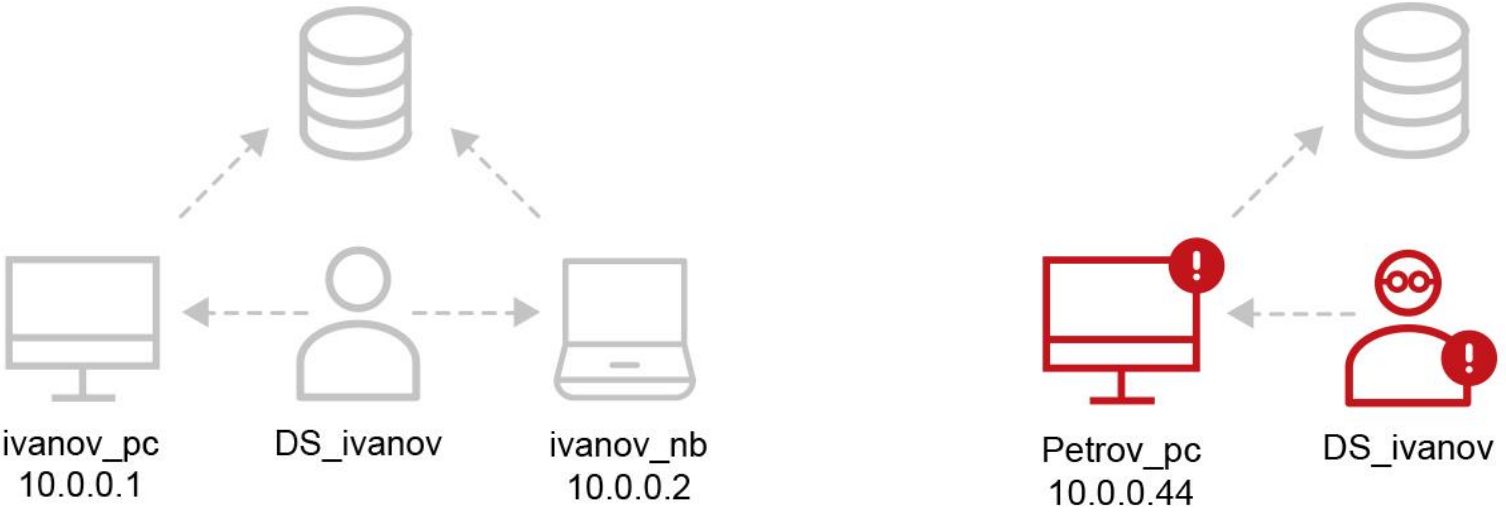
Профиль - это учетная запись, IP-адрес, имя компьютера, доменная УЗ и т. д.



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.

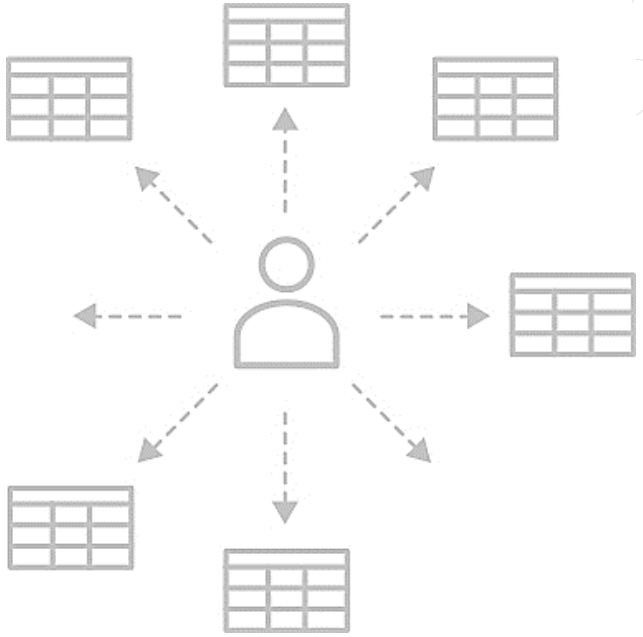


КЕЙС 2. ДОСТУП К ЧУЖОЙ/ИЗБЫТОЧНОЙ ИНФОРМАЦИИ

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

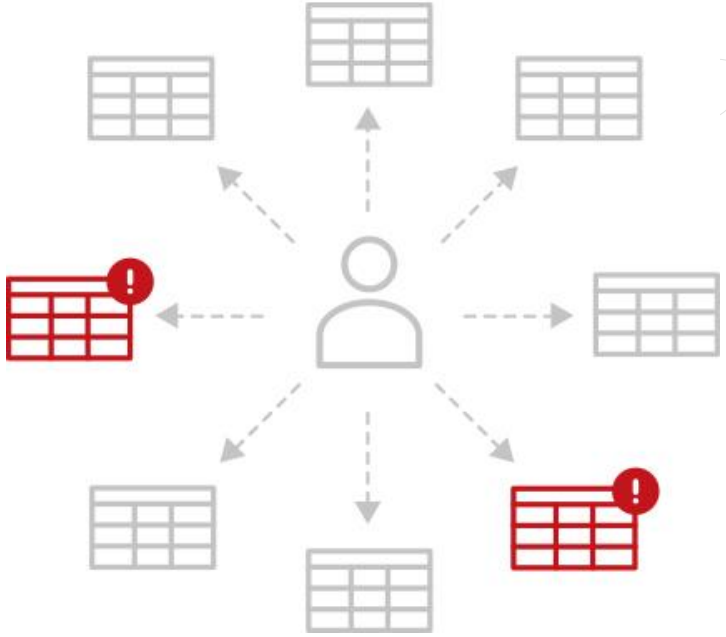
ГАРДА БД

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.

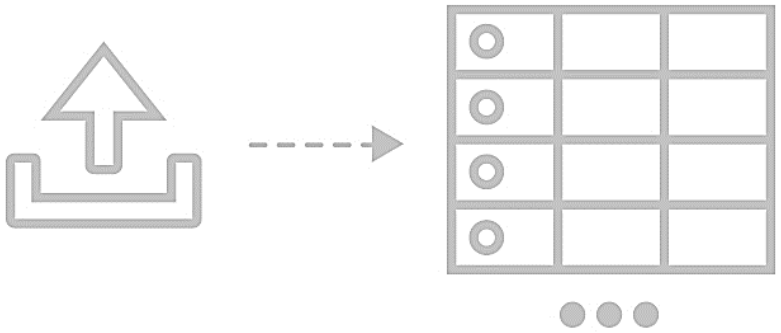
КЕЙС 3. КОЛИЧЕСТВЕННАЯ АНАЛИТИКА

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

БОЛЬШИЕ ВЫГРУЗКИ

Позволяет выявлять инциденты, как цепочку событий



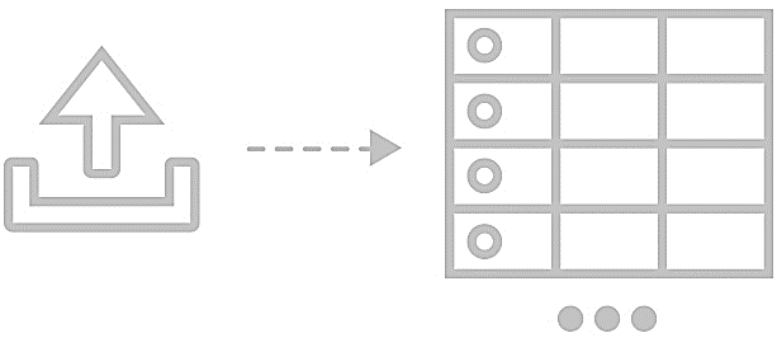
Выгрузка одним запросом

КЕЙС 3. КОЛИЧЕСТВЕННАЯ АНАЛИТИКА

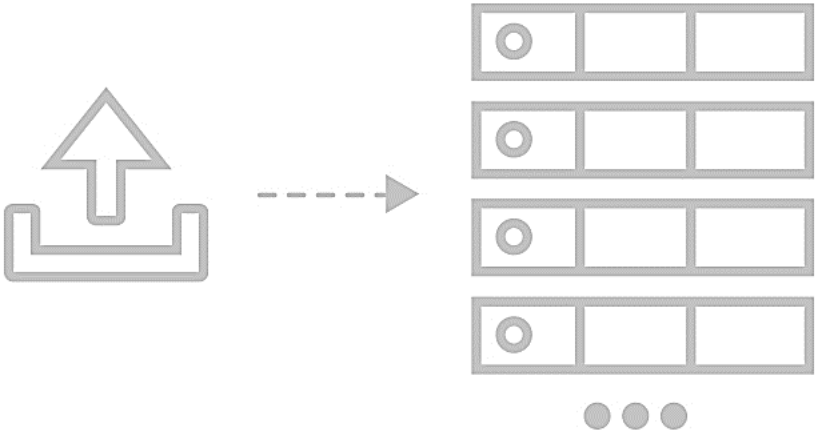
ГАРДА БД
ГАРДА ТЕХНОЛОГИИ

БОЛЬШИЕ ВЫГРУЗКИ

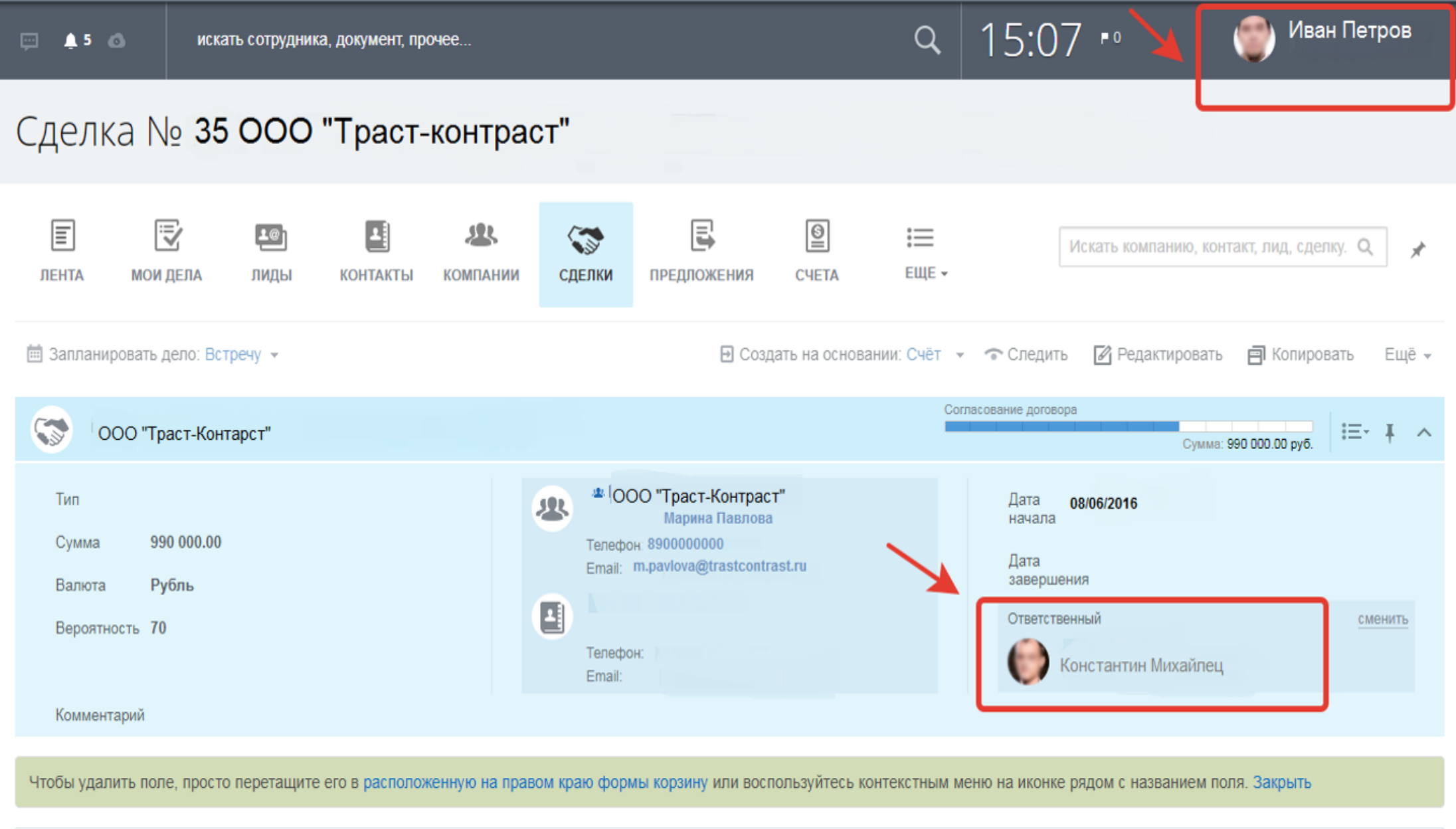
Позволяет выявлять инциденты, как цепочку событий



Выгрузка одним запросом



Выгрузка по частям


5
искать сотрудника, документ, прочее...
15:07
0
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

ГАРДА БД

ГАРДА БД ГАРДА ТЕХНОЛОГИИ

1. Анализ трафика

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

2. Долгосрочное хранение информации

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

3. Поиск баз

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

4. Сканирование баз

Классификация СУБД

Выявление уязвимостей СУБД (неоптимальных настроек)

Построение матриц доступа к СУБД

5. Аналитика/Отчеты + UBA

Выявление нарушения политик безопасности

Отклонения от модели типичного поведения пользователей.

6. Система оповещения.

Дашборды, уведомления о событиях по e-mail, передача данных во внешние SIEM-системы

СПАСИБО
ЗА ВНИМАНИЕ!

ГАРДА БД

ГАРДА ТЕХНОЛОГИИ

info@gardatech.ru
8 (831) 422 12 21
gardatech.ru