



ГАРДА
ТЕХНОЛОГИИ

Поведенческая аналитика при защите баз данных

Сергей Добрушский
14.02.2018

ПРЕДПОСЫЛКИ ТЕХНОЛОГИЙ АВТОМАТИЗАЦИИ

- Рост количества событий ИБ (цифровизация, переход к большим данным);
- Рост качественного уровня угроз/атак;
- Кадровый голод на рынке ИБ.



ПОДХОД ТРАДИЦИОННЫХ СИСТЕМ МОНИТОРИНГА



Compliance и решение внутренних задач ИБ

Правила белых/черных списков

- Где? (Критичная информация)
- Кто?
- Как, Когда, Ценность информации

Тотальная запись

- ретроспективный анализ

ПЛЮСЫ И МИНУСЫ

Плюсы

- + База для ретроспективного анализа;
 - + Низкие затраты на внедрение ИБ системы;
 - + Удовлетворение части нормативных требований.
-

Минусы

- Низкая эффективность выявления и расследования инцидентов;
- Необходимость постоянной актуализации/адаптации политик.



*По статистике в систему мониторинга
БД банка в день может поступать
~ 100 000 000 событий*

АЛЬТЕРНАТИВА: АВТОМАТИЗАЦИЯ



- UBA – выявление отклонений на основании поведенческой аналитики.
- Выявление атак/краж данных на ранних этапах (разведка).
- Действия пользователей прикладных систем – основная составляющая внутреннего фрода.

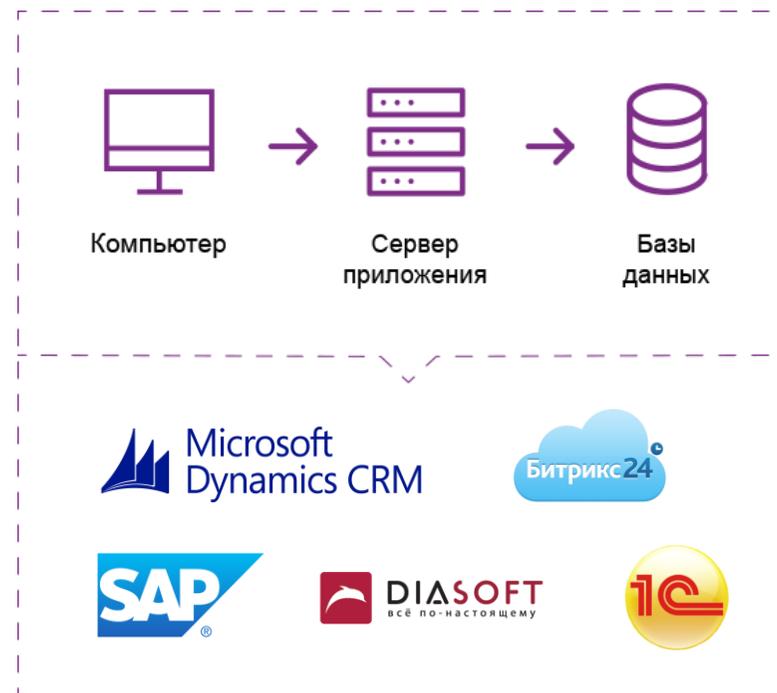
МОНИТОРИНГ АКТИВНОСТЕЙ В ПРИКЛАДНЫХ СИСТЕМАХ

Основная защищаемая система – это:

- клиентское ПО (браузер, десктоп);
- сервер приложения;
- сервер БД;

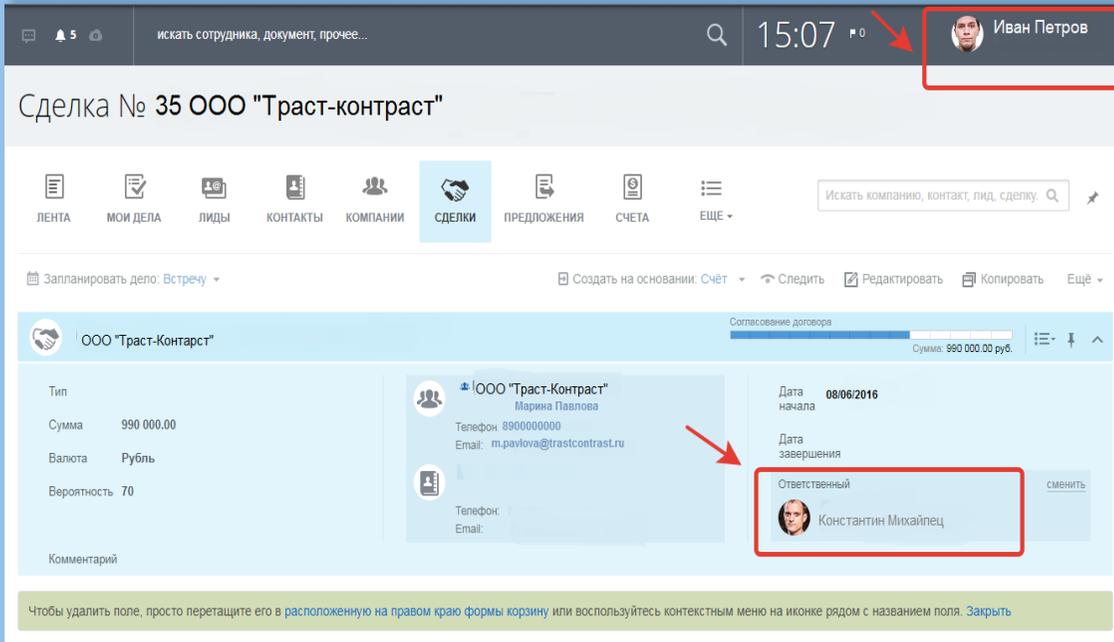
Действия пользователей –
авторизации, sql, http запросы, ответы

Базовые политики – большие выгрузки
из СУБД, Действия администраторов,
Доступ к КИ



ПРАКТИЧЕСКИЙ КЕЙС. ПЕРЕМАНИВАНИЕ «ГОРЯЧИХ» КЛИЕНТОВ

- Поиск по CRM «горячих» сделок, передача конкурирующей организации.
- Мотив – конфликтные отношения в компании.
- Ущерб ~15 млн рублей в год.



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-Контраст"

Согласование договора

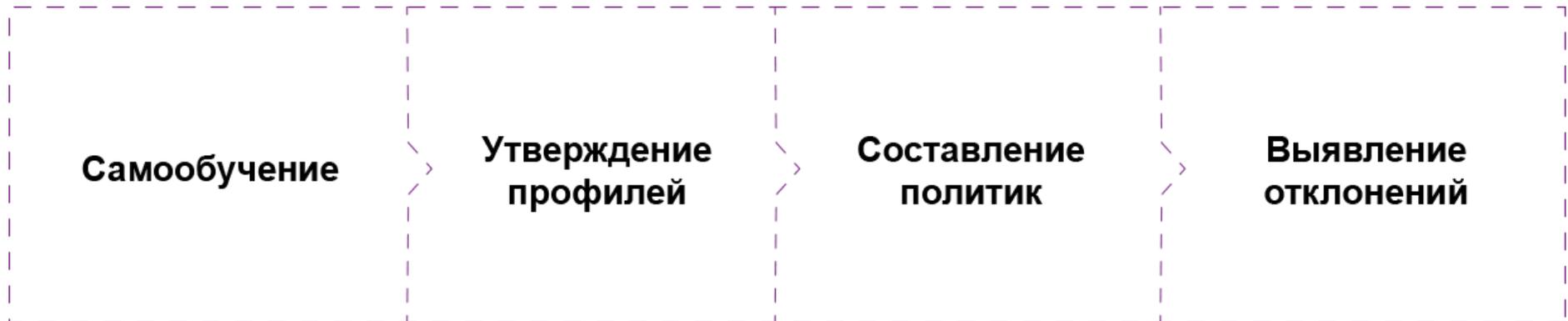
Сумма: 990 000 00 руб.

Тип		ООО "Траст-Контраст" Марина Павлова Телефон: 89000000000 Email: m.pavlova@trastcontrast.ru	Дата начала: 08/06/2016
Сумма	990 000.00		Дата завершения
Валюта	Рубль		Ответственный: Константин Михайлец
Вероятность	70		Сменить
Комментарий			

Чтобы удалить поле, просто перетащите его в расположенную на правом краю формы корзину или воспользуйтесь контекстным меню на иконке рядом с названием поля. Закрыть

ПРИНЦИП РАБОТЫ МОДУЛЕЙ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

UBA строится по принципу динамического профилирования



ПРИНЦИП РАБОТЫ МОДУЛЕЙ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

Профили включают в себя следующие данные:

- Кто (login, ip, компьютеры, приложения);
- Куда (базы данных, таблицы, поля, типы данных);
- Что (запросы к данным, к структуре БД, к правам пользователей);
- Как часто, сколько (объемы запросов, ответов, кол-во запросов).

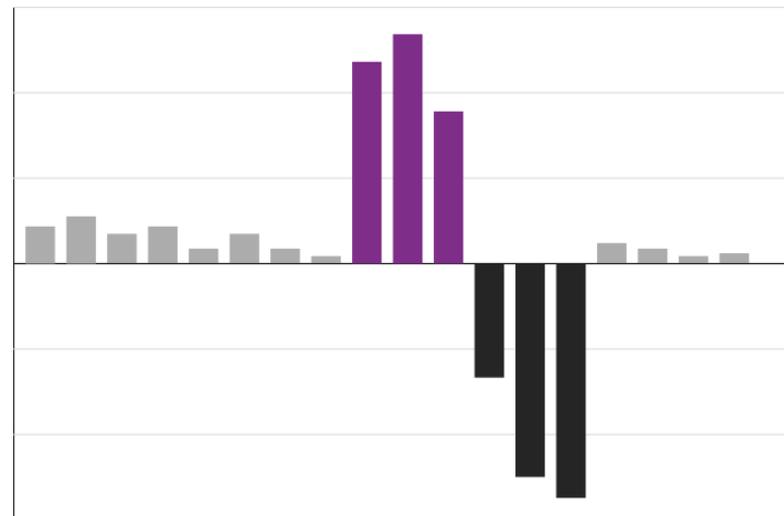
Изменение профиля пользователя



КАК ЭТО ПОМОГАЕТ ВЫЯВЛЯТЬ МОШЕННИКОВ?

Что можно найти:

- Выявление фактов злоупотребления правами.
- Нахождение “любопытных” сотрудников.
- Обнаружение крупных утечек данных (в том числе много маленьких запросов).
- Выявление “общих” либо скомпрометированных учетных записей.
- Ошибки при настройке прав доступа.



- Аномально высокий показатель
- Средний показатель
- Аномально низкий показатель



Широкий охват
внедрений решений ИБ



ГАРДА
ТЕХНОЛОГИИ



Разработка систем
высокой сложности
с 2005 года



Собственная
технологическая
платформа



Более 100 высоко-
квалифицированных
специалистов



ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ

Февраль 2018 © ГАРДА Технологии