ГАРДА
ТЕХНОЛОГИИ

Поведенческая аналитика при защите баз данных

Сергей Добрушский
14.02.2018

ПРЕДПОСЫЛКИ ТЕХНОЛОГИЙ АВТОМАТИЗАЦИИ

ГАРДА ТЕХНОЛОГИИ

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

ПОДХОД ТРАДИЦИОННЫХ СИСТЕМ МОНИТОРИНГА

ГАРДА ТЕХНОЛОГИИ

Complience и решение внутренних задач ИБ

Правила белых/черных списков

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

Тотальная запись

- ретроспективный анализ

ПЛЮСЫ И МИНУСЫ

ГАРДА ТЕХНОЛОГИИ

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

ГАРДА ТЕХНОЛОГИИ

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

МОНИТОРИНГ АКТИВНОСТЕЙ В ПРИКЛАДНЫХ СИСТЕМАХ

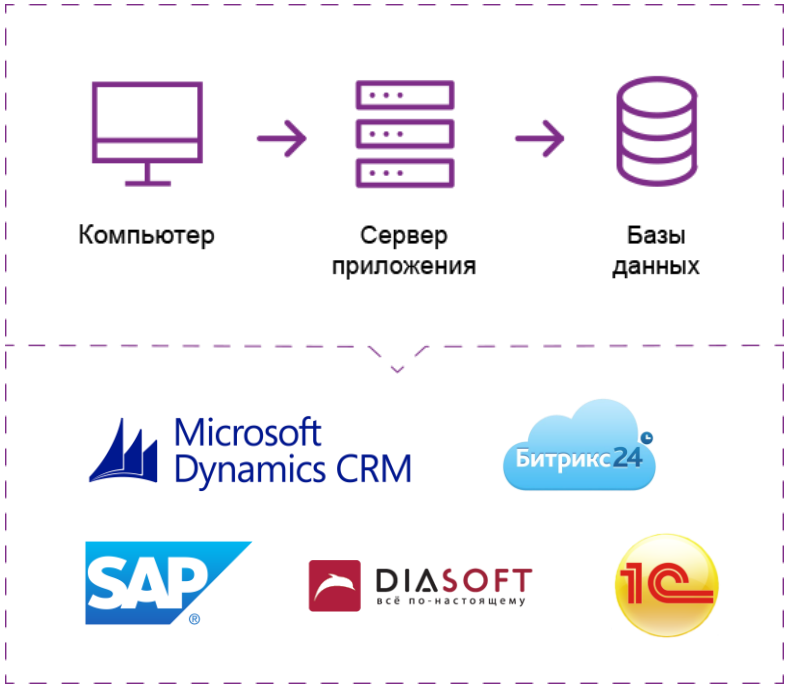
ГАРДА ТЕХНОЛОГИИ

Основная защищаемая система – это:

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

Действия пользователей – авторизации, sql, http запросы, ответы

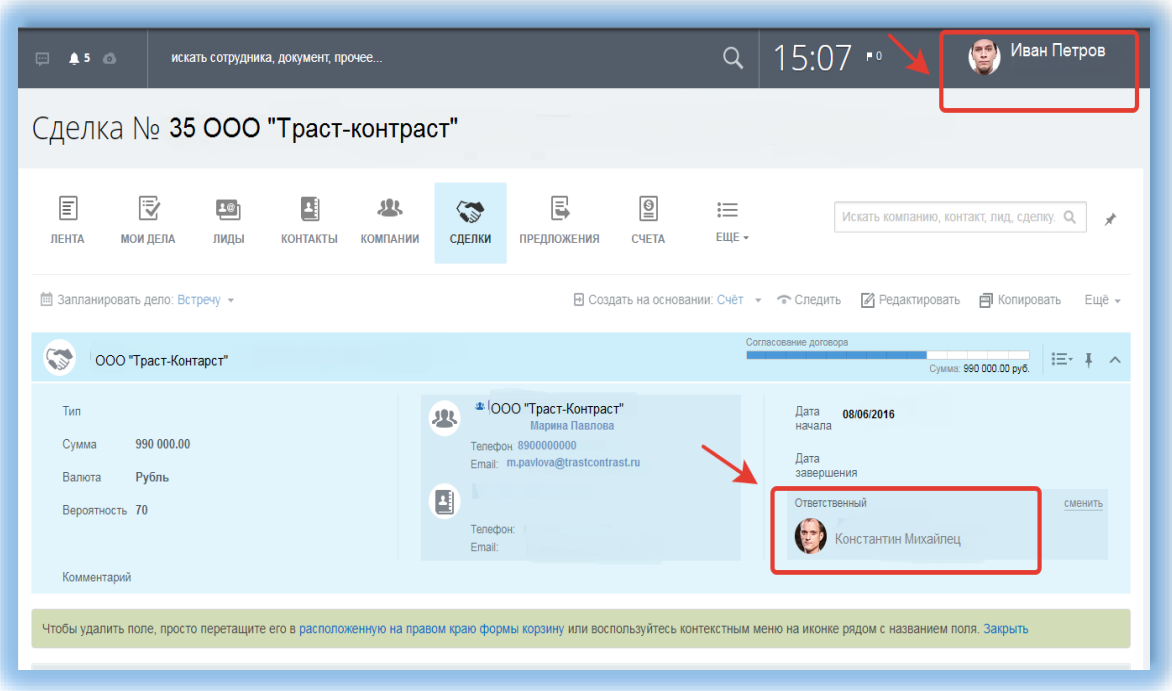
Базовые политики – большие выгрузки из СУБД, Действия администраторов, Доступ к КИ



ПРАКТИЧЕСКИЙ КЕЙС. ПЕРЕМАНИВАНИЕ «ГОРЯЧИХ» КЛИЕНТОВ

ГАРДА ТЕХНОЛОГИИ

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



ПРИНЦИП РАБОТЫ МОДУЛЕЙ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

ГАРДА ТЕХНОЛОГИИ

UBA строится по принципу динамического профилирования

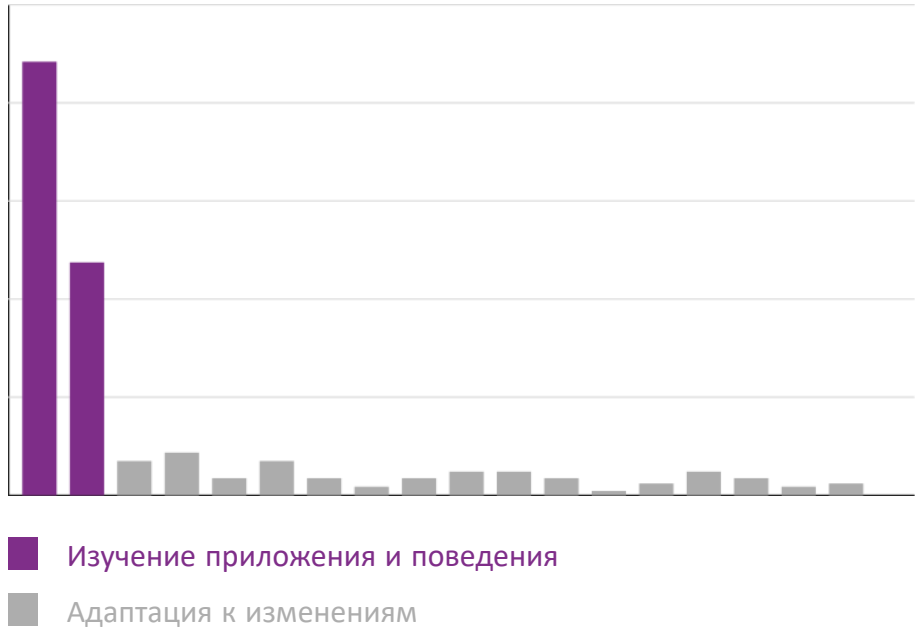
ПРИНЦИП РАБОТЫ МОДУЛЕЙ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

ГАРДА ТЕХНОЛОГИИ

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

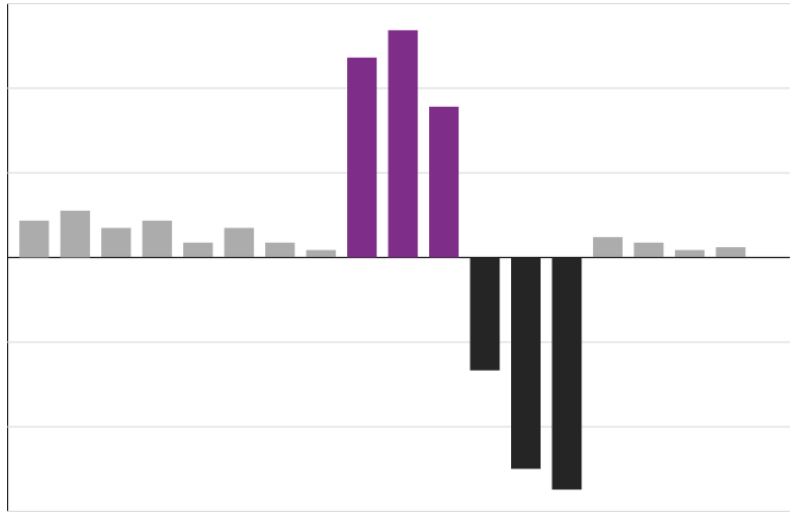


КАК ЭТО ПОМОГАЕТ ВЫЯВЛЯТЬ МОШЕННИКОВ?

ГАРДА ТЕХНОЛОГИИ

Что можно найти:

- Выявление фактов злоупотребления правами.
- Нахождение “любознательных” 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

ГАРДА
ТЕХНОЛОГИИ

Широкий охват
внедрений решений ИБ

Разработка систем
высокой сложности
с 2005 года

Собственная
технологическая
платформа

Более 100 высоко-
квалифицированных
специалистов

ГАРДА
ТЕХНОЛОГИИ

СПАСИБО ЗА ВНИМАНИЕ