10 YEARS JETSECURITY CONFERENCE 2019

ИЩИТЕ ОТВЕТЫ… ИЛИ КАК РАСШИРИТЬ ФУНКЦИОНАЛ DAM

Андрей Черных
Руководитель группы внедрения систем мониторинга и защиты приложений
Главный по DAMам
achernikh@jet.su

ЧТО ЕЩЕ ЗА DAM?

#DAM (Database Activity Monitoring) –
средство мониторинга активности пользователей в БД
и выявления инцидентов

КЛАССИЧЕСКИЙ ФУНКЦИОНАЛ

- Контроль администраторов
- Контроль критичных данных
- Контроль критичных операций

ПОПУЛЯРНЫЕ РЕШЕНИЯ

- Imperva DAM
- IBM Guardium

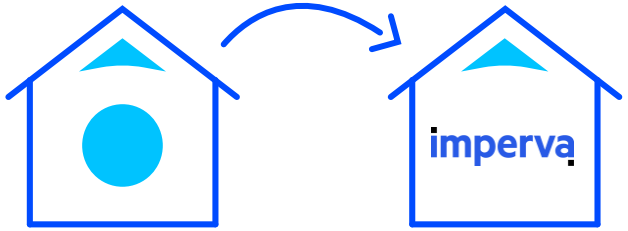
ЗАКАЗЧИК

Один из крупнейших РЕГИОНАЛЬНЫХ банков

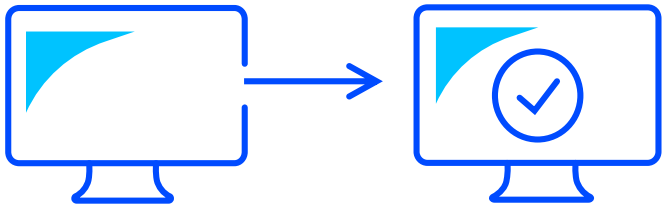
Бережное отношение к безопасности клиентов

Давний партнер «Инфосистемы Джет»

ЦЕЛЬ ПРОЕКТА

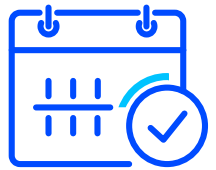


Заменить имеющийся DAM на Imperva DAM



Перенести всю логику работы

Реализовать функционал поиска сотрудников, обращавшихся к клиенту



Срок - неделя

ПОИСК СОТРУДНИКОВ, ОБРАЩАВШИХСЯ К КЛИЕНТУ

- Есть подозрение на мошенничество с данными клиента
- Данные клиентов доступны сотрудникам банка
- Нужно найти сотрудника, обращавшегося к данным клиента
- Необходимо провести расследование

ОСОБЕННОСТИ ЗАДАЧИ

- Заранее клиент НЕ ИЗВЕСТЕН
- Об инциденте становится известно спустя несколько дней/недель
- При обращении к данным клиента не всегда используются уникальные значения

ДЛЯ РЕШЕНИЯ ТРЕБУЕТСЯ

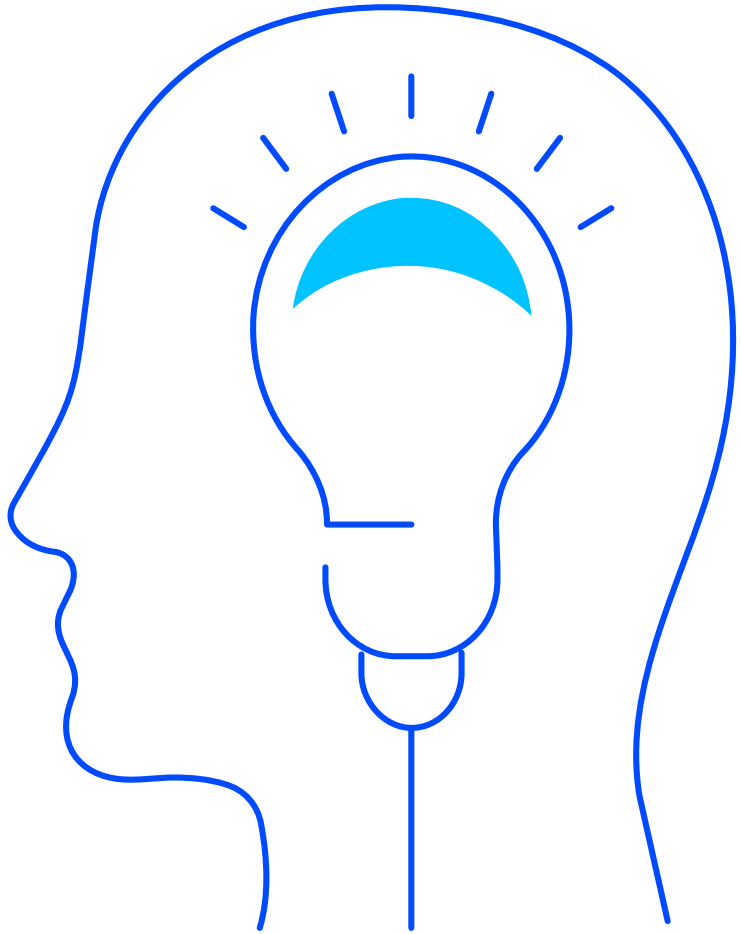
- Сохранять запросы БД
- Сохранять ответы БД
- Искать в ответах

ПРОБЛЕМА

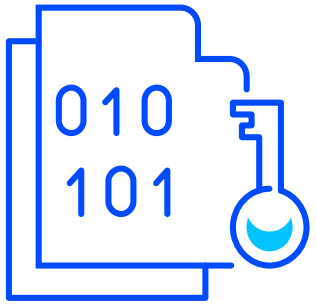
Imperva сохраняет ответы SQL-запросов,
но не умеет по ним искать

ВОЗМОЖНЫЕ РЕШЕНИЯ

- ~~Запрос на доработку ПО~~
- ~~Отправка ответов БД в Splunk~~
- Придумать свое решение



ПЕРВЫЙ ВАРИАНТ



Поиск по ключевому значению

Поиск данных за определенный период

ИВАНОВ	ИВАН	НИКОЛАЕВИЧ	г.Оренбург
ИВАНОВ	ИВАН	ДМИТРИЕВИЧ	г.Саратов
ИВАНОВ	ПЕТР	ПЕТРОВИЧ	г.Выборг
ИВАНОВ	НИКОЛАЙ	ВАСИЛЬЕВИЧ	г.Тверь
ИВАНОВ	ПОРФИРИЙ	КОРНЕЕВИЧ	с.Ореховка

ВТОРОЙ ВАРИАНТ

Поиск
по трем
значениям в
одной строке

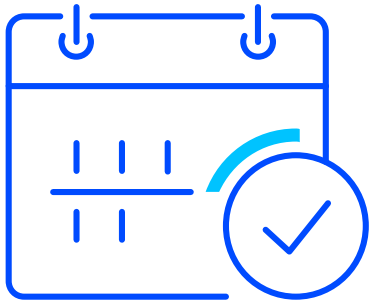
Регистронезависимый
поиск

Поиск
с использованием
регулярного
выражения

РЕЗУЛЬТАТЫ

Построен
новый DAM

Реализован поиск
сотрудников,
обращавшихся
к данным клиента



Срок – **5** дней

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Андрей Черных

Руководитель группы внедрения систем мониторинга и защиты приложений

Главный по DAMам

achernikh@jet.su