

# JET SECURITY CONFERENCE



## VIII ежегодная конференция Центра информационной безопасности

1-2 июня 2017 года

[WWW.JET.SU](http://WWW.JET.SU)

Radisson BLU



IMPERVA



POSITIVE TECHNOLOGIES

tufin

FORTINET



TRAPX  
SECURITY

ONE IDENTITY

RAPID7





## Секция



JET Detective:  
обзор решения в кейсах и технических  
деталях



Шире чем антифрод: AML, контроль  
операционных рисков и GRC на базе Jet  
Detective



PHDays: Первый антифрод на защите  
платежной активности виртуального  
города





**JET** CONFERENCE

01/06/2017

## JET DETECTIVE

Алексей Сизов,  
рук. направления решений по борьбе  
с мошенничеством



## Обзор

- Почему мы создали решение на столь конкурентном рынке
- Каковы наши отличия от конкурентов
- Какие выгоды дает наша разработка





# JET

CONFERENCE

Проблематика



Цель



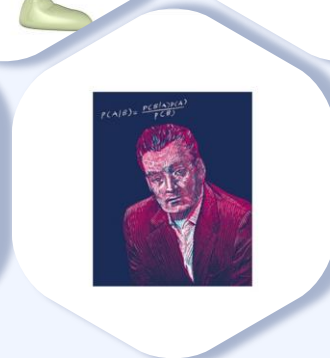
Задачи



Технологии



Методы



Экспертиза





**JET**  
CONFERENCE

**2017**

**JET DETECTIVE**

**LOADING...**



## Антифрод сегодня



Антифрод эффективен когда элементы ИБ становятся компонентами бизнес-процесса, и их эффективность оценивается влиянием на бизнес, удобство клиентов, достижение SLA



## Ключевые характеристики



- Обработка данных
- Создание и тестирование правил
- Принятия решений
- Масштабирования



- False positive
- False negative
- Human factors



## Три функциональных уровня

Представление  
данных



Обработка данных



Сбор и хранение  
данных





## Работа с данными



Inmemory



РСУБД



Bigdata



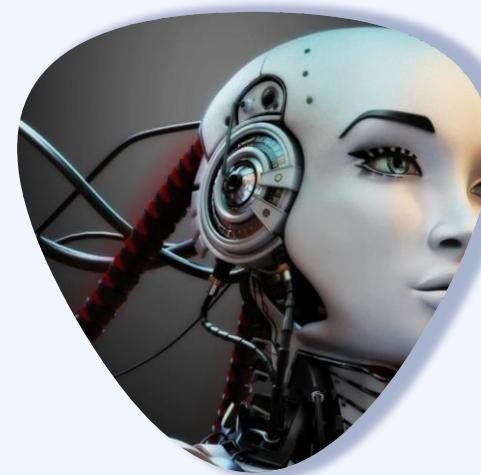
## Работа с данными

- Инструмент проектирования данных
- Инструмент управления данными





## Аналитика



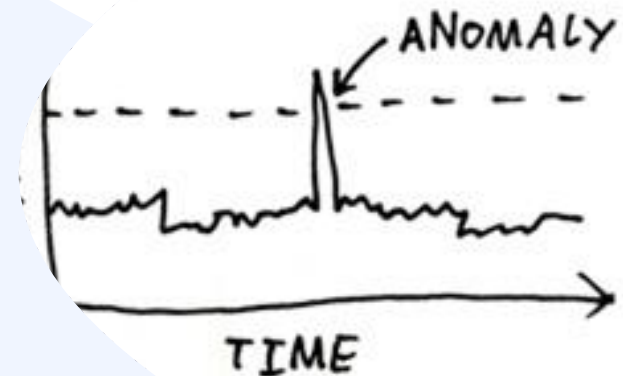
- Создание правил
- Профилирование
- Математическое моделирование



## Аналитика

- Модели с учителем
- Выявление аномалий
- Контроль процессов и технологий

nlc  
**XGBoost**





## Инструмент, а не серебряная пуля

- Оверфитинг
- Производительность
- Выбор метрики качества



## Расследование

- Анализ любых данных в одном окне
- Схема многопользовательской работы



- Механизмы визуального анализа
- SOON: система отчетности





## Выгода

- «Нет» массовому использованию реляционных СУБД
- Свобода выбора оборудования





## Выгода

- Создание правил по обработке событий в интерфейсе
- Моделирование правил на базе деревьев решений
- Управление моделью обучения на базе PMML





## Выгода

- Скорость принятия решения и тюнинга системы
- Моделирование не только риска, но действий при его наступлении
- Полная картина в едином инструменте





**JET** CONFERENCE

00/00/2017

**ИНФОСИСТЕМЫ ДЖЕТ**

Спасибо за внимание!