# JET SECURITY CONFERENCE

## VIII ежегодная конференция
## Центра информационной безопасности

1-2 июня 2017 года

WWW.JET.SU

Radisson BLU

Check Point SOFTWARE TECHNOLOGIES LTD
Premier Business Partner IBM
Hewlett Packard Enterprise
f5
IMPERVA
SKYBOX SECURITY
INFOWATCH МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ
TREND MICRO
paloalto NETWORKS
FireEye
KASPERSKY PLATINUM PARTNER
POSITIVE TECHNOLOGIES
tufin
FORTINET
SOLAR SECURITY software&services
CYBERARK
TRAPX SECURITY
ONE IDENTITY
RAPID7
iDeals VIRTUAL DATA ROOM

JET CONFERENCE

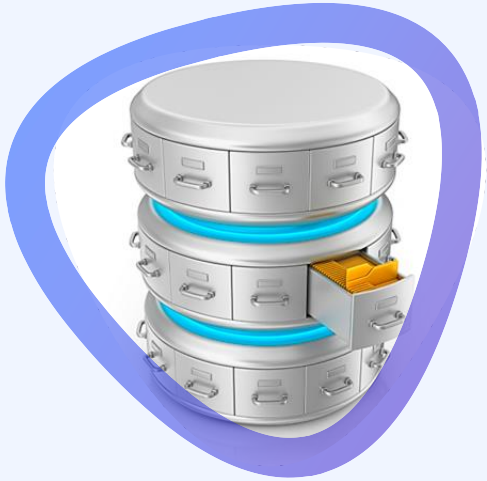
01/06/2017

# Шире чем антифрод

Евгений Колесников, руководитель направления

# Решение, а не продукт


**Бизнес-объекты**



**Единое хранилище**

**Complex Event Processing**

JET

CONFERENCE

# Контроль рисков: Проблематика

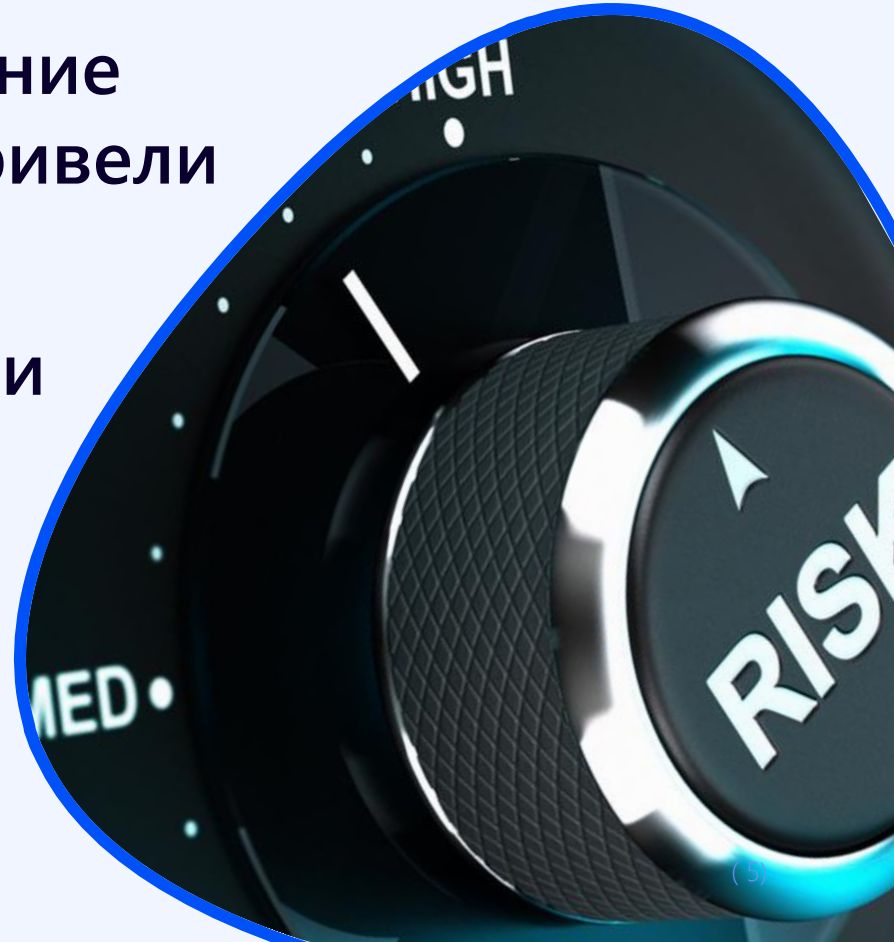
- **Стоимость рисков считается вручную**
- **Цепочки связанных событий не отслеживаются**
- **Ведение реестра рисков происходит вручную**

JET

CONFERENCE

# Контроль рисков: Решение

- **Настройка правил контроля рисков**
- **Автоматическое связывание с событиями, которые привели к реализации**
- **Предсказание реализации риска**



JET

CONFERENCE

# Контроль рисков: Кейс

- **Ретейл, свой логистический центр**
- **Ломается техника на рейсе, простой склада и магазина**

JET

CONFERENCE

# Результат

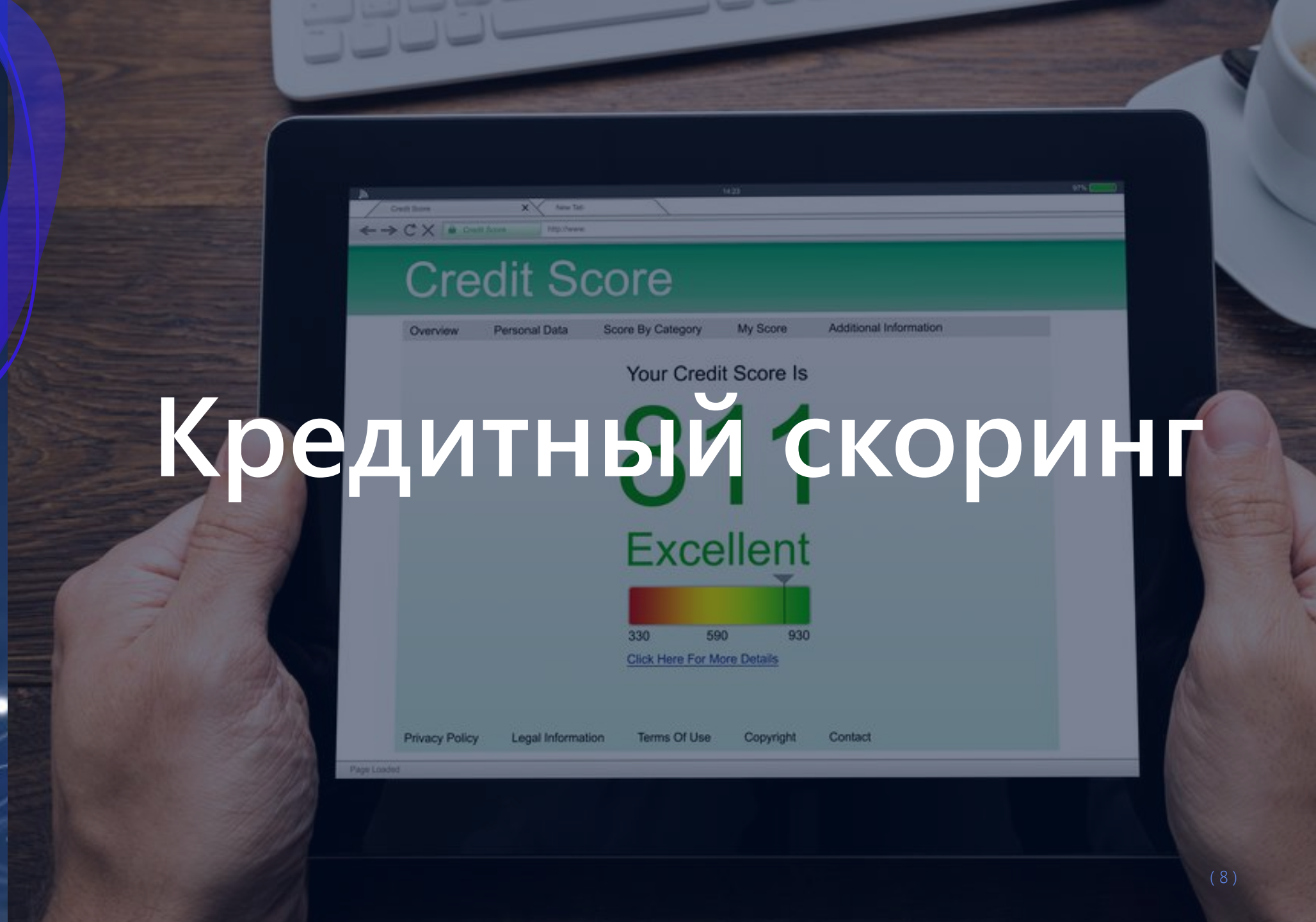
**Прогнозирование выхода из строя техники:**

- **по текущему состоянию, заявкам на обслуживание,**
- **мелким поломкам,**
- **задержкам на рейсе**

JET

CONFERENCE

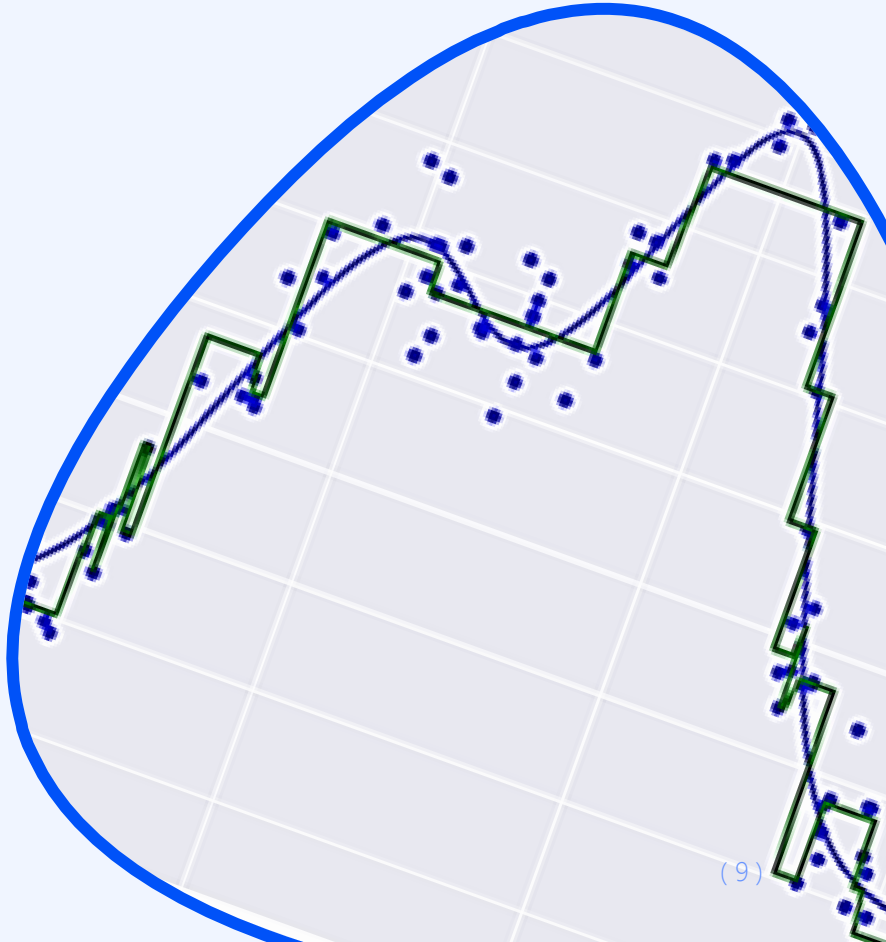
# Кредитный скоринг



JET
CONFERENCE

# Кредитный скоринг: Решение

- **Единое хранилище информации**
- **Скоринговая модель на основании ВСЕХ данных**
- **Использование современных методов ML**



# Кредитный скоринг: Кейс

**Вводные:**

- **10 000 заявок на кредит**
- **Просрочка до 3-х месяцев**

# Результат

- AUROC:
  - ✓ Человек – 0.7934
  - ✓ Машина – 0.7756
- GINI: 0.5869

JET
CONFERENCE

# ПОД/ФТ: Проблематика

- Это не мошенничество
- Много правил содержит слова: похоже, подобный и т.д.
- Нужно искать не конкретное событие, а цепочки

# ПОД/ФТ: Решение

- Контроль за каждым событием в режиме, близком к реальному
- Поиск «похожих» объектов при помощи ML
- Обработка всех событий ежесуточно правилами и ML

# ПОД/ФТ: Кейс

- Много переводов с разных карт на одну
- Выводы на крупную сумму с одной карты
- «Нормальные» платежи с карты дропера

JET
CONFERENCE

# Решение

- Ручное выявление нескольких случаев
- Построение модели на базе найденных случаев
- Ежедневная проверка

JET

CONFERENCE

# Контроль за бизнес-процессом

- БП не формализованы
- Есть workaround процессы
- Уязвимости БП используют при мошенничестве

JET
CONFERENCE

# Контроль за бизнес-процессом: Решение

- **Сбор логов активности сотрудника и систем**
- **Контроль за аномальным поведением**
- **Аналитический поиск процессов**

# Контроль за бизнес-процессом: Кейс

- **Производственная линия стали**
- **Умышленное «допущение» в объеме компонентов сплава**
- **Бракованная сталь продается по цене лома**

# Решение

- **Прогноз брака еще на этапе сбора сплава**
- **Реакция на инцидент еще до начала плавки**

JET CONFERENCE

01/06/2017

# ИНФОСИСТЕМЫ ДЖЕТ

Спасибо за внимание!