# КРОК

КАК В НОВЫХ УСЛОВИЯХ
СОХРАНИТЬ
## БЕЗОПАСНОСТЬ

**МАРСЕЛЬ АЙСИН,**
Эксперт по информационной безопасности

# ЧТО ИЗМЕНИЛОСЬ

## Статистика нашего Security Operation Center

Злоумышленнику стало проще скрыть свои действия в числе легитимных, так как поведение сотрудников и подрядчиков изменилось

Число средств удаленного подключения с большей вероятностью позволяют злоумышленнику остаться незамеченными

Вектор фишинговых атак на почтовые клиенты домашних компьютеров сотрудников приобрел новую силу

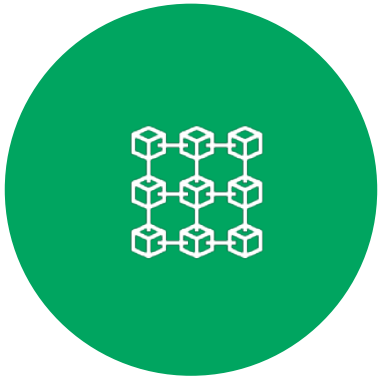
Значительно увеличилось количество вирусных проникновений в корпоративную инфраструктуру

# РЕШЕНИЕ

## Безопасность через мониторинг аномалий с применением поведенческой аналитики в Security Operation Center

**Профилирование**
на сетевом уровне

**Анализ обращений**
к веб-серверам, базам данных, файловым ресурсам



Обнаружение аномалий на уровне **бизнес-систем**

# ВАРИАНТЫ ПРИМЕНЕНИЯ

## Профилируем поведение каждого пользователя и узла сети

Частота действий (событий) + Типы действий + Результат действий + Источник событий (хосты, geo-метки)

## Добавляем переменную времени

Сумма событий за час\день\неделю\месяц + День недели при генерации событий + Пики\спады количества событий

## Сравниваем с похожими пользователями и узлами сети

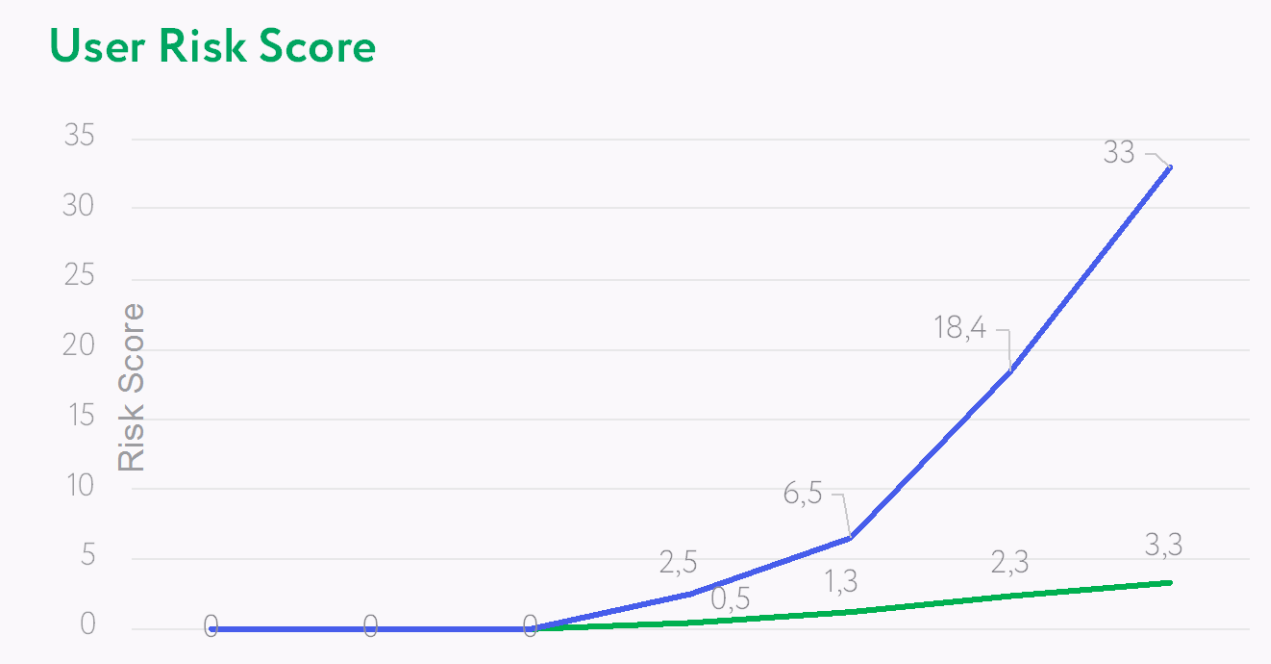
Что делают пользователи с такой же должностью,
в том же месте, с тем же руководителем и т.д.

# ОБНАРУЖЕНИЕ APT-АТАКИ С ПОМОЩЬЮ ПОВЕДЕНЧЕСКОГО АНАЛИЗА

- Ironport: Phishing Anomaly: receives a Phishing email
- Proxy редирект на «outlookscansafe.net»
- Выявлен редкий процесс
- Windows New logon type «10» обнаружен
- Копирование данных на внешний сервер
- Windows: Wevtutil.exe обнаружен.
- Domain controller обнаружил очистку Audit Log.

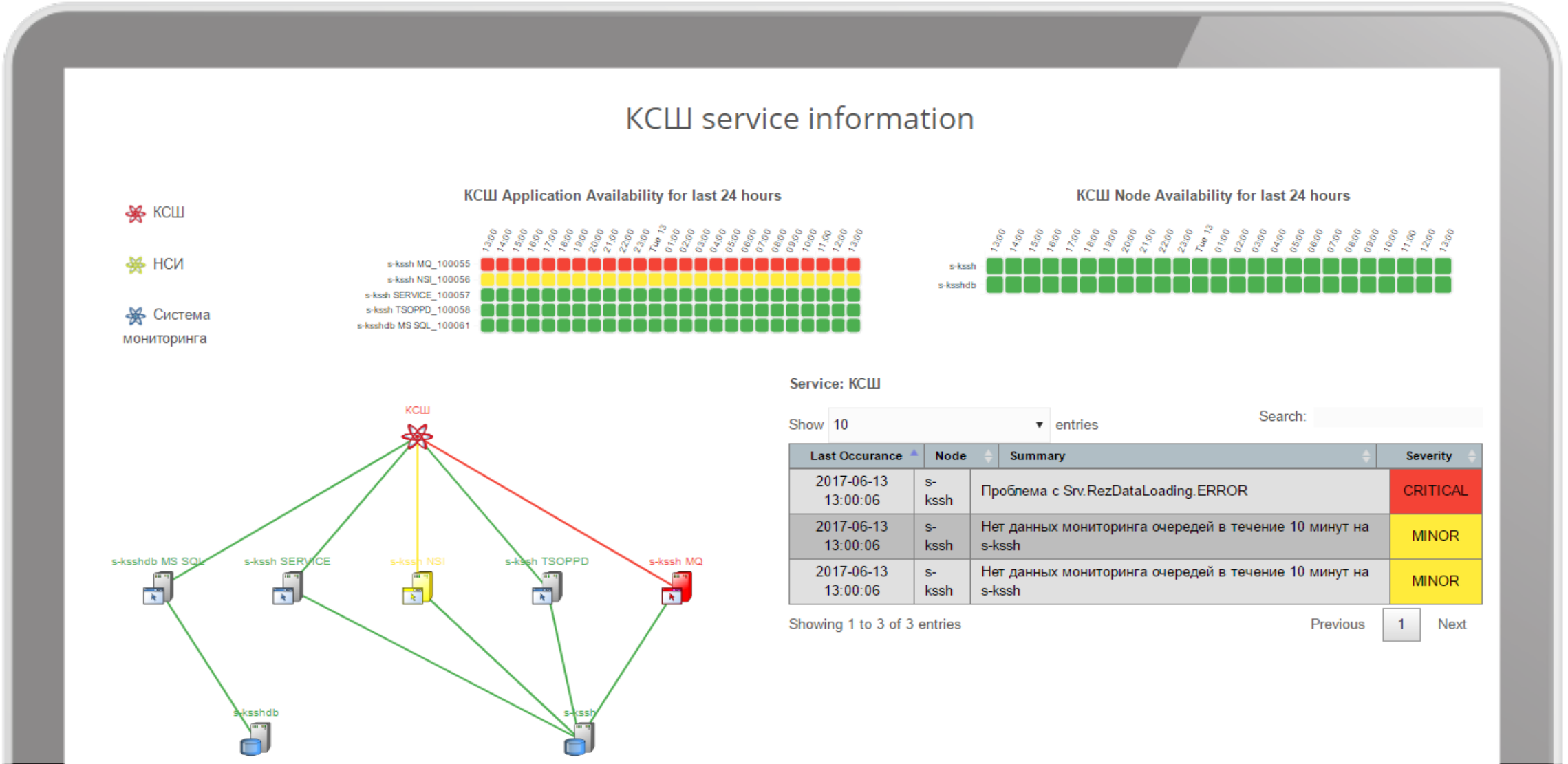
**Модель угрозы:**

Phishing Attack + Suspicious URL+ Rare Process + Anomalous Access + Data Egress + Log Tampering




КРОК

# РАСЧЕТ РЕСУРСНО-СЕРВИСНОЙ МОДЕЛИ С УЧЕТОМ ЗНАЧИМОСТИ АКТИВОВ




# Спасибо за внимание!
# Вопросы?

**maysin@croc.ru**
**+7 495 974 22 74**
**croc.ru**