ThreatMark

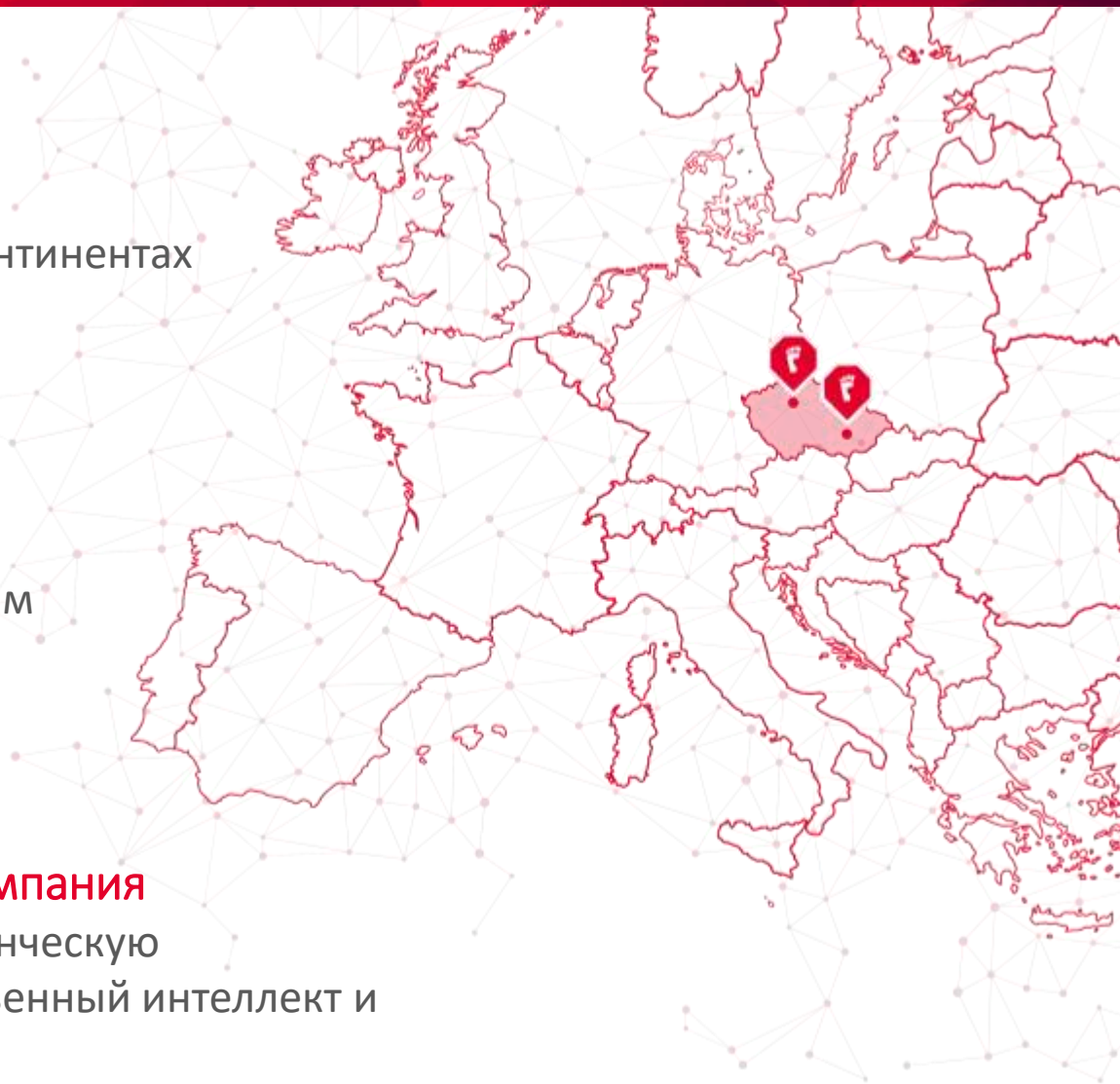
AFS

Антифрод решение для систем ДБО (веб- и мобильный банкинг)

Компания ThreatMark

Основана в 2015
бывшими этическими хакерами

Сделано в Чехии
используется на 4 континентах

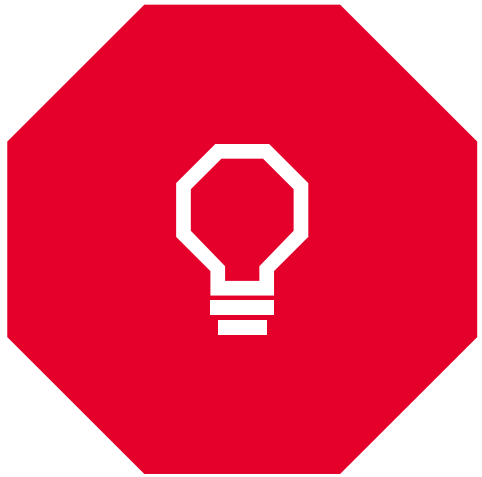


20+ миллионов
клиентов защищено

50+ экспертов
для работы над одним продуктом

Разработано
специально для банков

Инновационная компания
с фокусом на поведенческую биометрию, искусственный интеллект и машинное обучение



С чем банки сталкиваются сегодня

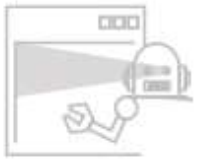
Атаки на клиентов и кража денег в онлайн банкинге

Банковские трояны

Социальная инженерия

Кража личности

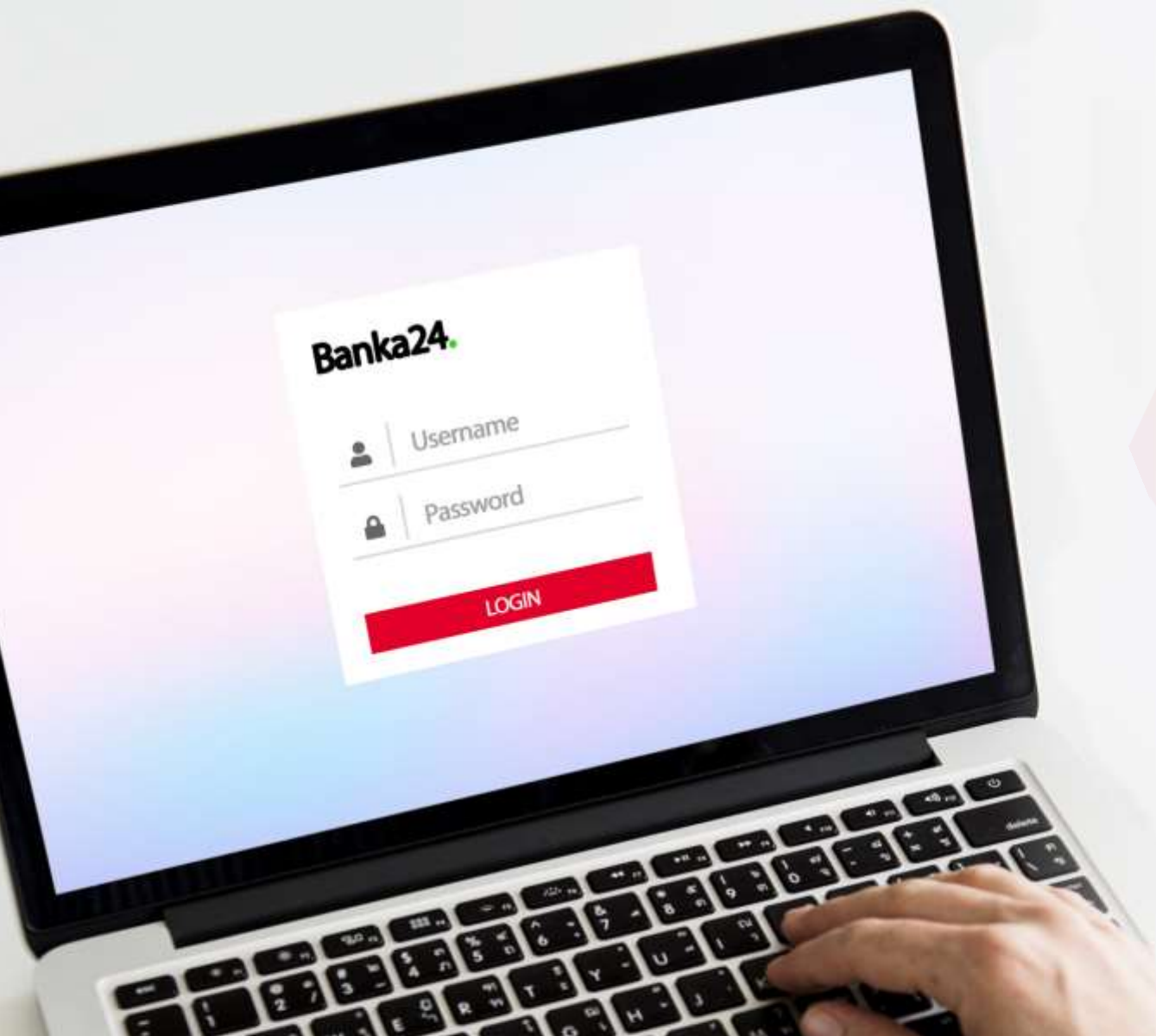
Фишинг



Боты и веб-скрапинг

Атаки на мобильный банкинг

Неэффективность



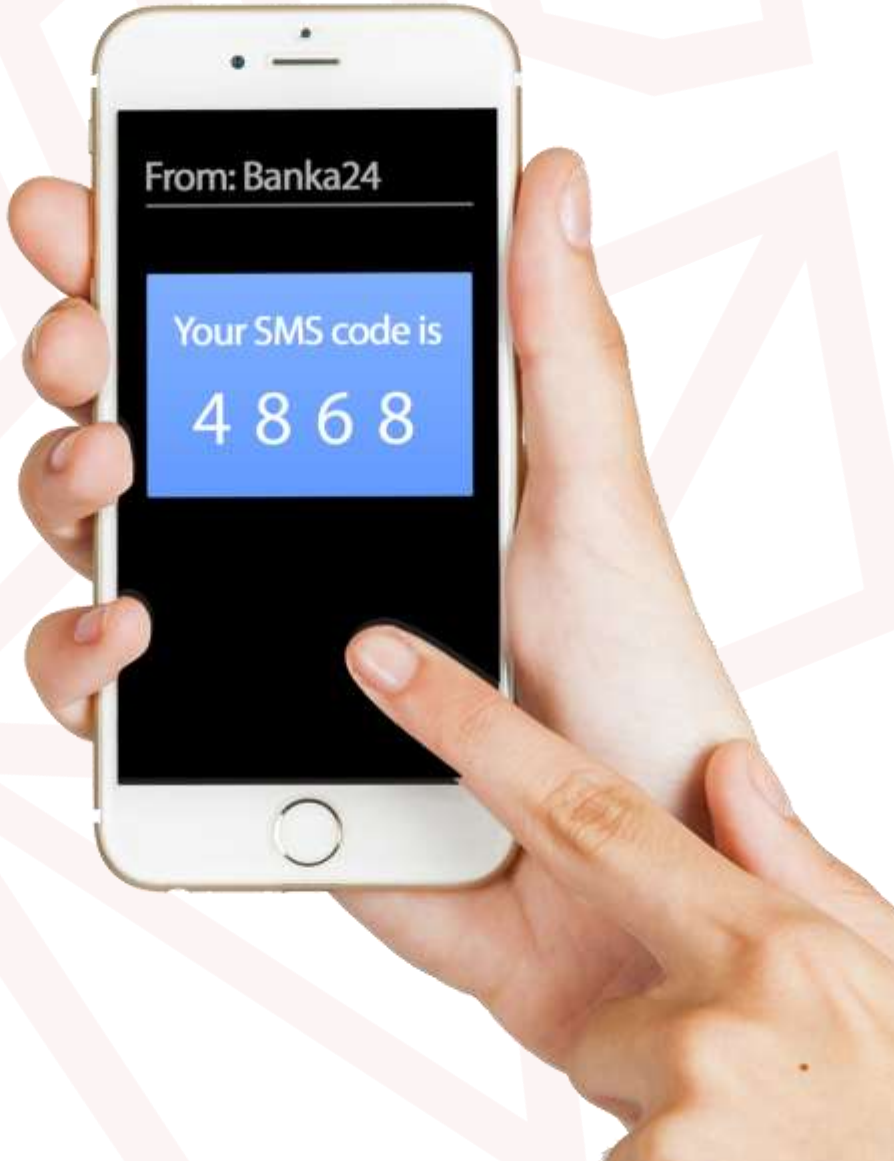
False positives

False negatives

Двухфакторная аутентификация

Затраты на СМС

Неудобство для клиентов

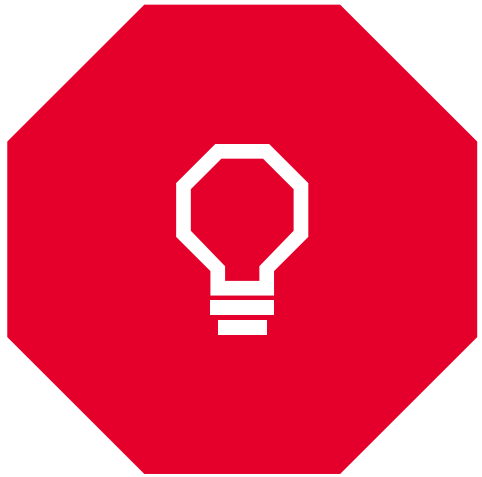


Требования регуляторов

PSD2 (Евросоюз)

BDDK (Турция)

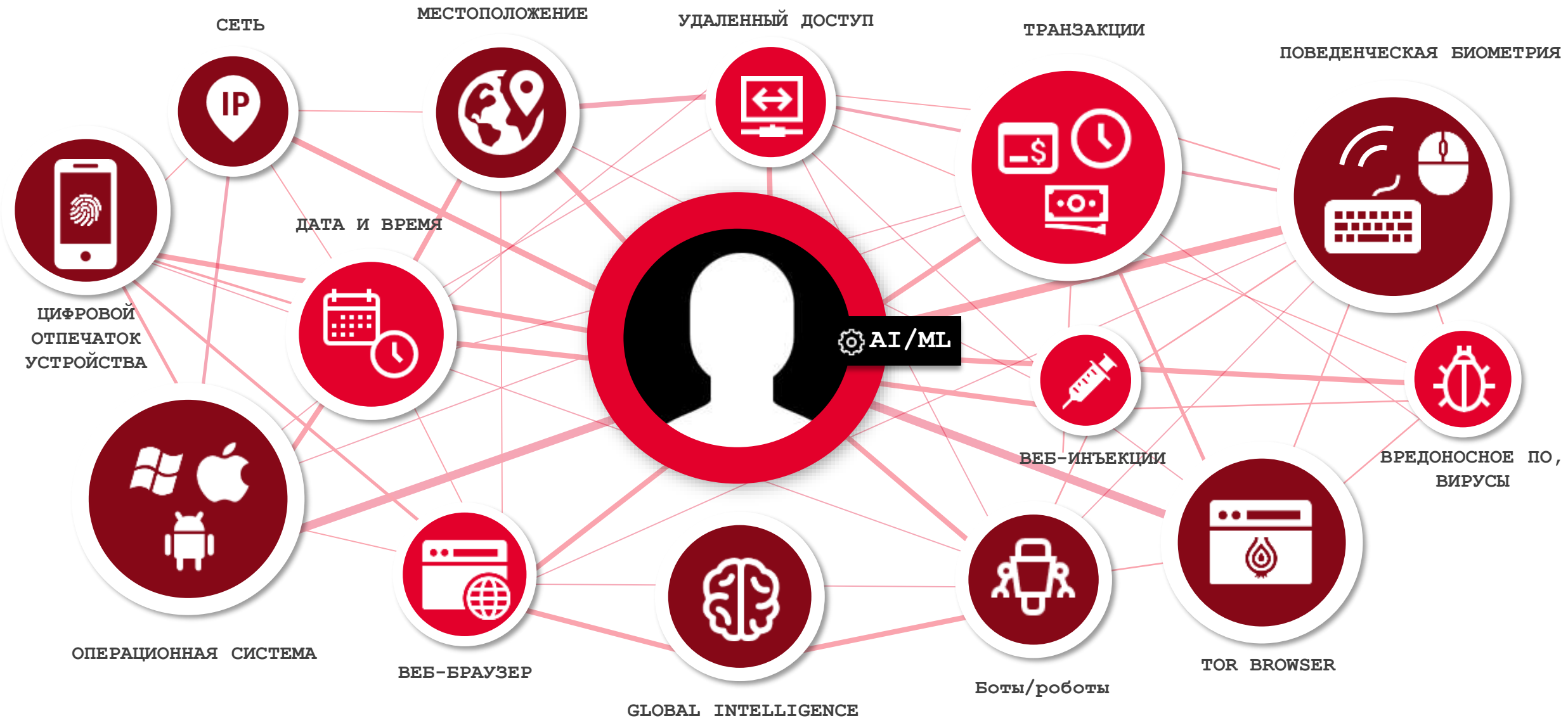
? (Украина)



Антифрод Решение

Комплексная защита интернет и мобильного банкинга

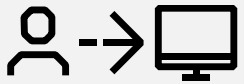
Проверка Цифровой Идентичности



Многоуровневая Безопасность

УРОВЕНЬ 1

УСТРОЙСТВО



Проверка подключения (TOR, анонимайзер)

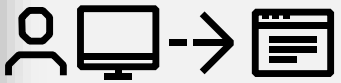
Проверка безопасности браузера и ОС

Обнаружение вредоносного ПО и фишинга

Цифровой отпечаток устройства

УРОВЕНЬ 2

АВТОРИЗАЦИЯ



Проверка геолокации

Проверка времени авторизации

Анализ биометрии

Скорость переходов

Контекстный анализ действий

УРОВЕНЬ 3

НАВИГАЦИЯ

Навигация по приложению

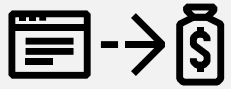
Обнаружение роботов и скриптов

Проверка перехвата сессии

Поведенческая биометрия и взаимодействие с приложением

УРОВЕНЬ 4

ТРАНЗАКЦИИ



Проверка по спискам «денежных мулов»

Анализ транзакций и выявление аномалий

Целостность транзакций

УРОВЕНЬ 5

АНАЛИЗ БОЛЬШИХ ДАННЫХ

Big Data AI/ML

Непрерывное профилирование пользователей

Улучшение алгоритмов на основе обратной связи от банка

Индивидуальные настройки

Уровни защиты согласно Gartner

УРОВЕНЬ 5

Global intelligence: все клиенты пользуются преимуществами Центра обмена информацией об атаках и девайсах

УРОВЕНЬ 4

Межканальная защита: собранные данные оцениваются в контексте всех покрываемых онлайн каналов.

УРОВЕНЬ 3

Защита каналов: каждое ипользование приложения мониторится и оценивается в историческом контексте для данного пользователя

УРОВЕНЬ 2

Защита сессий: все сессии анализируются и оцениваются по многочисленным параметрам

УРОВЕНЬ 1

Защита девайсов: все устройства мониторятся и профилируются

Простая имплементация

AFS веб компонент

Встраивание JavaScript компонента в код веб-приложения

AFS Аналитический сервер

Настройка аналит. сервера (предоставляется в виде виртуальной машины)

Интеграция

Опционально: настройка API для интеграции с внутренними и сторонними системами

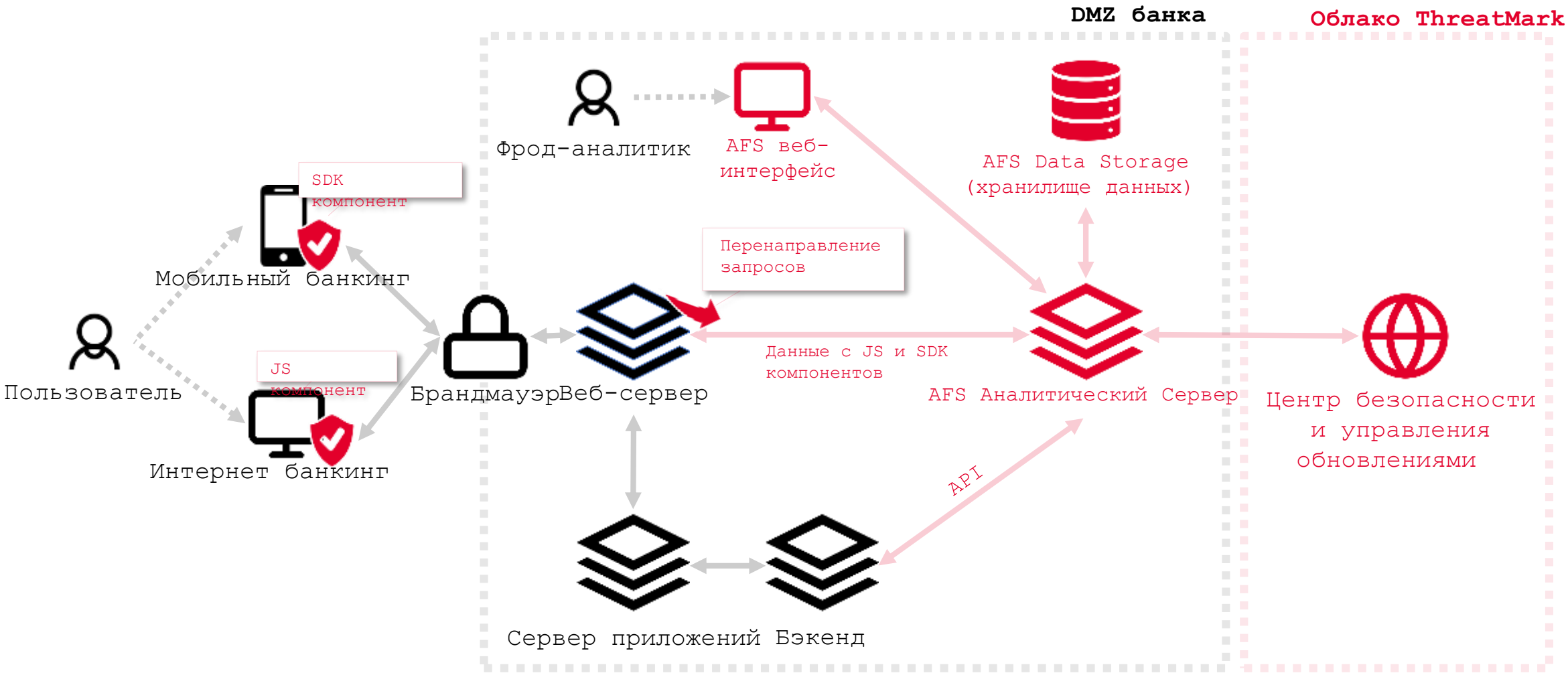
AFS мобильный компонент

Встраивание SDK компонента в мобильное приложение

Настройка доступа

Настройка коммуникации между аналитическом сервером и инфраструктурой банка

Архитектура решения



Преимущества

- Низкие затраты на внедрение и использование
- Модульный подход
- Возможность интеграции со сторонними системами
- Машинное обучение с использованием обратной связи от банков
- Комплексная защита от онлайн-мошенничества «все в одном»
- Центр обмена информацией об атаках и устройствах

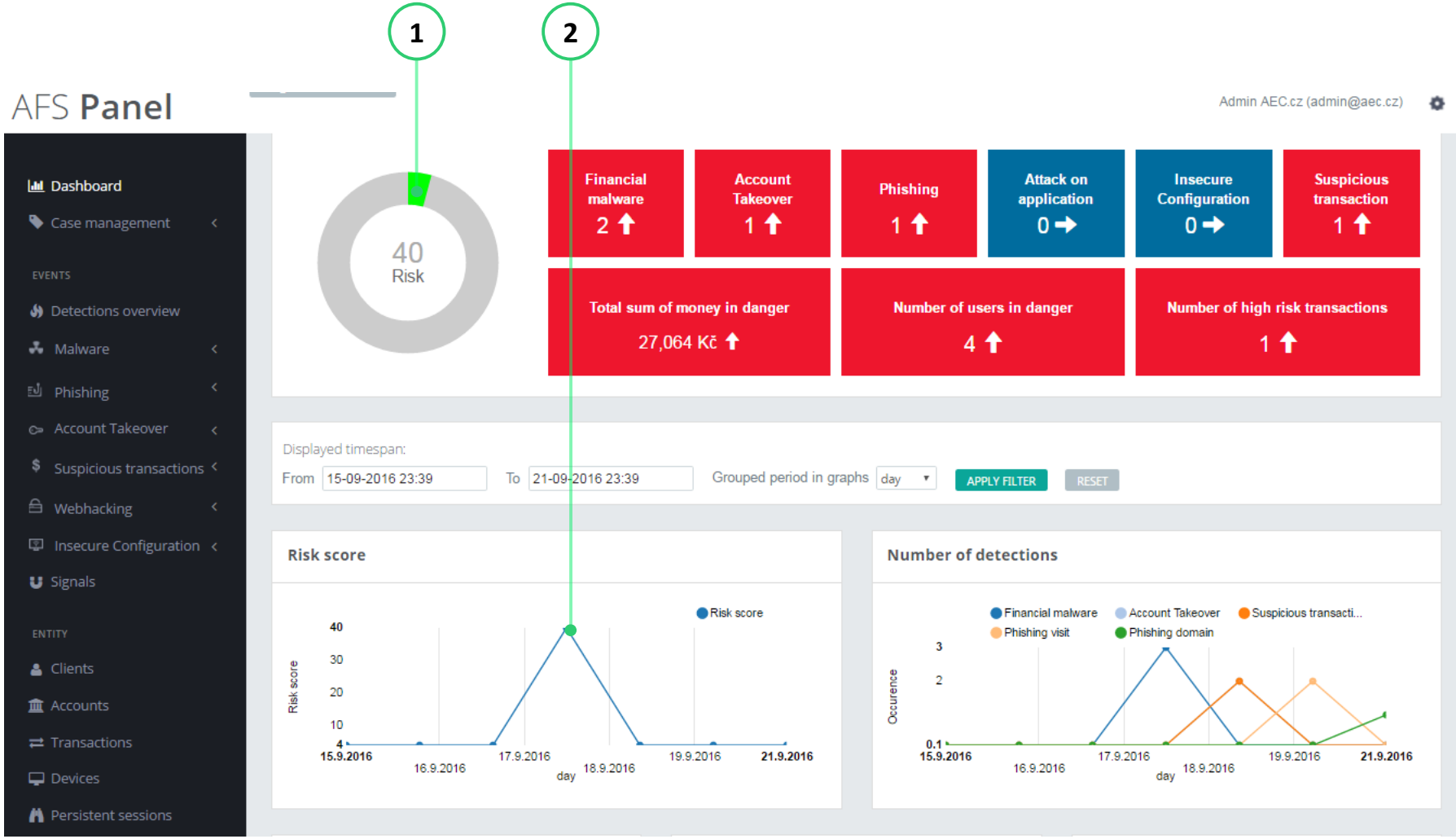
Преимущества для бизнеса

- Меньше ложных срабатываний
- Повышение удобства использования приложений
- Эффективная пользовательская аутентификация
- Рост доверия со стороны клиентов
- Повышение эффективности уже используемого антифрод решения
- Наглядность и прозрачность принятия решений через веб-интерфейс

Веб-интерфейс – общий вид

1. Текущая ситуация и количество угроз и атак за последние 48 часов

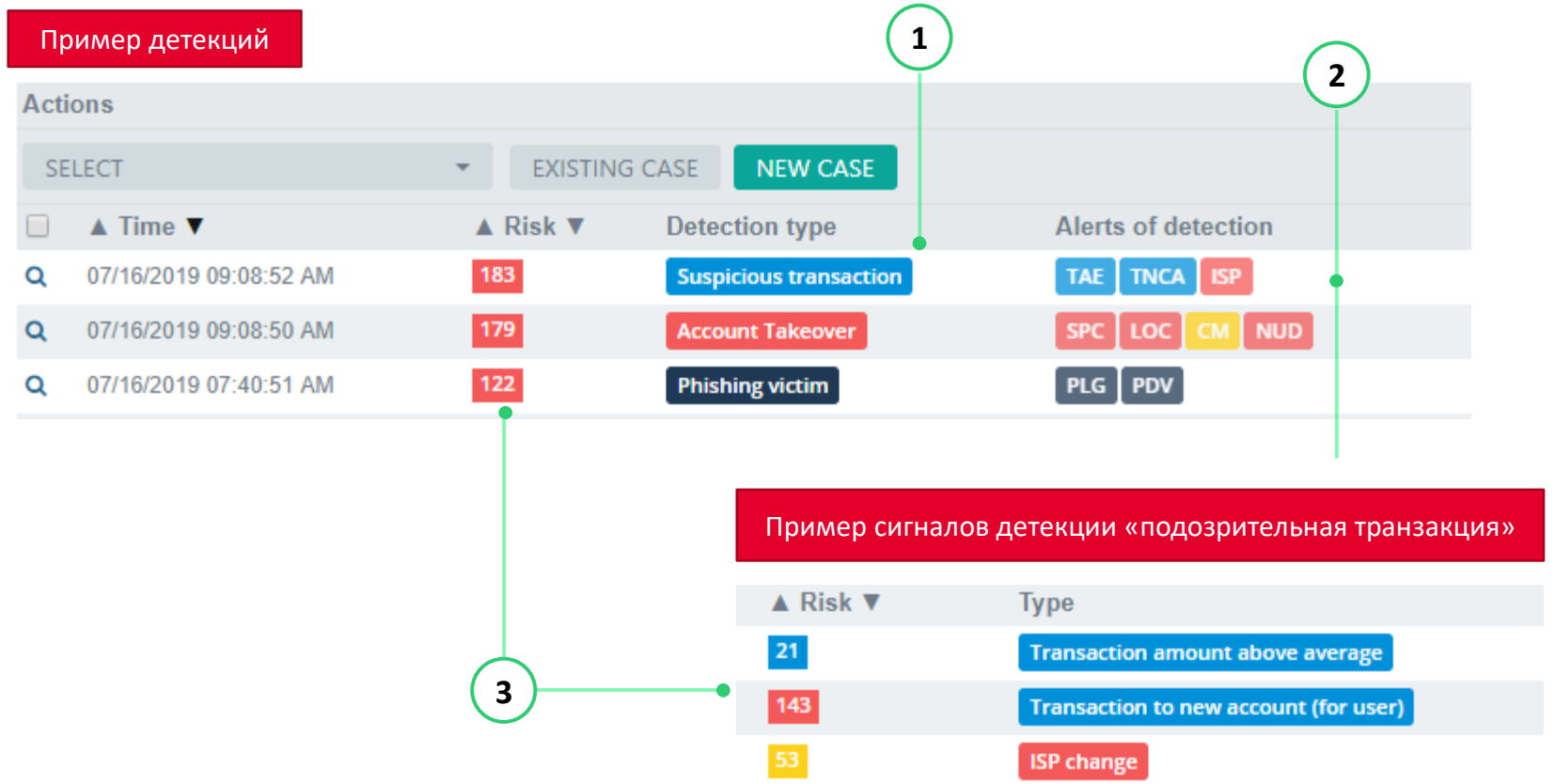
2. Текущая кампания по заражению девайсов вирусами



Веб-интерфейс – пример детекций

1. **Детекции (1)** создаются на основе нескольких **сигналов (2)**

2. Каждая детекция и сигнал имеют **оценку риска (3)**



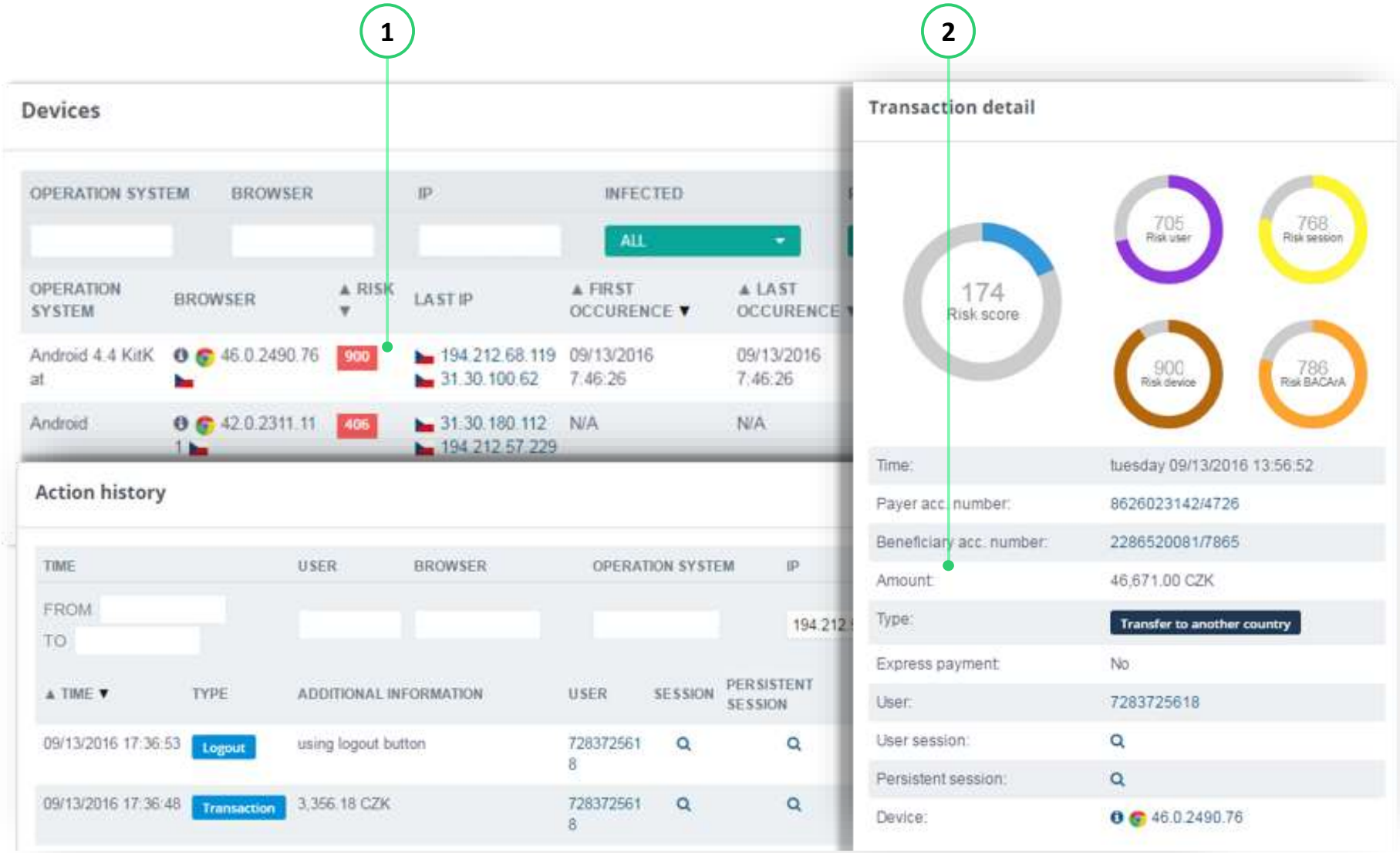
Веб-интерфейс – детали

1. Детали и информация о каждом клиенте банка:

- Устройства
- Геолокация
- История действий
- Оценка риска
- Программное обеспечение
- История обнаруженных аномалий и угроз

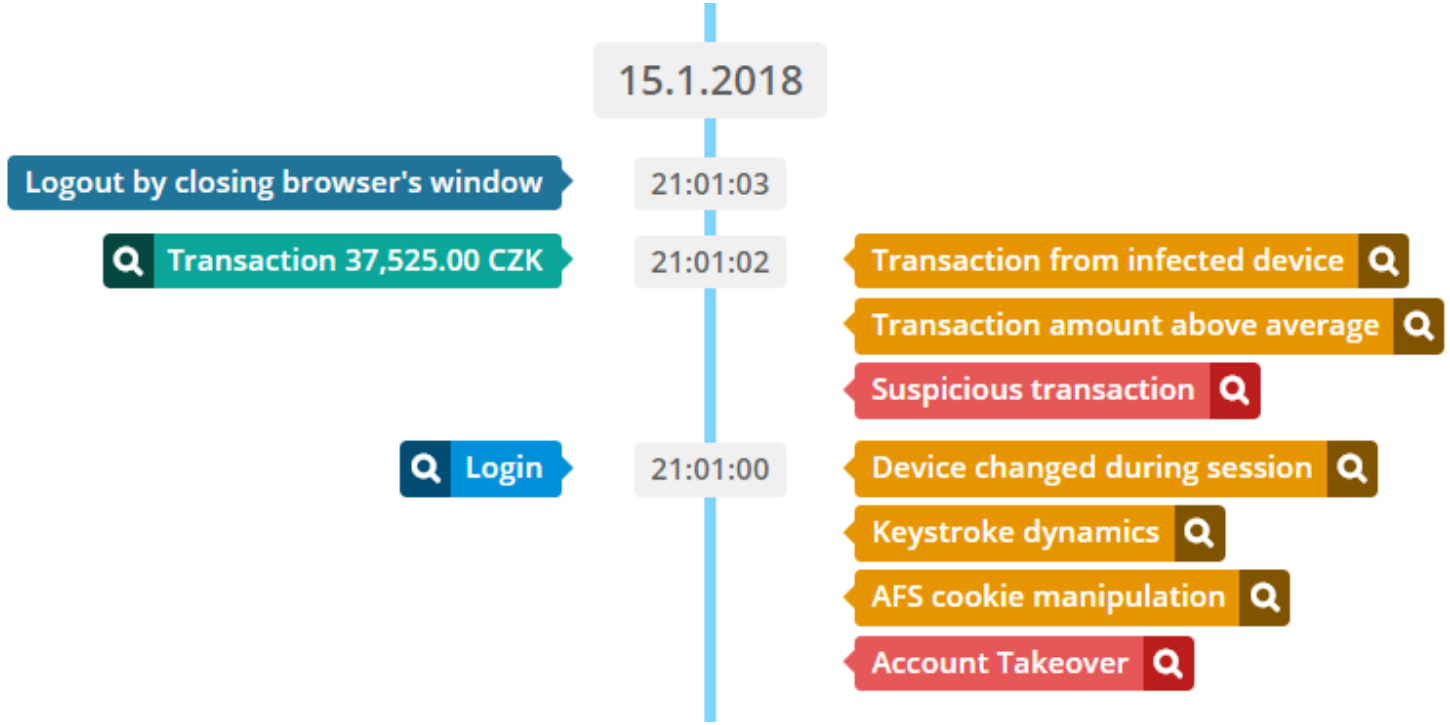
2. Детали анализа для

- Транзакций
- Клиентов
- Сессий
- Устройств



Веб-интерфейс – временная шкала

В интерфейсе можно проверить каждое действие клиента в приложении по секундам (слева от временной шкалы) и просмотреть обнаруженные аномалии (справа).



Что говорят наши клиенты

Более эффективное обнаружение угроз

Меньше ложных срабатываний

Экономия на двухфакторной аутентификации

Защитите Ваш бизнес. Сейчас!

www.threatmark.com

С чем сталкиваются банки сегодня

Проблема	Наше решение	Преимущества
Рост онлайн мошенничества	Наиболее полное обнаружение онлайн мошенничества	Предотвращение мошенничества и удобство для пользователей
Конкуренция со стороны финтехов	Проверка идентичностей пользователей	Доверие клиентов и репутация
Официальные стандарты и регламенты	Полное покрытие требований регуляторов в онлайн каналах	Соответствие стандартам, сокращение расходов, улучшение пользовательского опыта (UX)

Традиционный подход

- Не видят всей картины, только транзакции
- Не эффективно: сигнатуры, статичные правила
- Сложно внедрять и использовать

Типичные сценарии использования

Мошеничество
в интернет банкинге

Мошеничество в
мобильном банкинге

Проверка
идентичностей
пользователей

Обнаружение
кибер-угроз

Защита девайсов

Непрерывная
адаптивная
аутентификация

Соответствие
регламентам

Защита веб и моб.
приложений

И другое…