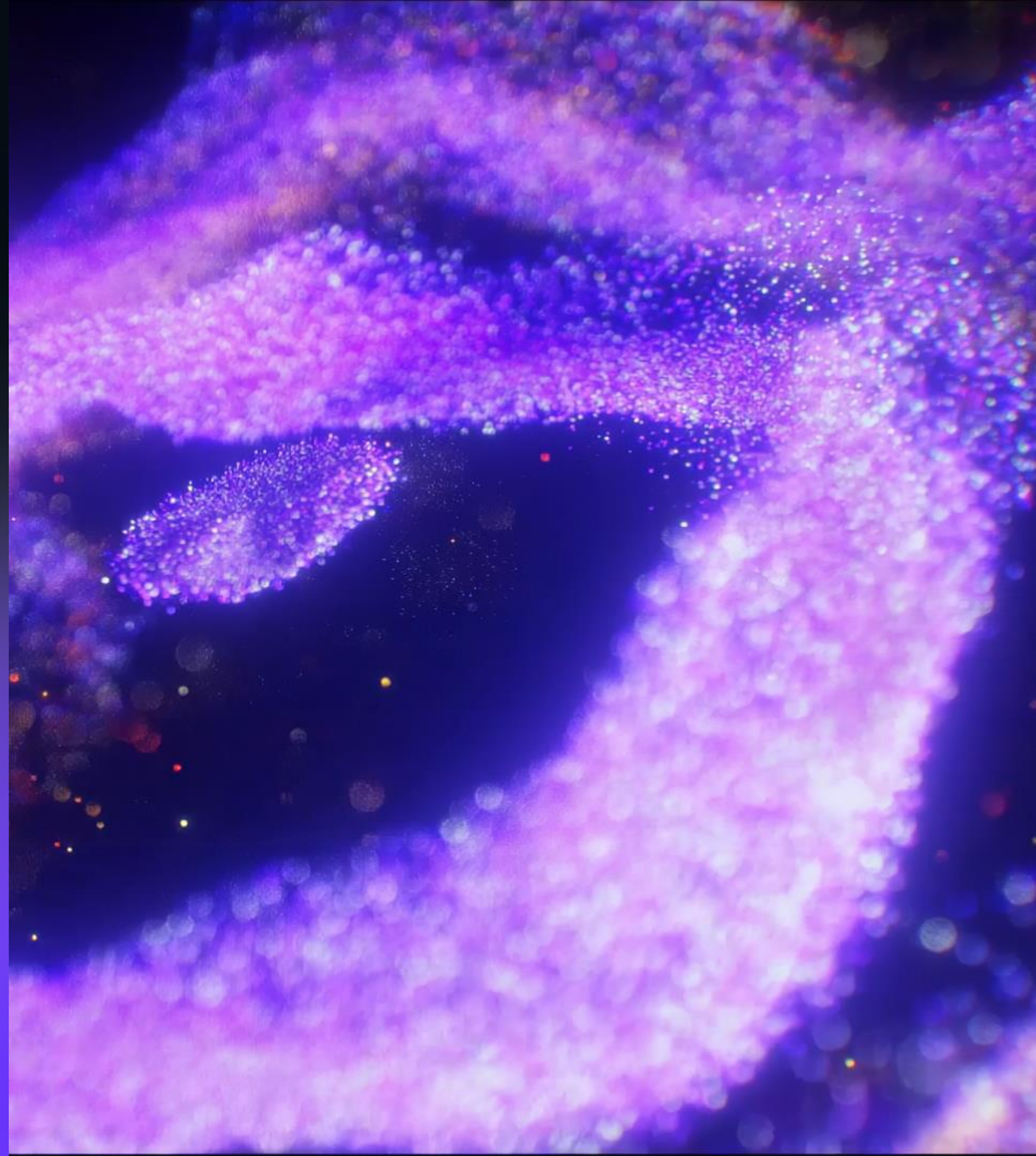
F6

Fraud Protection

Комплексная защита цифровой личности



F6

1 300+
успешных исследований киберпреступлений по всему миру

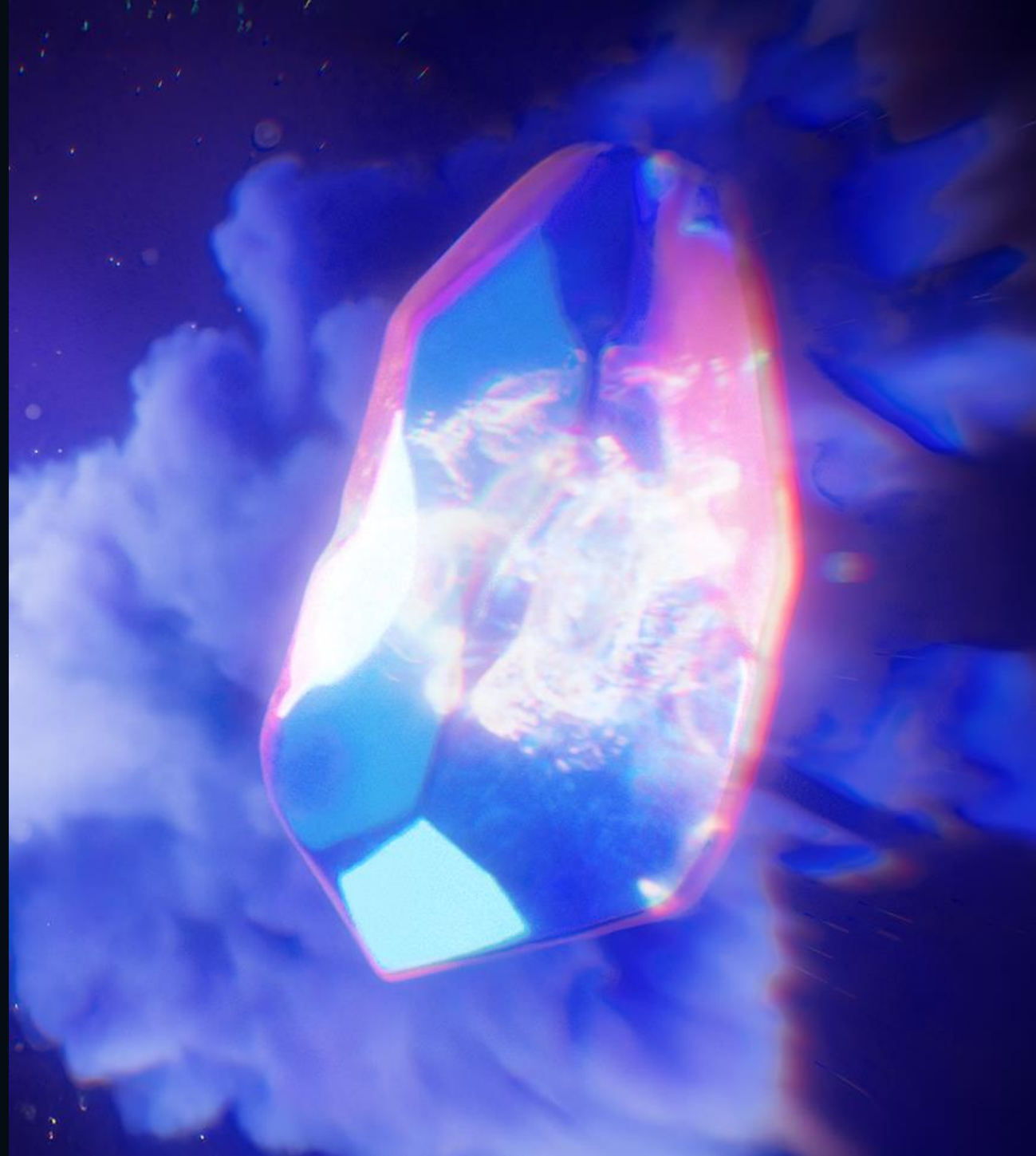
600
enterprise-клиентов

№1
первый поставщик услуги Incident Response в России

120+
патентов и заявок

20 млрд+
рублей сохраняют наши технологии в бюджете клиентов ежегодно

20 лет
практики и уникальной экспертизы на рынке РФ

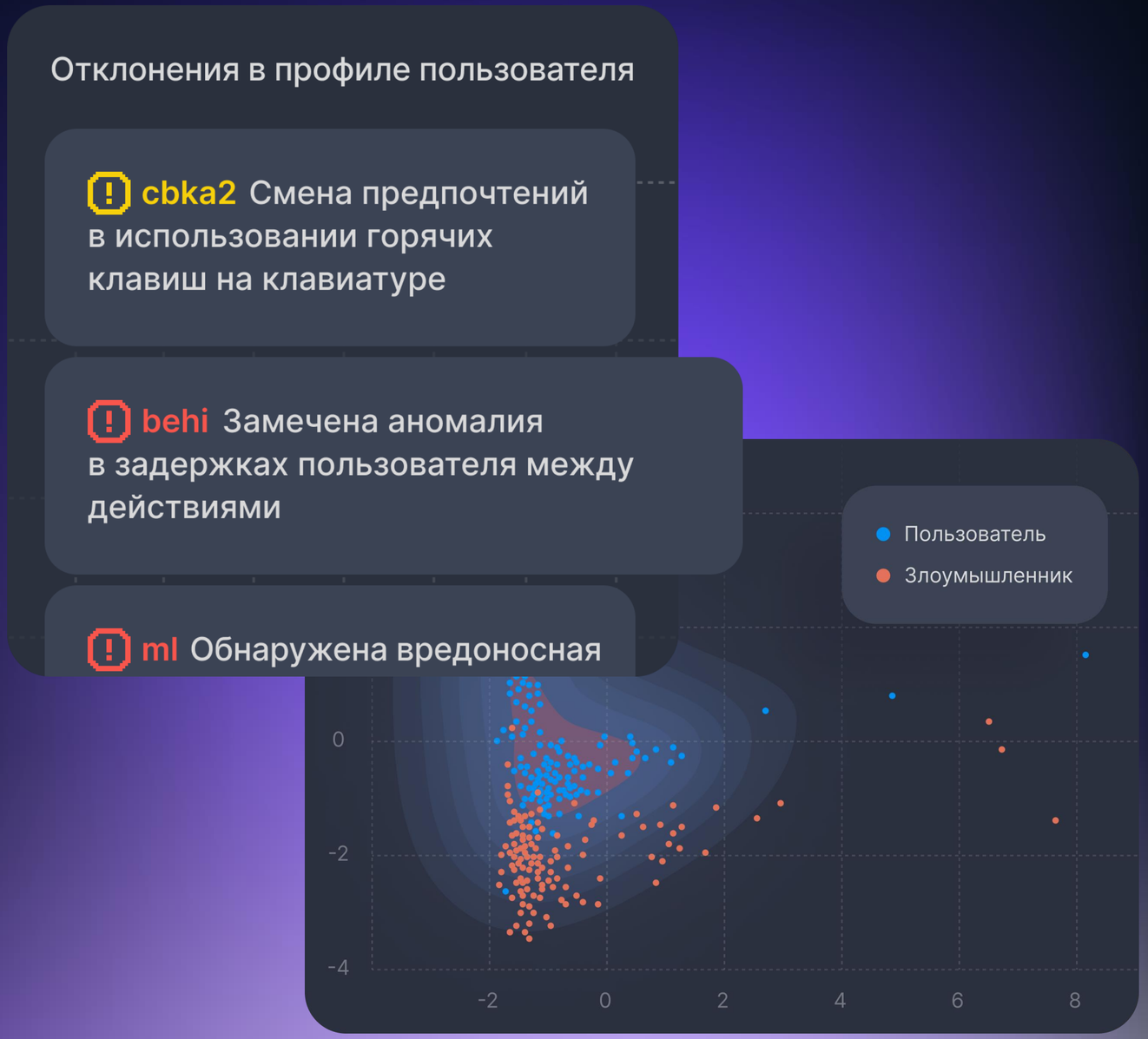


Fraud Protection

F6

Fraud Protection от F6 – это комплексное решение, в котором используются технологии снятия цифровых отпечатков устройств, выявления мошенничества и поведенческий анализ для защиты мобильных и веб-приложений.

Fraud Protection защищает виртуальную личность во всех цифровых каналах



F6

Зачем

Fraud Protection дает ответы на ключевые вопросы безопасности:

F6

1.

Как снизить финансовые потери от мошеннических транзакций и операций?

2.

Как избегать штрафов и санкций, полностью соответствуя стандартам безопасности и нормативным требованиям регулятора?

3.

Как оптимизировать операционную деятельность путем автоматизации процессов выявления и предотвращения мошенничества?

4.

Как эффективно прогнозировать новые типы угроз и быстро адаптироваться к ним, обеспечивая долгосрочную защиту бизнеса, используя машинное обучение?

5.

Как предотвращать потенциальные финансовые потери и снижать расходы на управление рисками?

6.

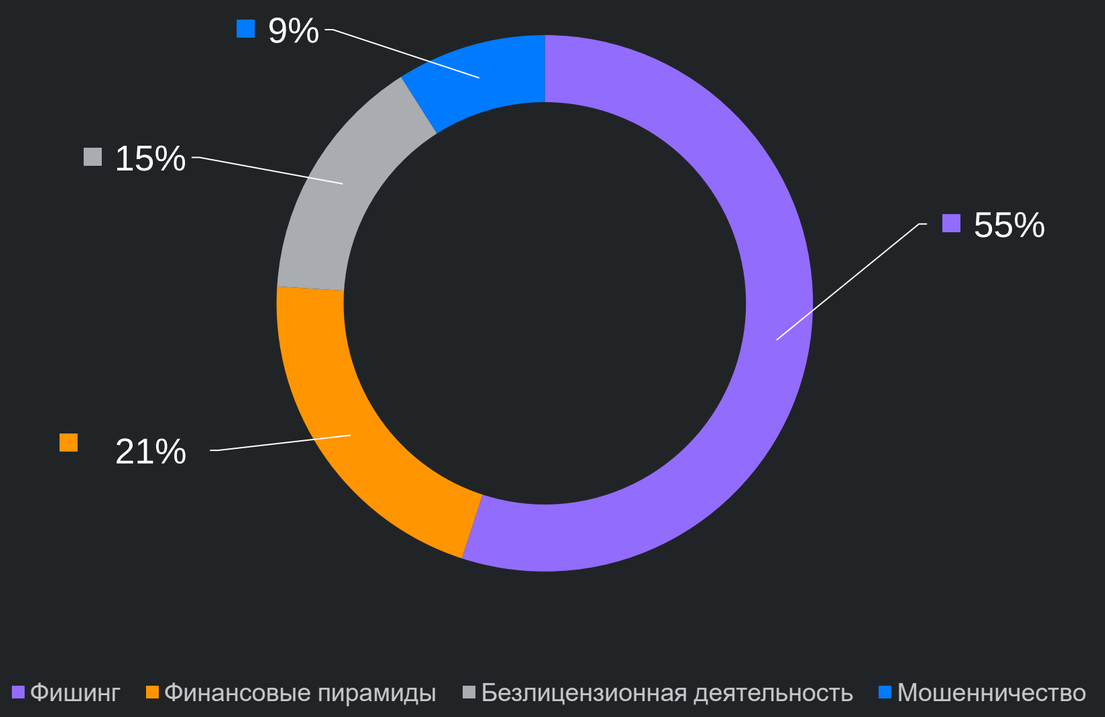
Как повысить доверие клиентов и улучшить репутацию бренда путем обеспечения безопасности данных и транзакций?

Статистика инцидентов

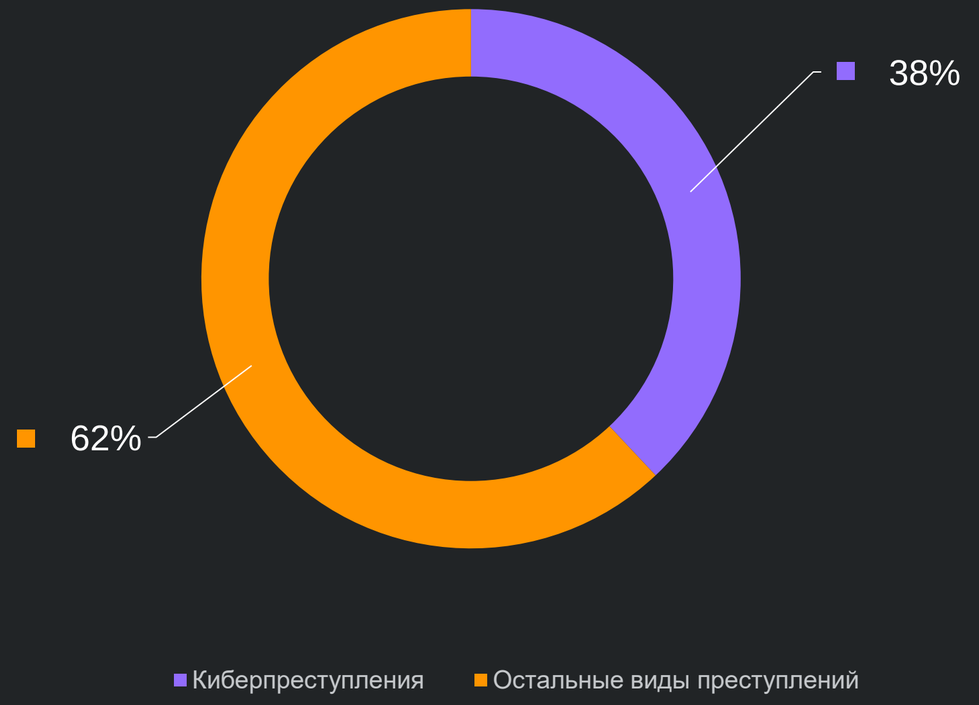
F6

210 млрд. ₽ — ущерб от IT-преступлений
в России за первые полгода 2024 г

Тип ресурсов, используемых мошенниками в 2024 г в России (%)



Доля киберпреступлений в России за первые 4 месяца 2024 г. (%)



Мошенничество или не мошенничество?

F6

Цель антифрода, влияющая на оставшиеся <1%

Клиенты, подвергающиеся атакам мошенников

99%

Активность легитимных пользователей

Почему важно защищать мобильные и веб-приложения в реальном времени?

F6

Высокие операционные затраты — повышаем конверсию

Штрафы за несоответствие требованиям регулятора — защищаем от утечек

Высокий показатель fraud to sale* — снижаем уровень мошенничества

Атакуемые приложения

- Интернет Банк
- Мобильный Банк
- Card-2-Card
- 3DSecure
- Интернет Эквайринг
- Кредитные заявки
- Кабинеты маркетплейсов
- Бонусные программы
- Сервисы регистрации
- Беттинги

Проблемы

- Хищение денежных средств со счетов
- Платежи с нелегальных ресурсов
- Отмывание доходов
- Платежное мошенничество
- Кредитное мошенничество
- Нелегитимные мерчанты
- Мошенничество с использованием вредоносного ПО
- Вредоносная бот-активность
- Мошенничество с бонусами
- Атаки на сервисы рассылки смс

Последствия

- Потеря денежных средств клиентами банков
- Репутационные потери
- Штрафы и издержки от регуляторов и платежных систем
- Финансовые потери из-за простоя бизнес-процессов и систем
- Нагрузка на антифрод систему
- Затраты на смс
- Издержки банка на обработку «фейковых» заявок на кредит

* Показатель влияет на доходы, репутацию и доверие клиентов

«Обеление» клиентов

F6

Расширены лимиты на операции для доверенных устройств при отсутствии негативной информации по ним и учетным записям клиентов

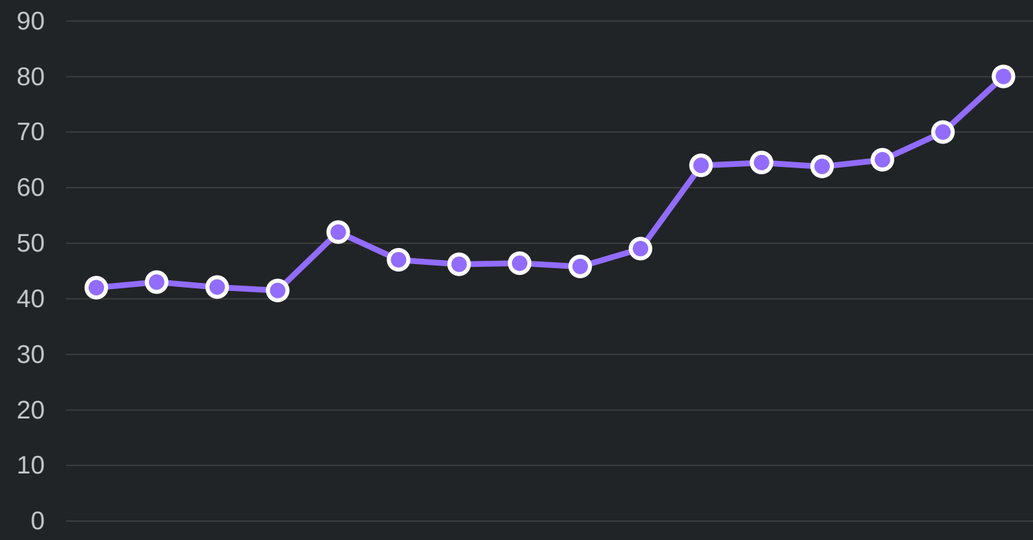
В 2,5 раза

снижена нагрузка на подразделение противодействия мошенничества

В 2,5 раза

снижено количество звонков клиентам

Динамика роста платежей с доверенных устройств среди всех платежей, %



Используйте Fraud Protection от F6

F6

Обнаруживайте ботов до того как они станут атаковать

Запатентованная технология Preventive Proxy выявляет и блокирует все типы бот-атак, включая скрапинг данных, брутфорс-атаки, нелегитимное использование API, и т.д.

Обеспечьте верификацию пользователя на всех уровнях

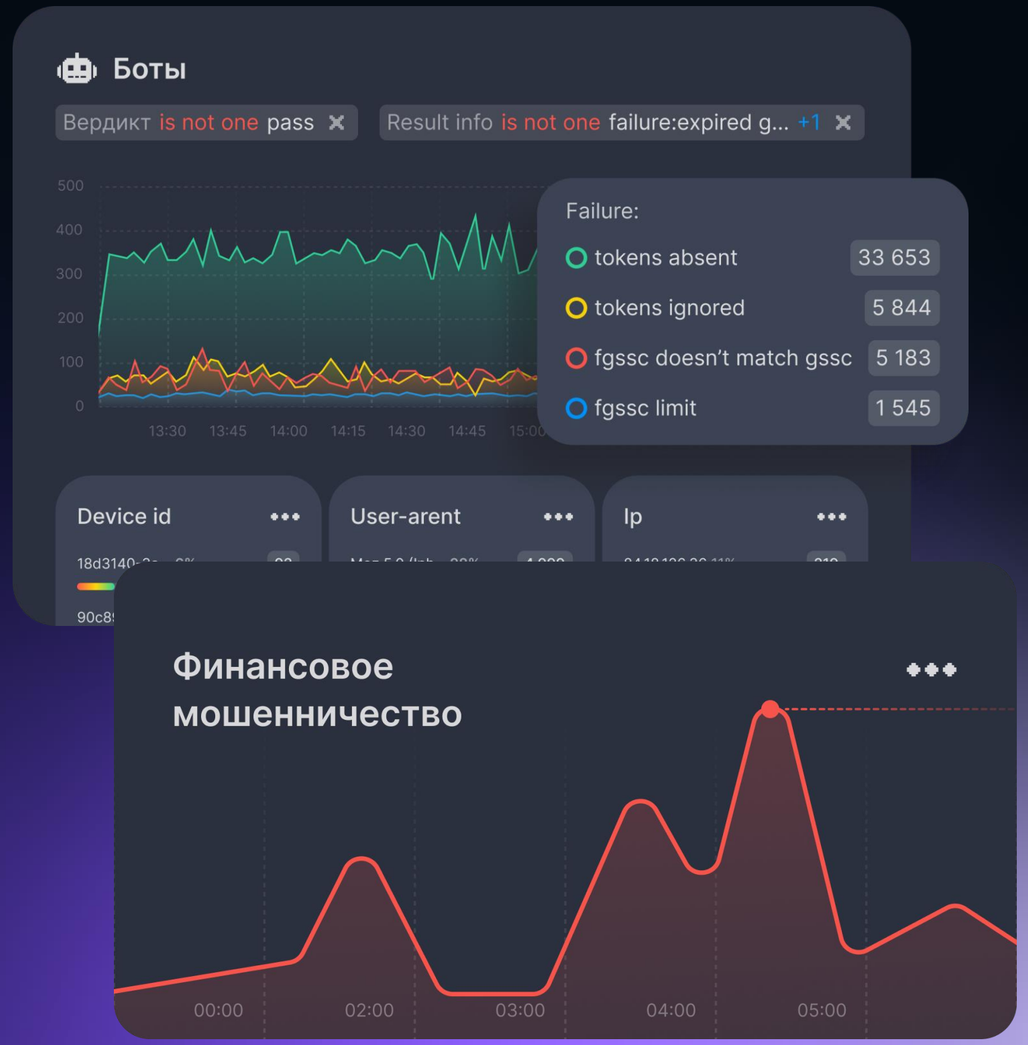
Fraud Protection анализирует активность пользователя с помощью алгоритмов машинного обучения и выявляет аномальную активность, позволяя снизить расходы на верификацию транзакций и потери от мошенничества

Оптимизируйте защиту вашей организации

Принимайте обоснованные решения по улучшению политики безопасности и внедрению необходимых защитных мер, что помогает компаниям быстрее реагировать на угрозы

Минимизируйте финансовые потери от кибератак

Снижайте убытки до 30% в сравнении с компаниями, которые не используют продвинутые решения по управлению угрозами



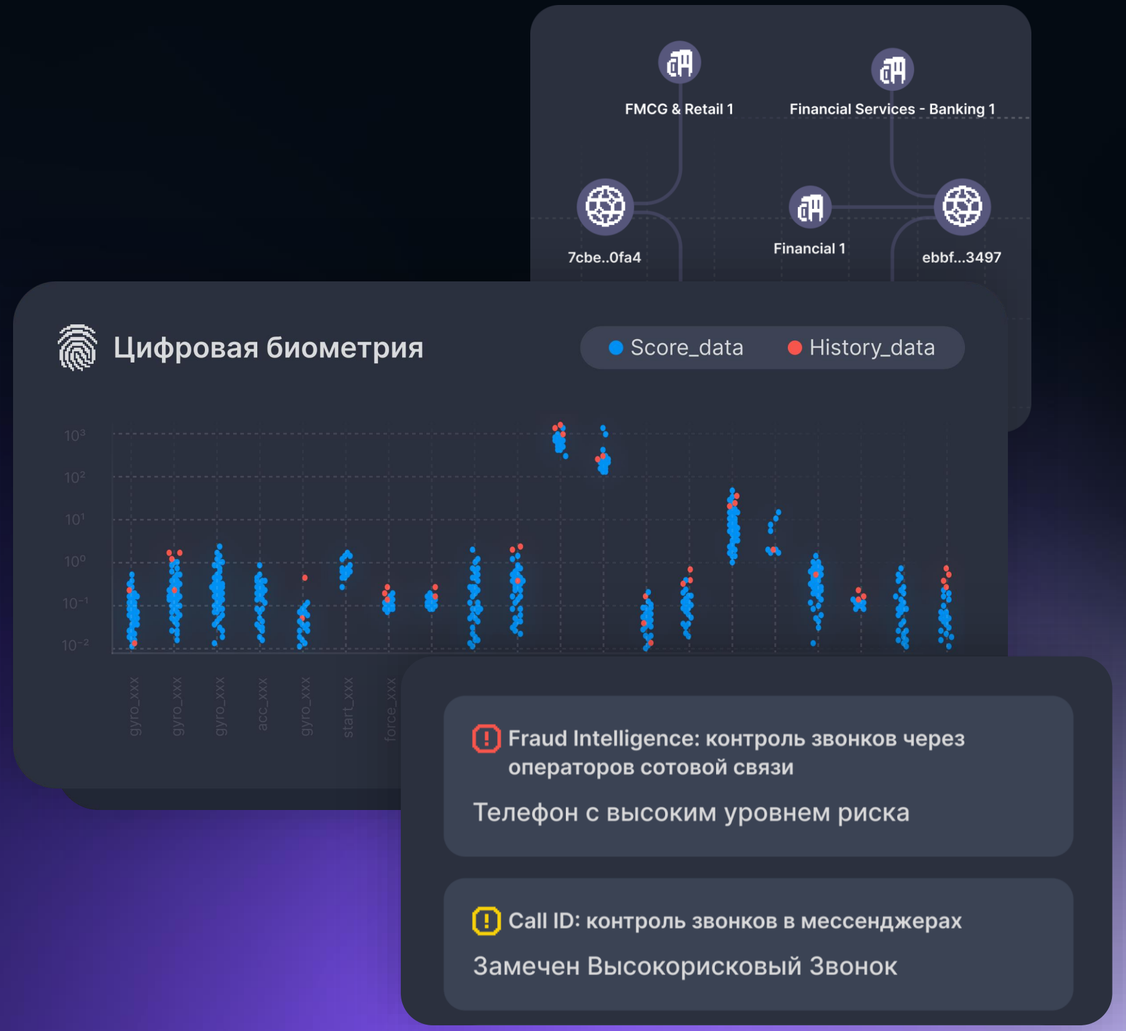
F6

Функционал

Функциональные преимущества

F6

- F6 Global ID
- Анализ поведения
- Защита от ботов
- Цифровой отпечаток устройства
- Выявление отмывания денег
- Кросс-канальный анализ
- Предотвращение Социотехнических атак
- Предотвращение мошенничества card-not-present
- Графический исследовательский инструмент
- Построение правил и управление ими
- Компьютерная криминалистика и исследования
- Прозрачный искусственный интеллект



Непрерывная защита всех цифровых каналов

F6

Веб-страницы и мобильные приложения

- Информация об устройствах
- Обнаружение ботов
- Выявление вредоносного ПО
- Обнаружение фактов удаленного доступа
- Определение использования пользователем приложения во время телефонного звонка
- Целостность операционных систем
- Проверка по глобальным идентификаторам мошеннических устройств

Пользовательские логины и пароли

- Поведенческая биометрия
- Антифишинг-проверки
- Цифровые отпечатки устройств
- Геолокация
- Анализ типа связи
- Беспарольная аутентификация

Непрерывный мониторинг

- Поведение пользователя в сравнении с предыдущими сессиями
- Обнаружение скриптов
- Выявление атак типа Man-in-the-Browser
- Обнаружение фактов удаленного доступа
- Определение использования пользователем приложения во время телефонного звонка

Мониторинг транзакций

- Скомпрометированные кредитные карты
- Счета обнальщиков
- Анализ связей между счетами

* Все скрипты, трафик и данные модифицируются для предотвращения перехвата третьими сторонами. Идентифицирующая личность информация не собирается.

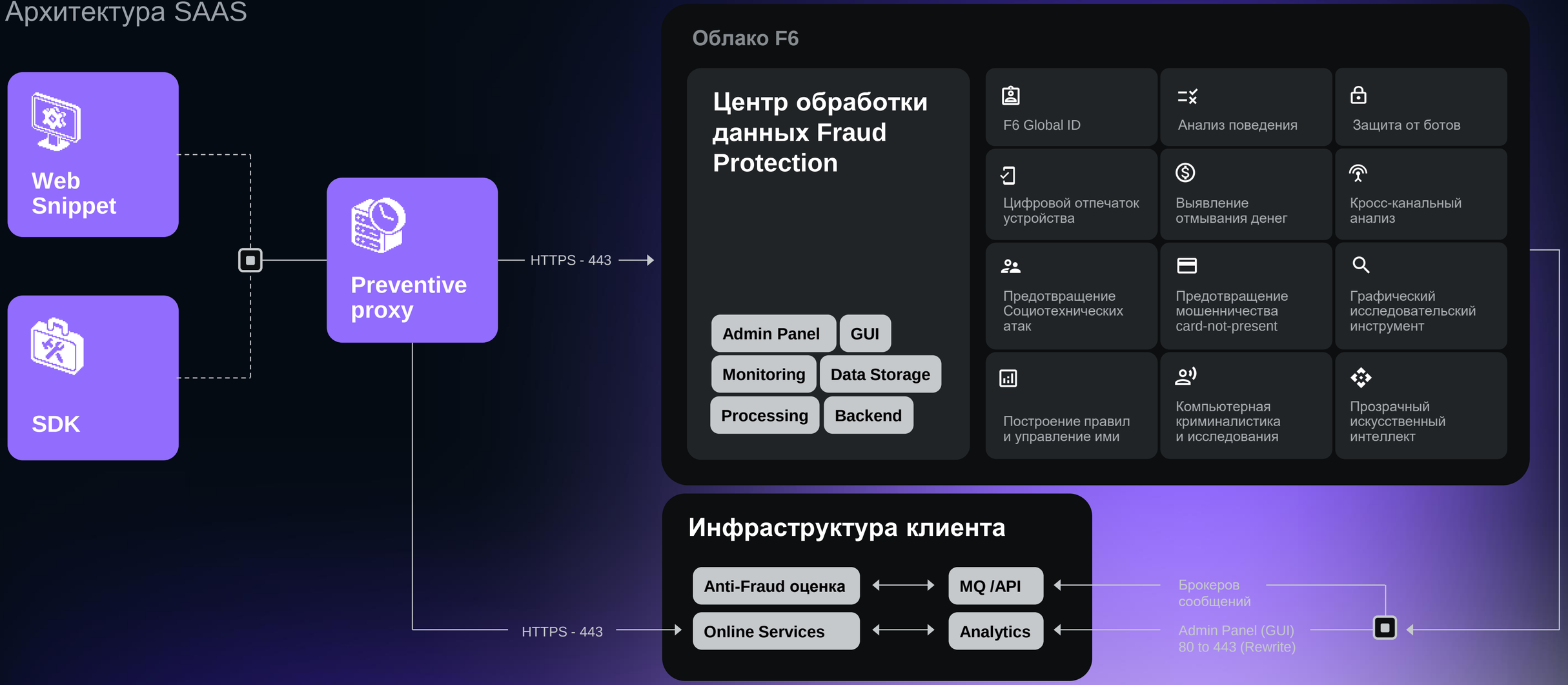
F6

Архитектура

Fraud Protection

F6

Архитектура SAAS

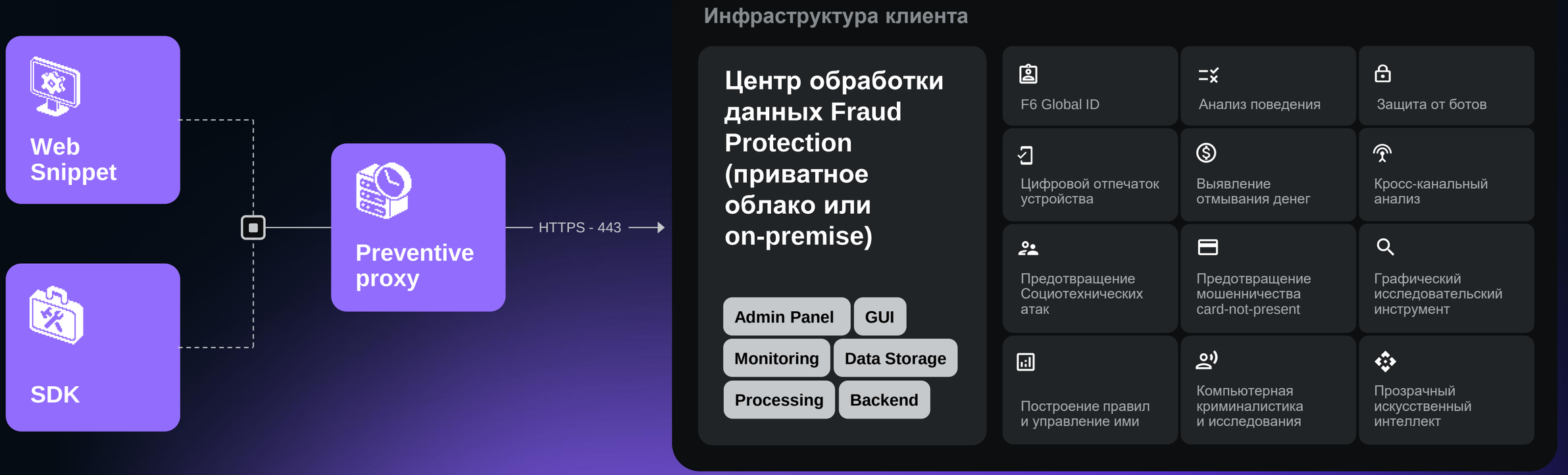


* Все скрипты, трафик и данные модифицированы для предотвращения вмешательства третьих сторон.
Сбор персональной и другой конфиденциальной информации не осуществляется.

Fraud Protection

F6

Архитектура On-premise



* Все скрипты, трафик и данные модифицированы для предотвращения вмешательства третьих сторон.
Сбор персональной и другой конфиденциальной информации не осуществляется.

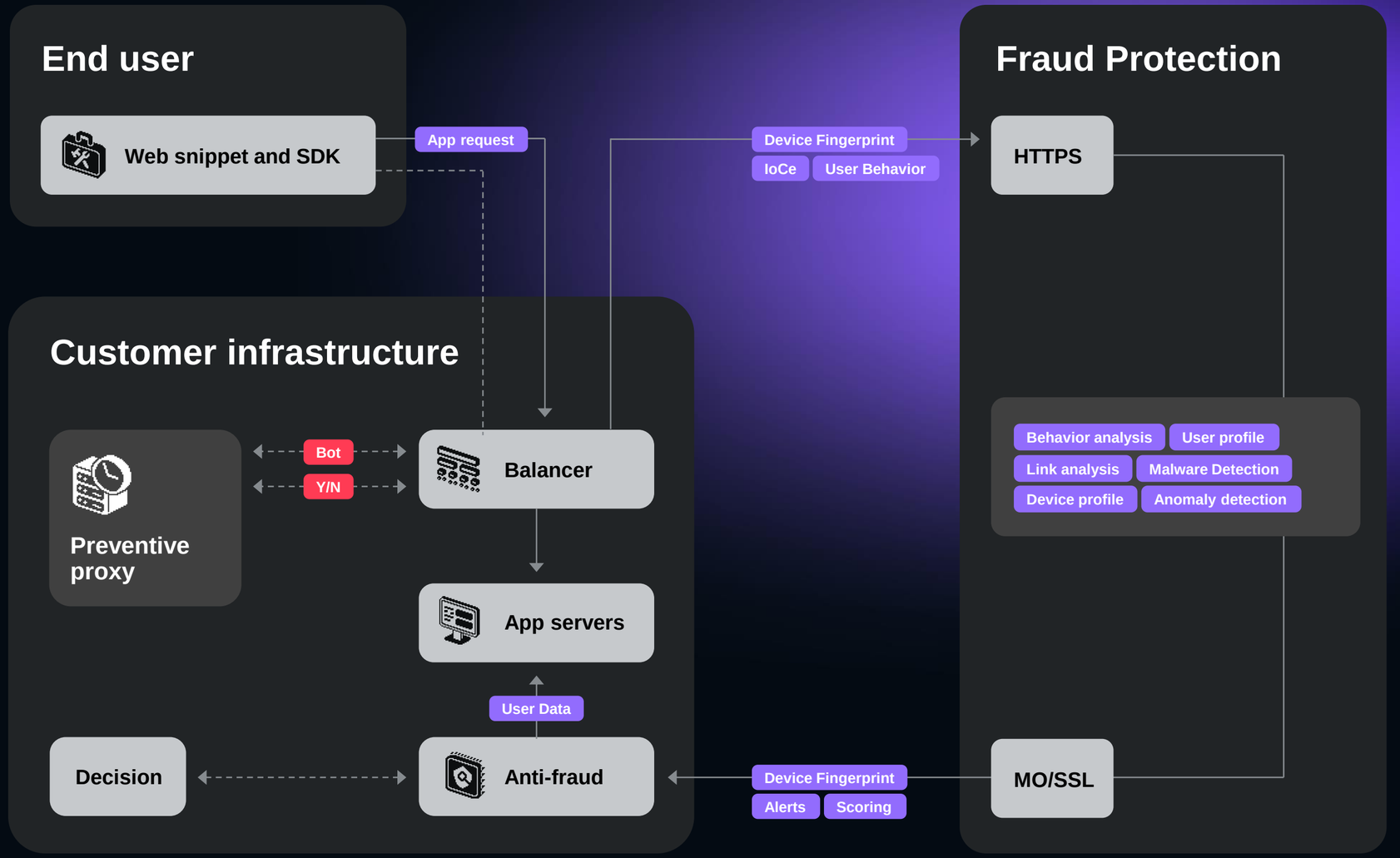
Preventive Proxy

F6

Архитектура Preventive Proxy

Модуль Preventive Proxy защищает мобильные и веб-приложения от различных типов бот-активности, включая:

- Скрапинг
- Брутфорс
- Скальпинг
- Подстановку учетных данных
- DDoS-атаки уровня 7
- Кражу файлов cookie
- Арбитраж
- Атаки на мобильный API
- Несанкционированное использование API
- Средства автоматизации Selenium, PhantomJS и др.



Fraud Protection

F6

Сравнение архитектур

Общие вопросы	SaaS	On-Premise
Время внедрения	✓ Простота внедрения, поддержки и использования системы без дополнительных затрат.	! Высокая стоимость лицензии, включающая затраты на внедрение и поддержание локального ПО, значительные инвестиции в оборудование.
Масштабируемость	✓ Легко масштабировать, по мере необходимости, без необходимости дополнительных инвестиций в аппаратное обеспечение или инфраструктуру.	! В случае высокого роста клиентской базы возникают проблемы оперативного масштабирования инфраструктуры, влекущие подготовку обоснования приобретения и прохождения последующий процедур закупки.
Обновление и поддержка	✓ Самые первые актуальные обновления Fraud Protection и антифрод правил. Оперативное решения технических и аналитических вопросов.	! Сложность в обновлении и поддержке, в том числе аналитической. Обновление по графику в согласованные технологические окна с использование предейственных каналов связи.
Безопасность	✓ Высокие стандарты безопасности и постоянно контроль доступа, актуальные обновления сопутствующего программного обеспечения.	! Затраты на самостоятельное обеспечение безопасности данных, обновление сопутствующего ПО.
Экономическая эффективность	✓ Нет никаких сопутствующих затрат	! Затраты на аппаратное обеспечение, обслуживание и обновления приложений

F6

Модули

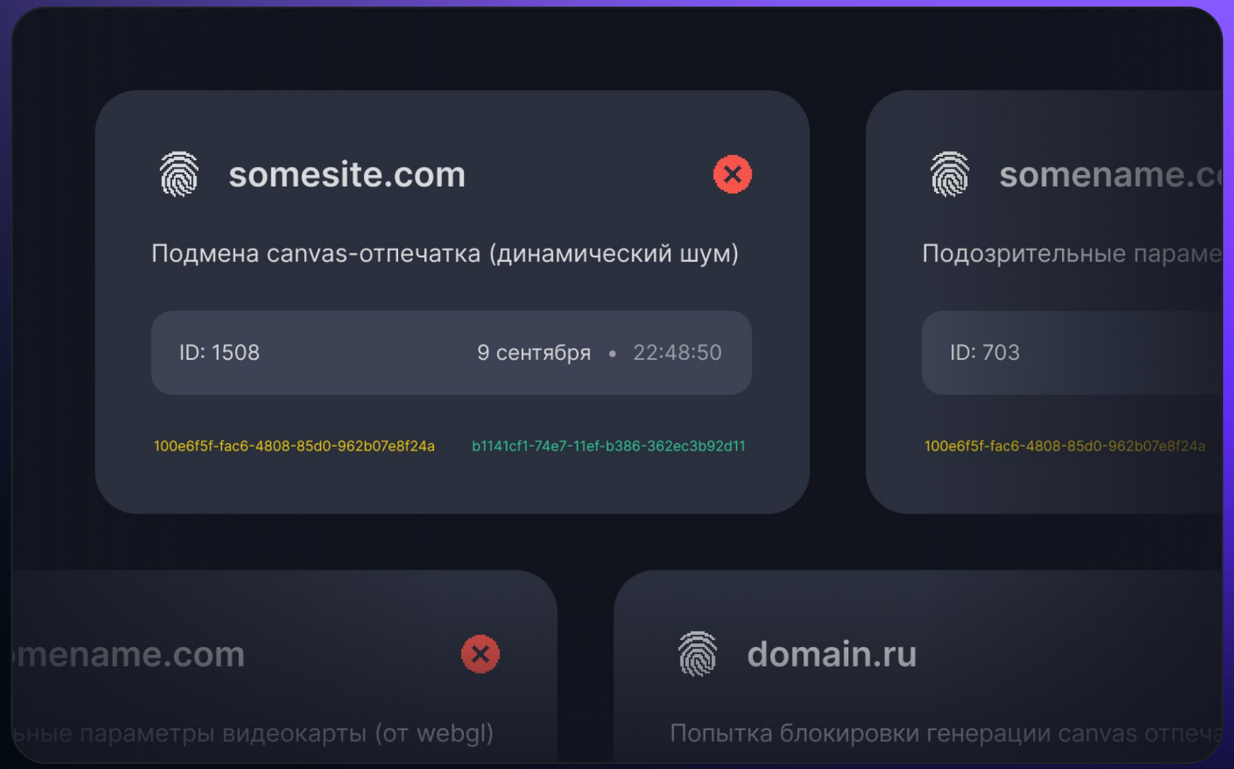
Защита веб-приложений

F6

Отпечатки устройств и цифровая биометрия

Поведенческий анализ, цифровая биометрия

- Информация о переходе пользователя по страницам защищаемого ресурса
- Идентификатор пользователя, зашифрованный публичным RSA-ключом клиента (по желанию)
- Обезличенный идентификатор пользователя
- Умное обнаружение троянов удаленного доступа на основе поведения указателя мыши
- Мониторинг портов троянов удаленного доступа
- Динамика нажатия клавиш пользователем
- Динамика движения курсора пользователя
- Индивидуальные закономерности пользовательского поведения
- Усредненная модель поведения пользователя
- Распознавание поведения пользователя
- Сопоставление поведения пользователя с известными закономерностями мошеннической активности
- Сравнение текущей активности пользователя с его поведением ранее для выявления факта контролирования сессии сторонним лицом
- Подтверждение легитимности пользовательских сессий



Цифровая биометрия и снятие цифрового отпечатка устройств в Web-канале

F6

Цифровая биометрия поведенческий анализ (клавиатурный и поведенческий подчерк)

Графическая конфигурация устройства и дисплея

Технические характеристики устройства

Обнаружение вредоносных программ, ботов и RAT

Конфигурация браузера

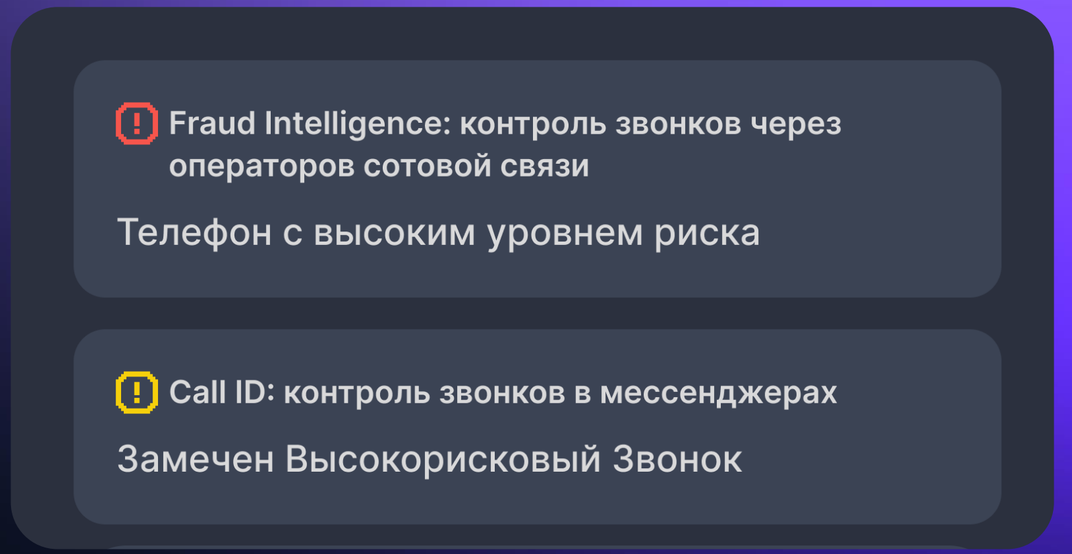
Защита мобильных приложений

F6

Отпечатки устройств и цифровая биометрия

Мониторинг характеристик мобильного оператора

- Идентификатор подписчика мобильной сети
- Идентификатор мобильного оператора
- Название мобильного оператора
- Страна мобильного оператора
- Серийный номер SIM-карты
- Страна выпуска SIM-карты
- Идентификатор мобильного оператора SIM-карты
- Название мобильного оператора SIM-карты
- Состояние SIM-карты
- Групповой идентификатор для GSM-сетей
- URL MMS-агента
- MMS-агент
- Флаг доступности обмена данными
- Флаг нахождения телефона в роуминге
- Название пакета приложения для приема SMS-сообщений
- Код страны
- Код мобильной сети
- Код зоны расположения
- Идентификатор соты (CID)
- Статус VoIP



Цифровая биометрия и снятие цифрового отпечатка мобильного устройства

F6

Обнаружение вредоносных программ, ботов и RATv

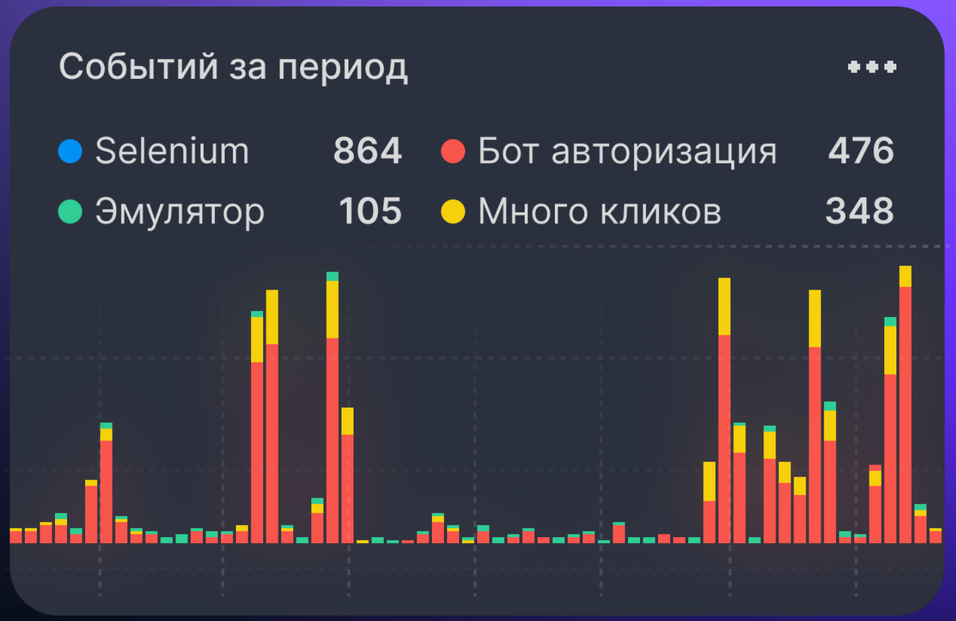
Мониторинг характеристик мобильного оператора

Цифровая биометрия, поведенческий анализ

Технические характеристики устройства

Мониторинг конфигурирования операционной системы Android или iOS

- Мониторинг датчиков устройств,
- Акселерометр
- Датчики приближения
- Сенсорные датчики
- Гироскопические датчики
- GPS-навигатор



F6

Ключевые преимущества

Fraud Protection

F6

Машинное обучение

Fraud Protection processing hub

Алгоритмы машинного обучения

Обучение без учителя

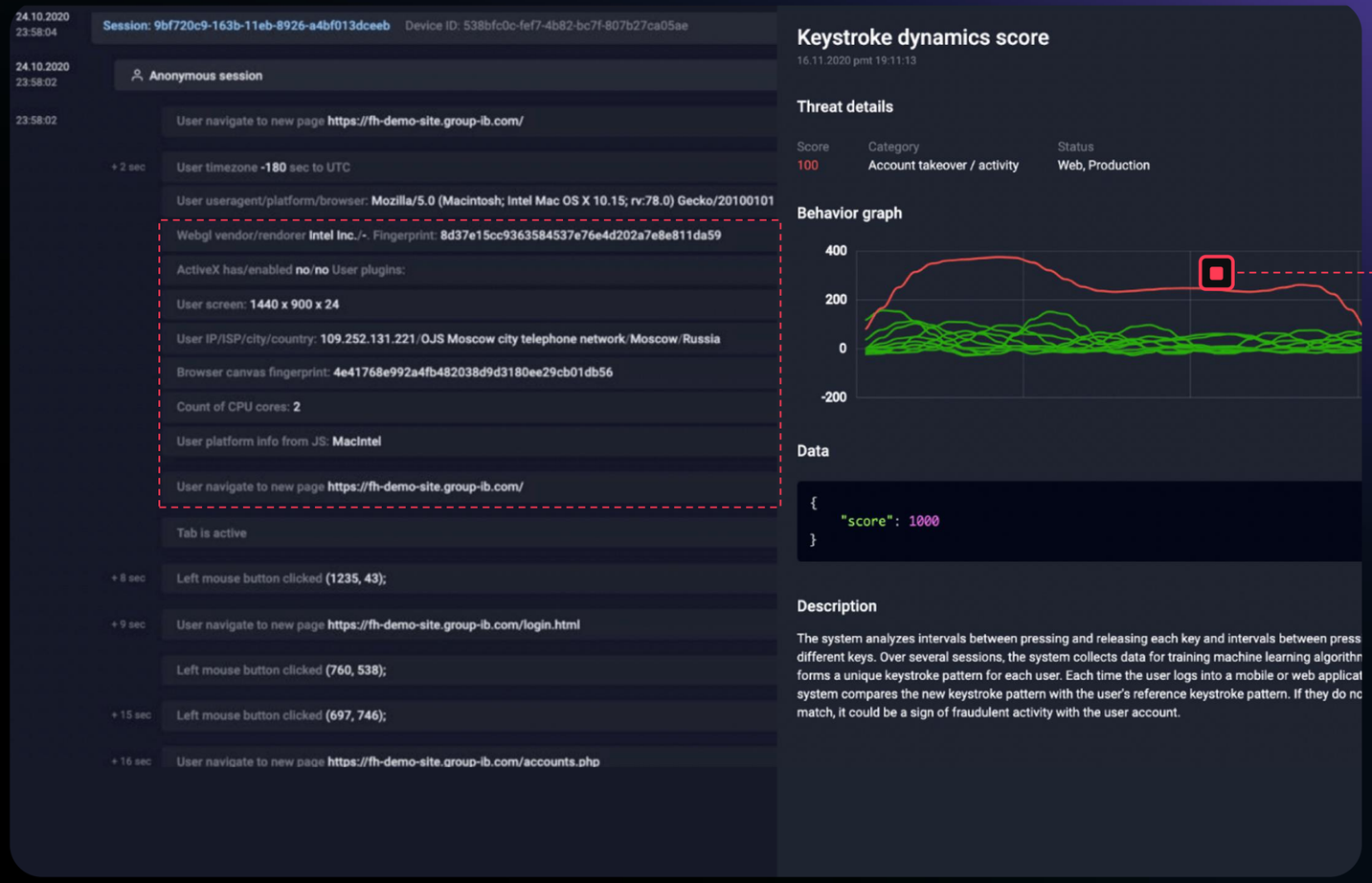
- Выявление аномалий
  - Одноклассовая машина опорных векторов
    - Поведение пользователя на мобильных устройствах (одно и то же устройство)
    - Поведение пользователей мобильных устройств (cross-mobile)
    - Идентификация пользователя по последовательностям действий
    - Анализ движения мыши
- Локальный уровень выброса
  - Идентификация пользователя по последовательностям действий
  - Анализ нажатий клавиш
- Кластеризация
  - CLOPE
    - Обнаружение составного устройства #

Обучение с учителем

- Классификация
  - Случайный лес
    - Анализ движения мыши
    - Идентификация пользователя по последовательностям действий
  - Градиентное повышение
    - Поведение пользователя на мобильных устройствах (одно и то же устройство)
  - Деревья решений
    - Автоматические комбинации правил
- Регрессия
  - Линейная регрессия
    - Обнаружение RAT

Анализ цифровых «отпечатков» В веб-каналах и цифровая биометрия

F6



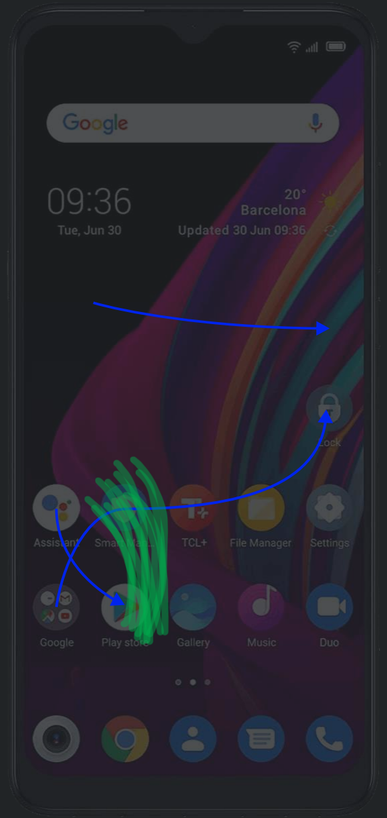
Индикаторы мошеннического поведения в пользовательской сессии

Анализ цифровых «отпечатков» устройств и цифровая биометрия для мобильных приложений

F6

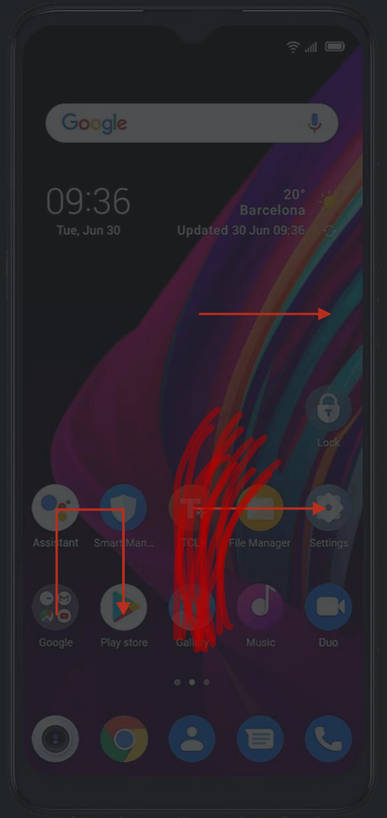
Определение легитимности пользователя: индивидуальные паттерны пользовательского поведения

- Прикосновения к экрану (сила и точки нажатий)
- Углы траектории свайпов
- Анализ свайпов
- Средняя скорость свайпов
- Средний угол отклонения свайпов от горизонтальной оси



Индикаторы мошенничества в пользовательской сессии

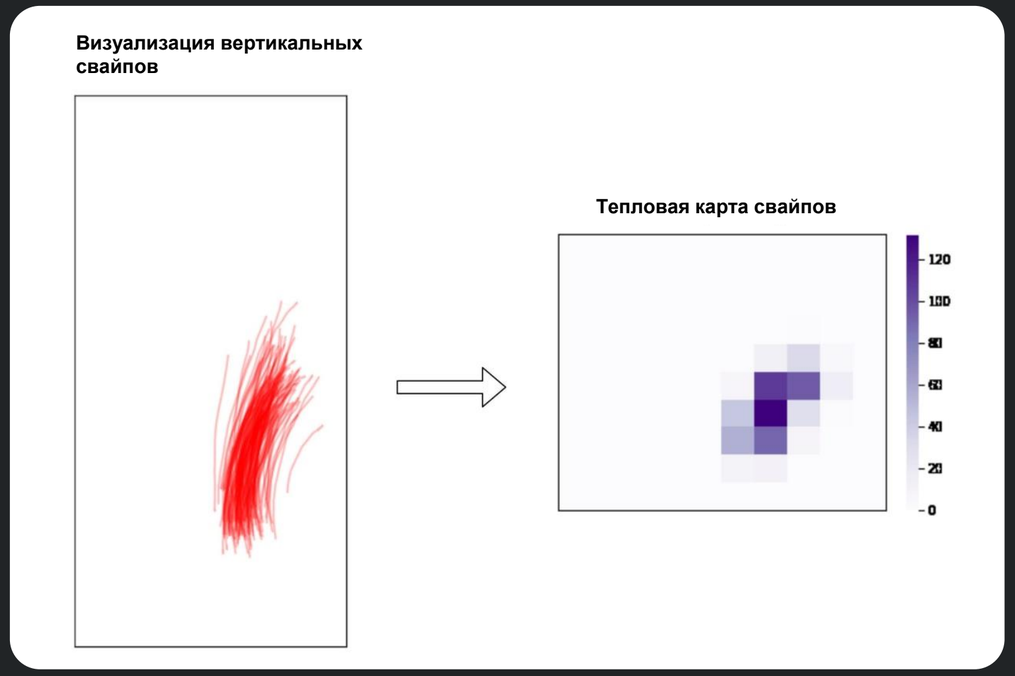
- Отклонения в характеристиках прикосновений к экрану (сила и точки нажатий)
- Отклонения в углах траекторий свайпов
- Отклонения в скорости свайпов
- Нетипичные значения углов отклонения свайпов от горизонтальной оси



Мобильная биометрия

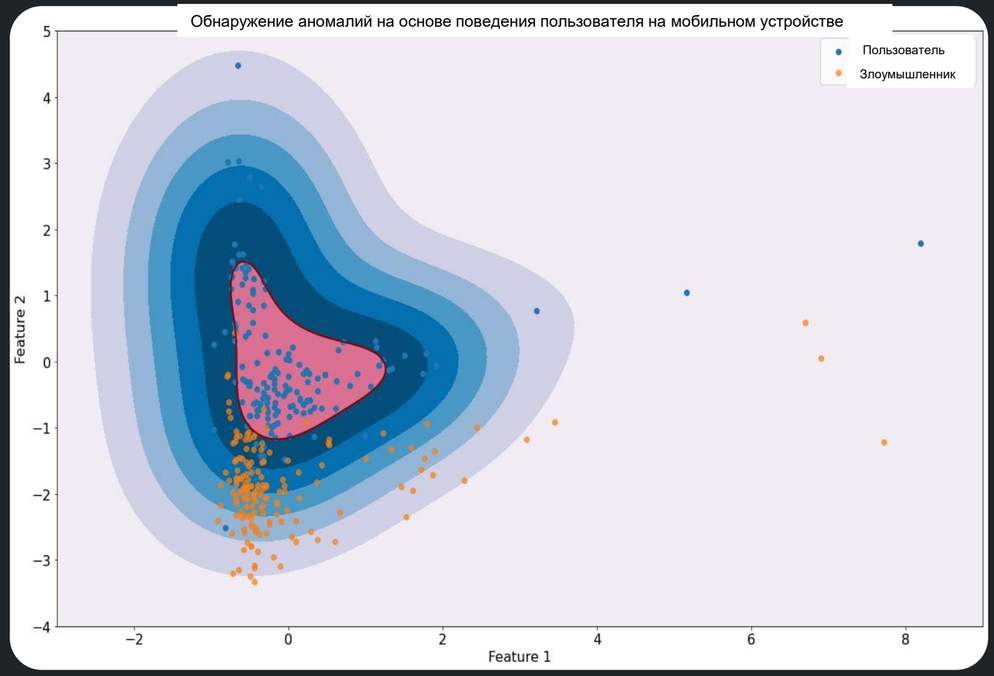
F6

Использование датчиков мобильных устройств для сбора цифровой биометрии



Показатели акселерометра и гироскопа

Тепловая карта прикосновений и свайпов

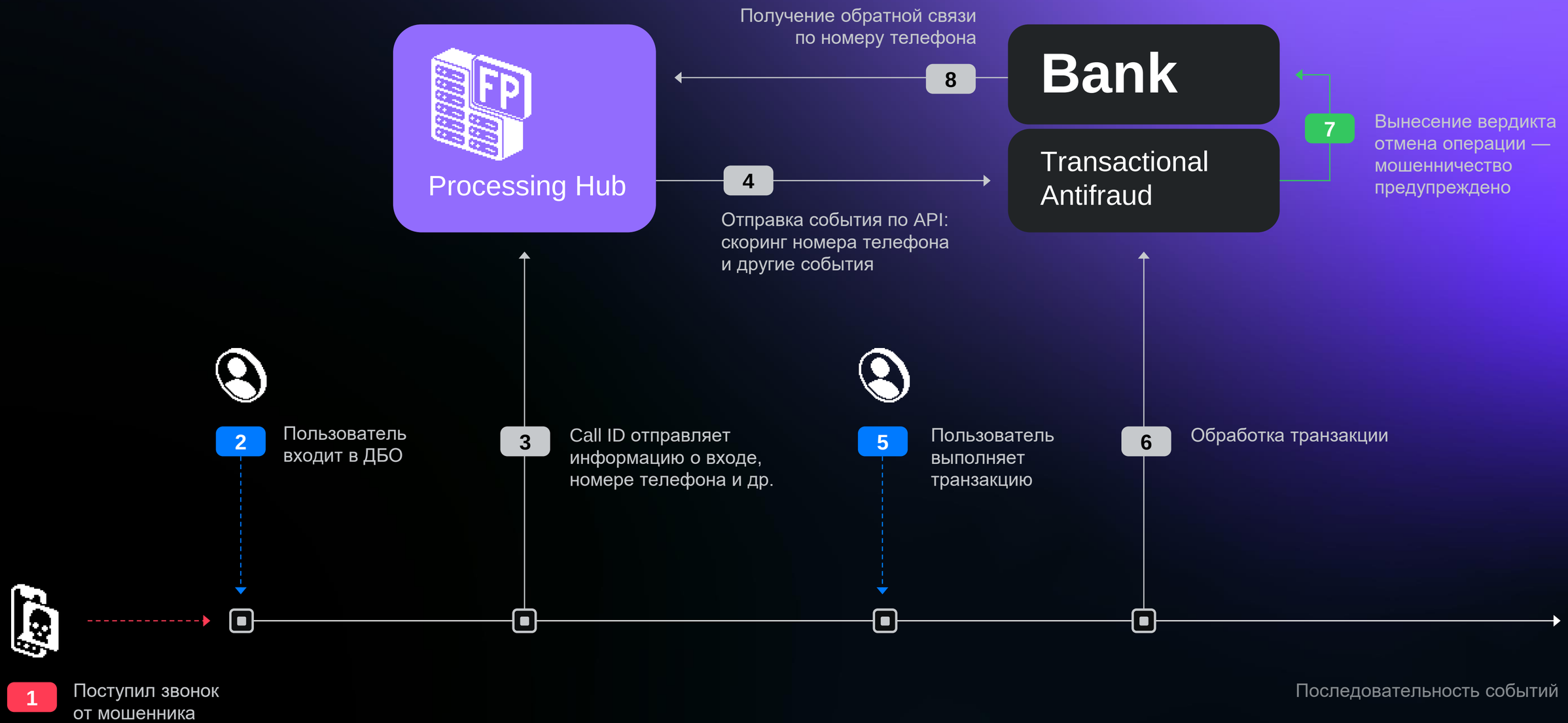


Интенсивность и частота прикосновений

Длительность и направление свайпов

Выявление мошеннических звонков

F6

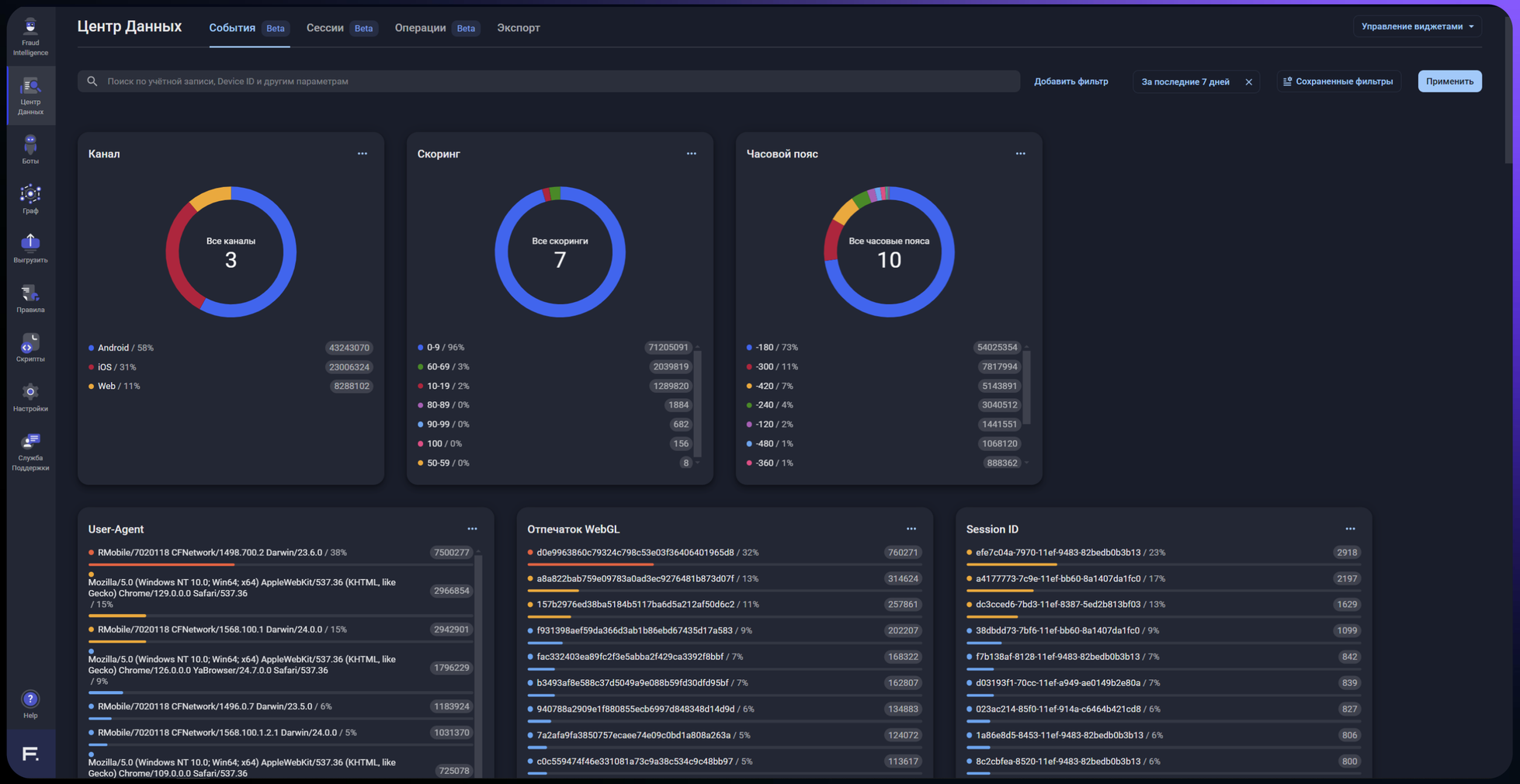


F6

Комфортный UI

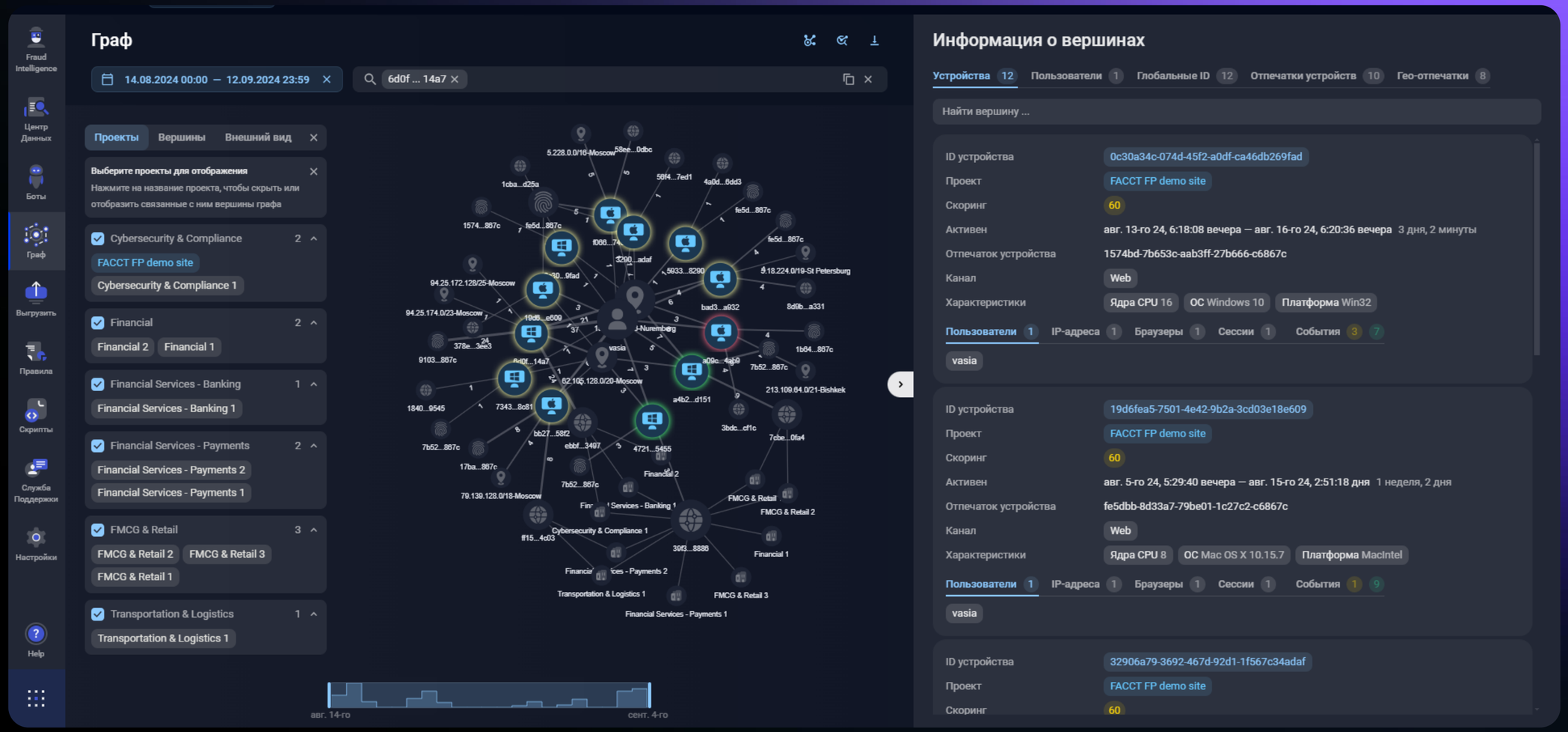
Интерактивная панель управления

F6



Отраслевой графовый анализ

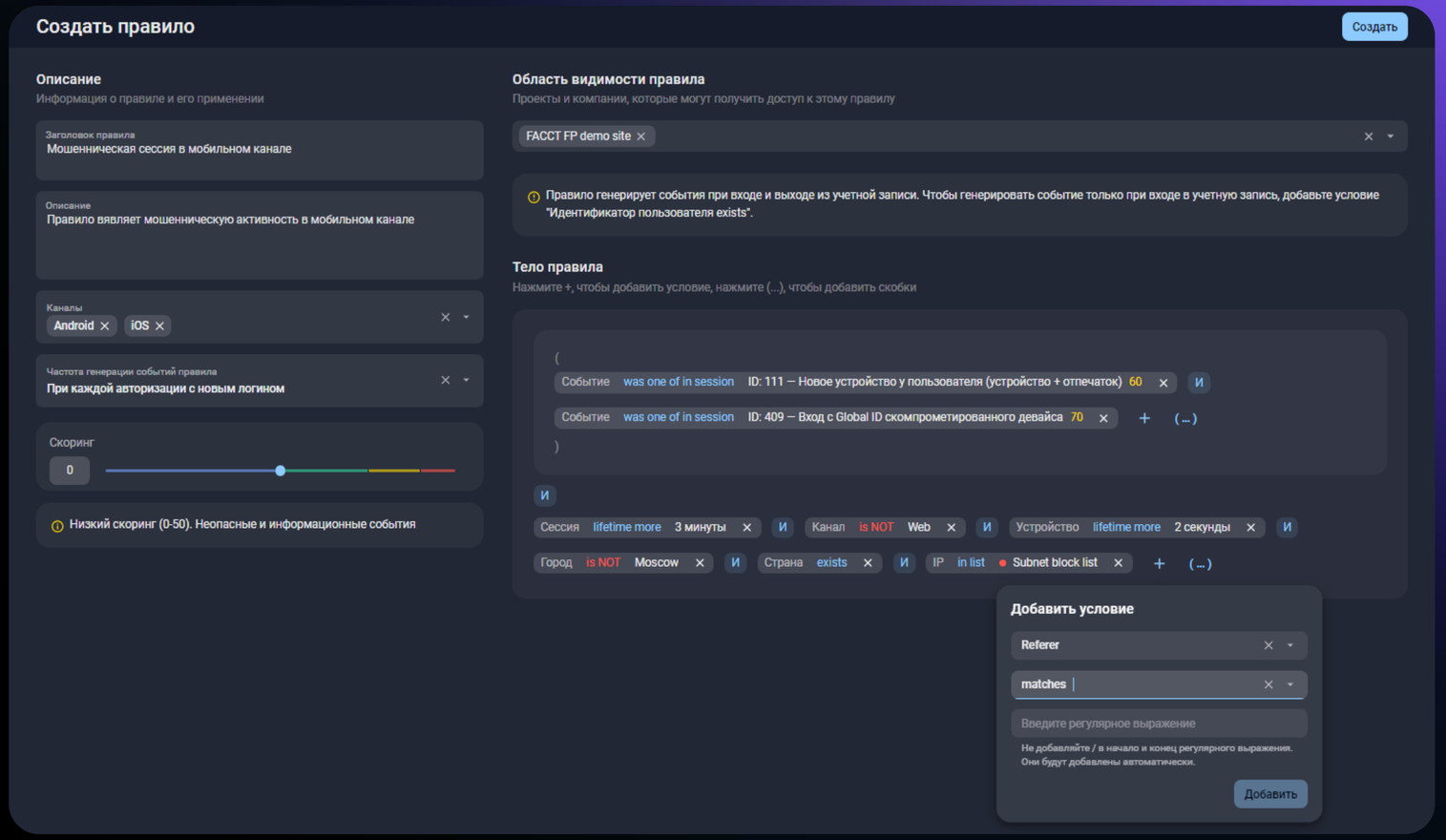
F6



Конструктор правил

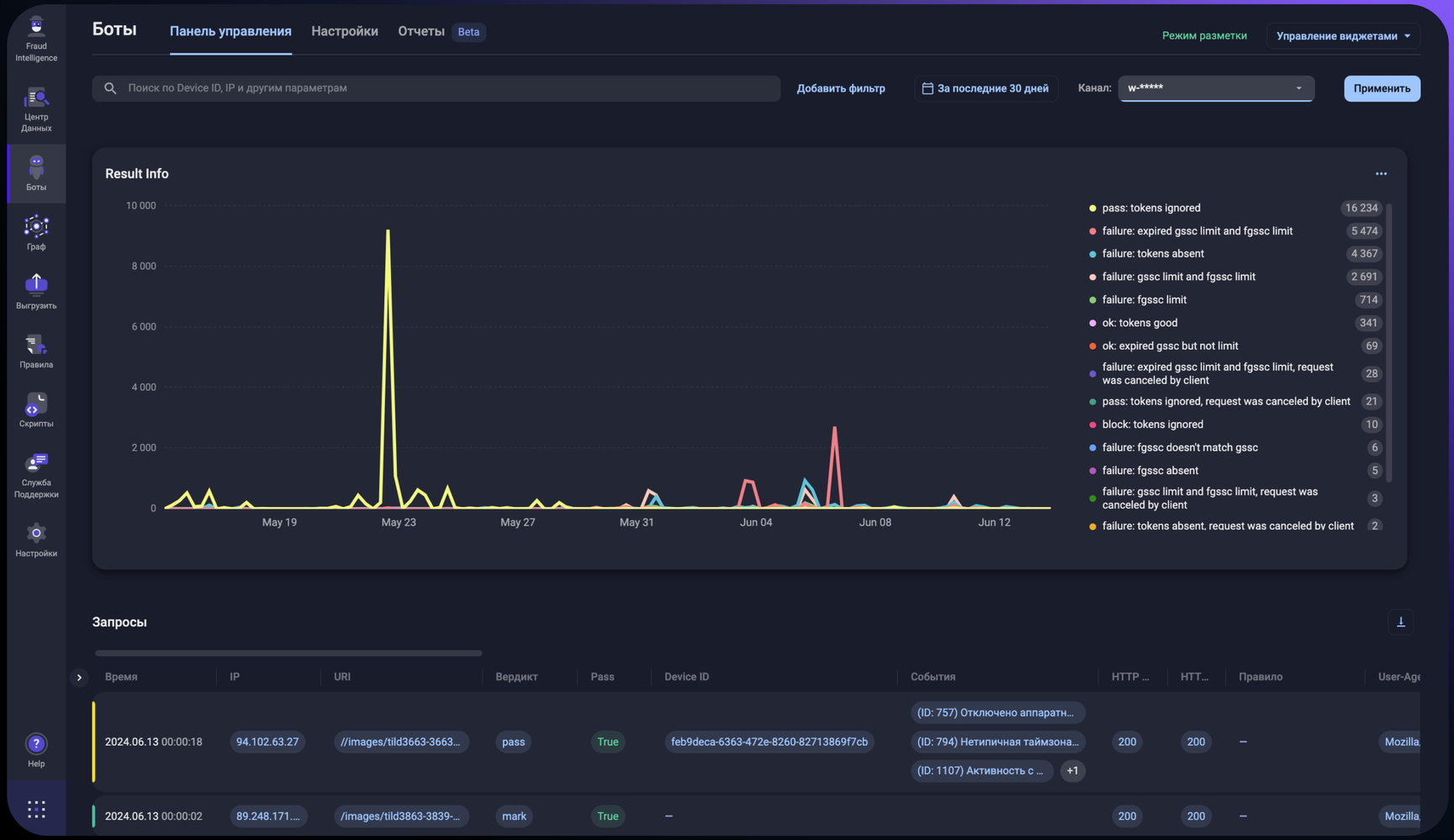
F6

Визуальный конструктор правил позволяющий самостоятельно создавать условия реагирования на новые выявленные случаи мошенничества.



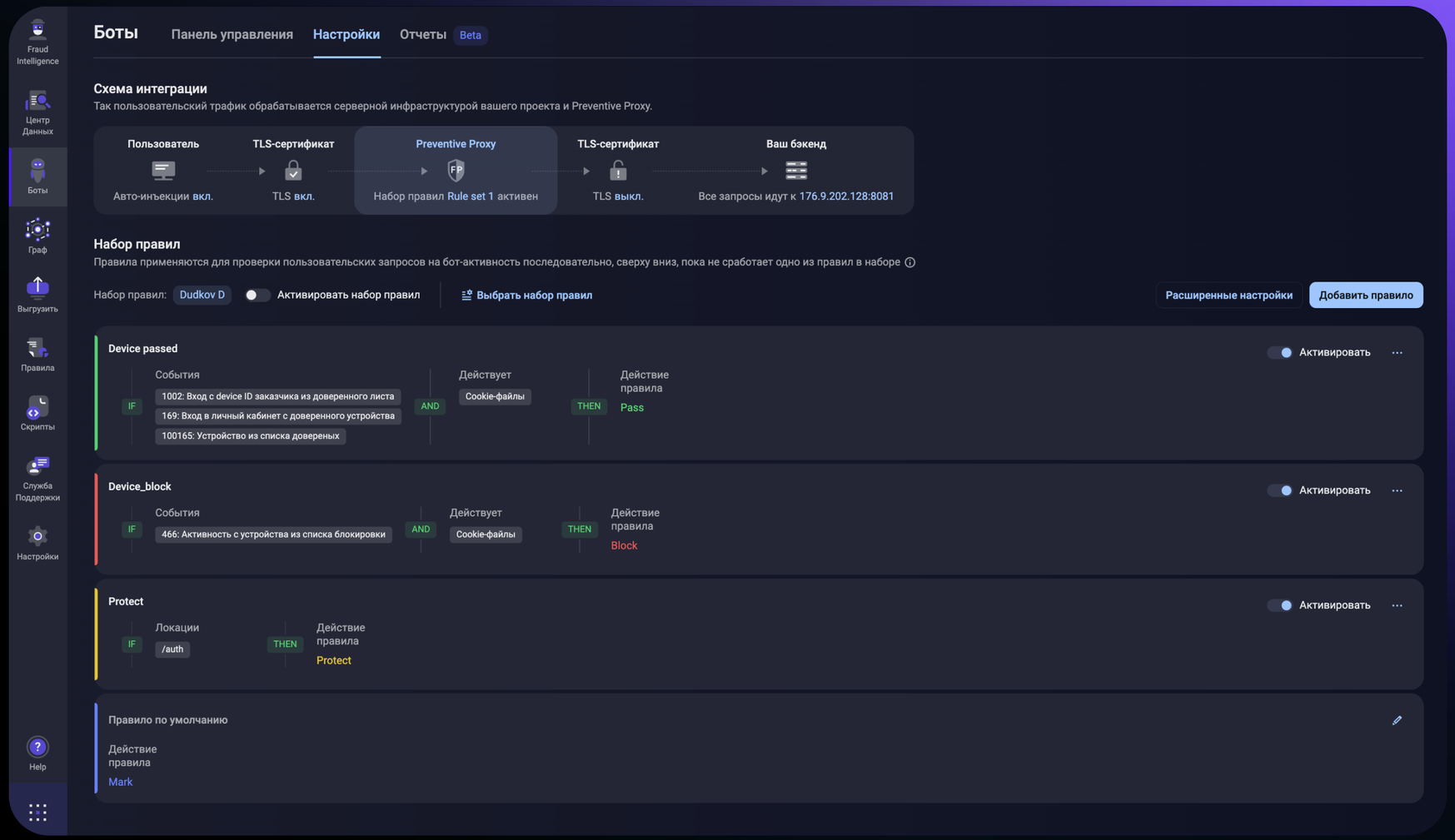
Контроль и оценка всех запросов

F6



Универсальная панель управления Правилами реагирования

F6

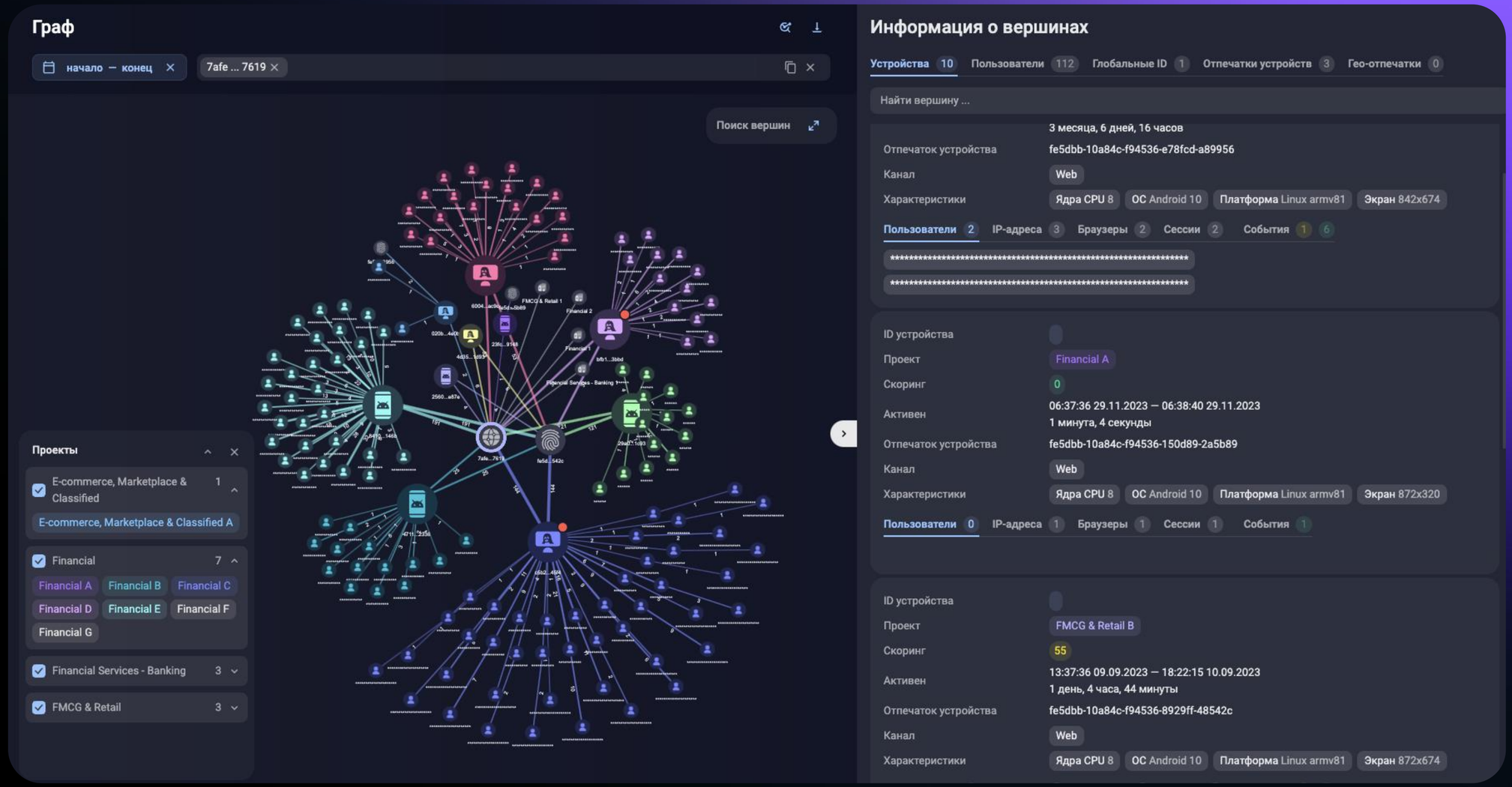


F6

Примеры атак FP

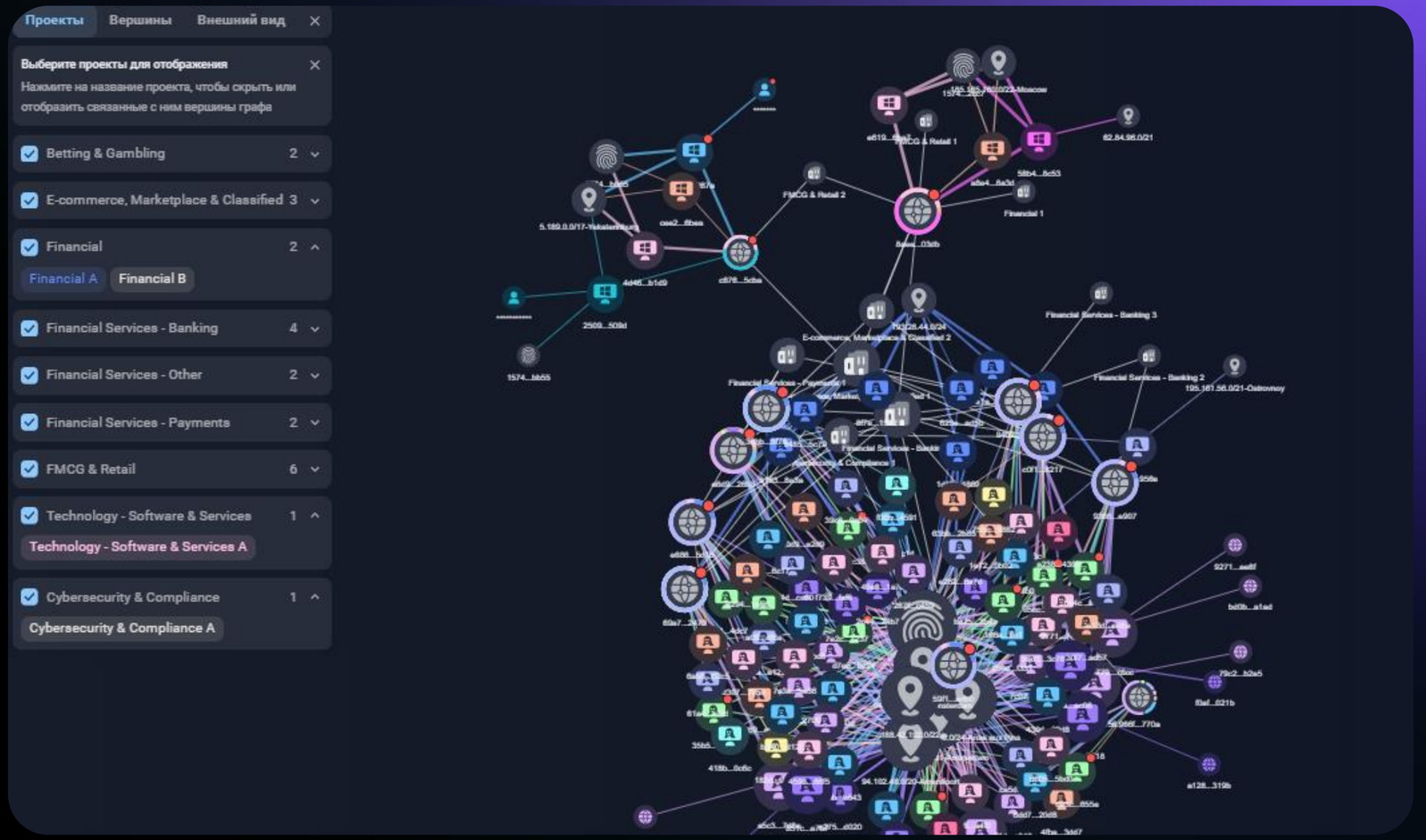
Активность устройства дроповода

F6



Сообщество F6. Сообща борется с киберпреступностью

KYC и AML, мошеннические подсети, Global ID



Обнаружение КРОСС-клиентских атак

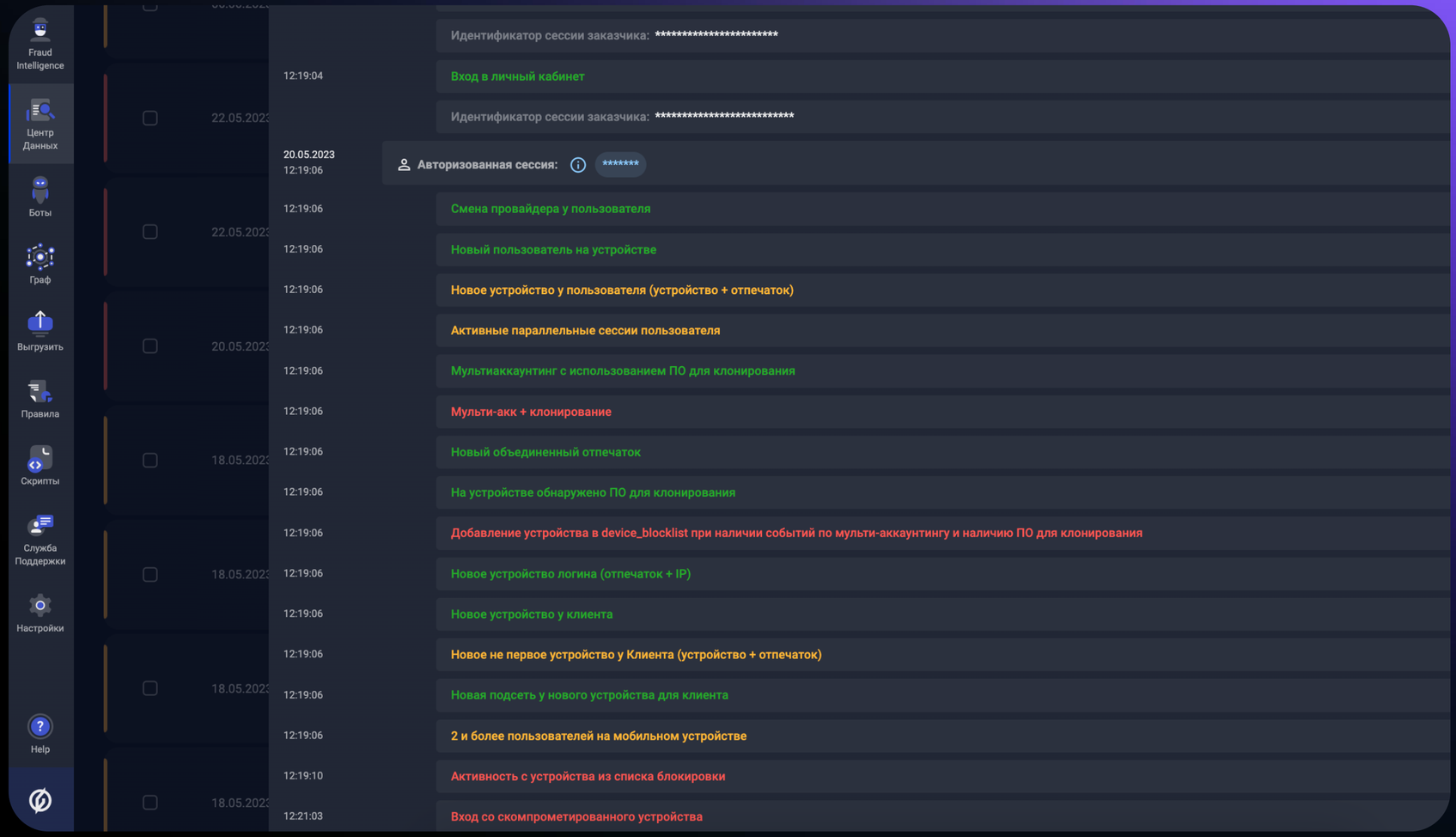
F6

Технология Global ID обеспечивает глобальную распределенную идентификацию пользователей.

Global ID позволяет обмениваться информацией о зафиксированных случаях аномальной активности во всех защищаемых приложениях. Если злоумышленники получили доступ к другим приложениям или клиентским платформам, Fraud Protection обнаружит совпадения Global ID между используемыми ими устройствами и учетными записями пользователей. Эти совпадения позволяют установить закономерности в действиях злоумышленников, а также выявить скомпрометированные учетные записи пользователей и устройства.

Мошеннические звонки и рассылки (удаленное управление)

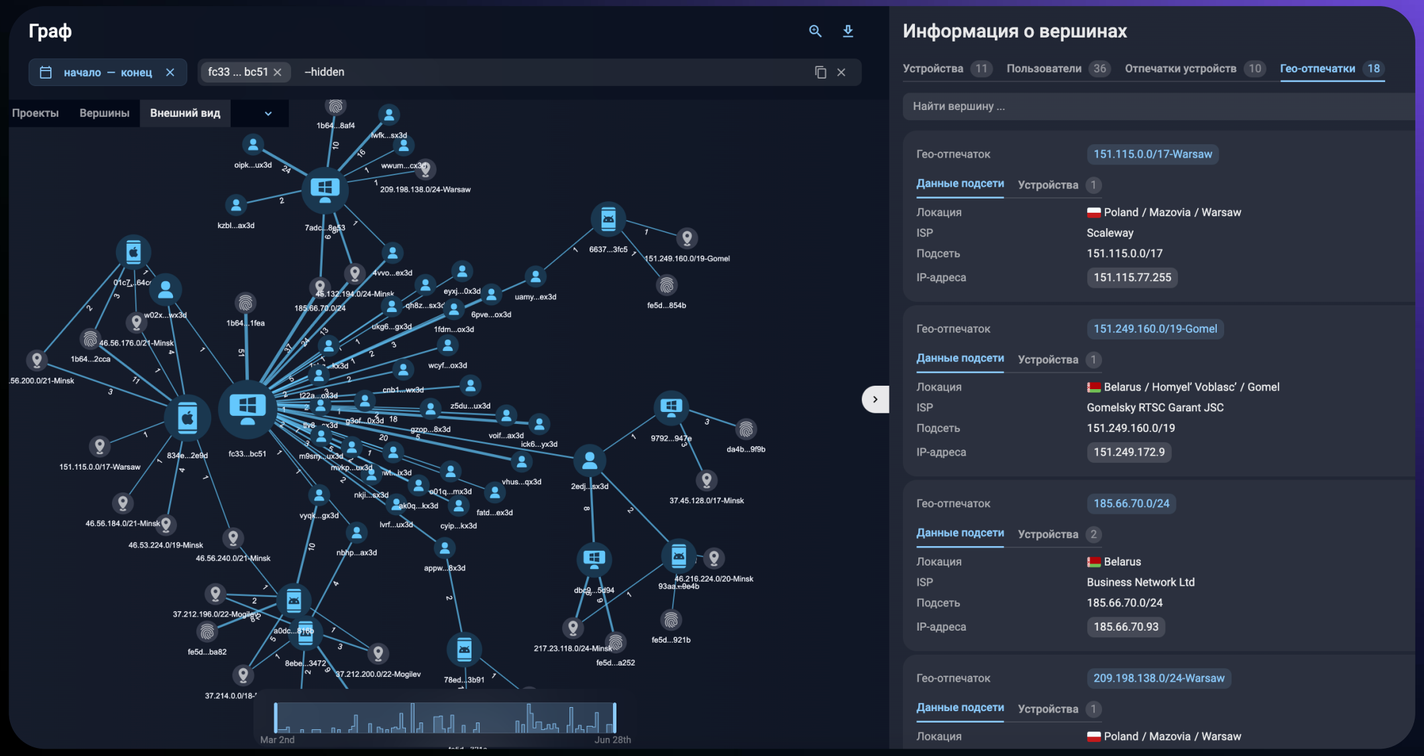
F6



Массовая авторизация/Brute force

F6

Массовая авторизация – высоко-рисковое поведение при котором через одно устройство происходит множественные входы в личные кабинеты разных учетных записей



* Событие проверяет количество уникальных учетных записей, которые используются на одном устройстве (agent_id), и если оно больше заданного порога событие сработает. Учитываются только успешные входы в систему. Может быть признаком мошеннических действий, направленных на хищение персональных данных, доступ к которым был получен путем фишинга или социальной инженерии.

Вредоносная кампания

F6

Воркер

Создает объявление
и ссылку на скачивание
мобильного приложения-
клона (APK) в Telegram-боте

**Объявление
с отключенной
доставкой**

Переход в
мессенджер

**Воркер присылает
ссылку на фейковый
сайт Google Play для
скачивания APK, либо
направляют приложение
через мессенджер**

**Жертва скачивает
и устанавливает APK,
заражение устройства**

**Кража логов
и перехват SMS**

Вбивер

Списывает
денежные средства

Находит объявление

Жертва

70% от краденной суммы перечисляет воркеру.
30% распределяется между «админом» сообщества и вбивером

Детектирование поддельных приложений

F6

Android: Выявлено фэйковое приложение с правами администратора

04.07.2024 в 14:54:08

Детали угрозы

Скоринг	Категория	Статус
91		Android

Данные


```
{
    "source_of_installation": "com.google.android.packageinstaller",
    "APK_NAME": "corners.spencrgherer.make",
    "APK_LABEL": "Мой МТС",
    "SHA1": "8a6405cfce043ab327b8b94717cafa3ce487a106",
    "installation_date": "2024-07-04T11:01:53.413Z",
    "permissions": ["SET_WALLPAPER", "REQUEST_IGNORE_BATTERY_OPTIMIZATIONS", "POST_NOTIFICATIONS", "READ_MEDIA_IM
    "flags": ["admin_enabled", "admin_active"]
}
```


Описание

Правило срабатывает при наличии на устройстве подозрительного приложения, маскирующегося под оригинальное приложение, и установленного из нелегитимного источника.

Выявление Buhtrap

F6

Распаковка и запуск Buhtrap RAT в памяти процесса rundll32.exe

Лоадер Buhtrap RAT

Удаленное управление зараженной машиной

Сохранение лоадера Buhtrap RAT на диск и его запись в автозагрузку

Актор

Wordpad.exe

Запуск wordpad.exe

Дроппер второй стадии

Распаковка следующей стадии и запуск в памяти процесса лоадера

Загрузка вредоносного архива

Вредоносный ZIP-файл

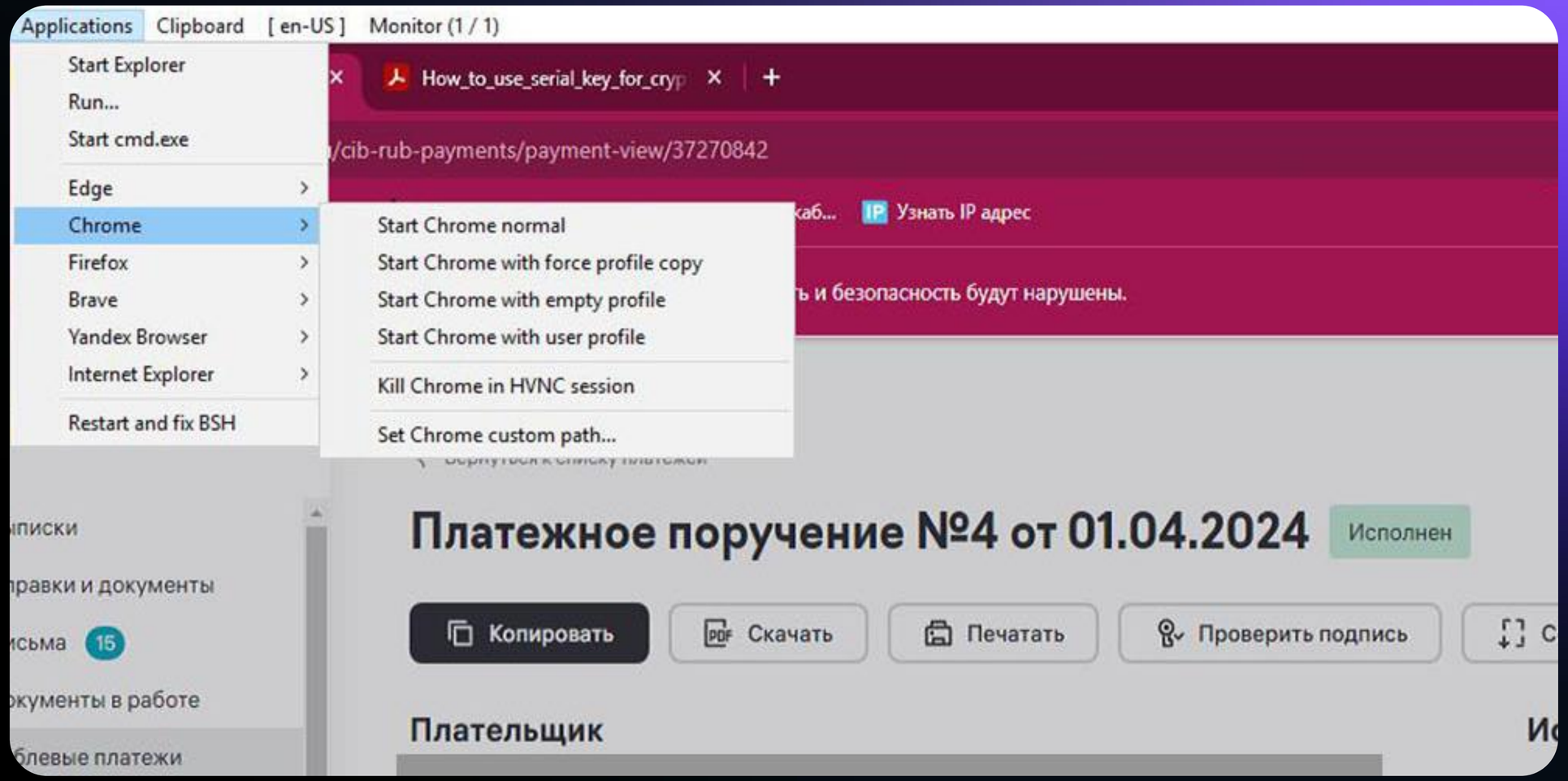
Распаковка содержимого архива

Дроппер второй стадии

Выявление Buhtrap

F6

Пример слежки злоумышленником за действиями бухгалтера



Детектирование удаленного управления

F6

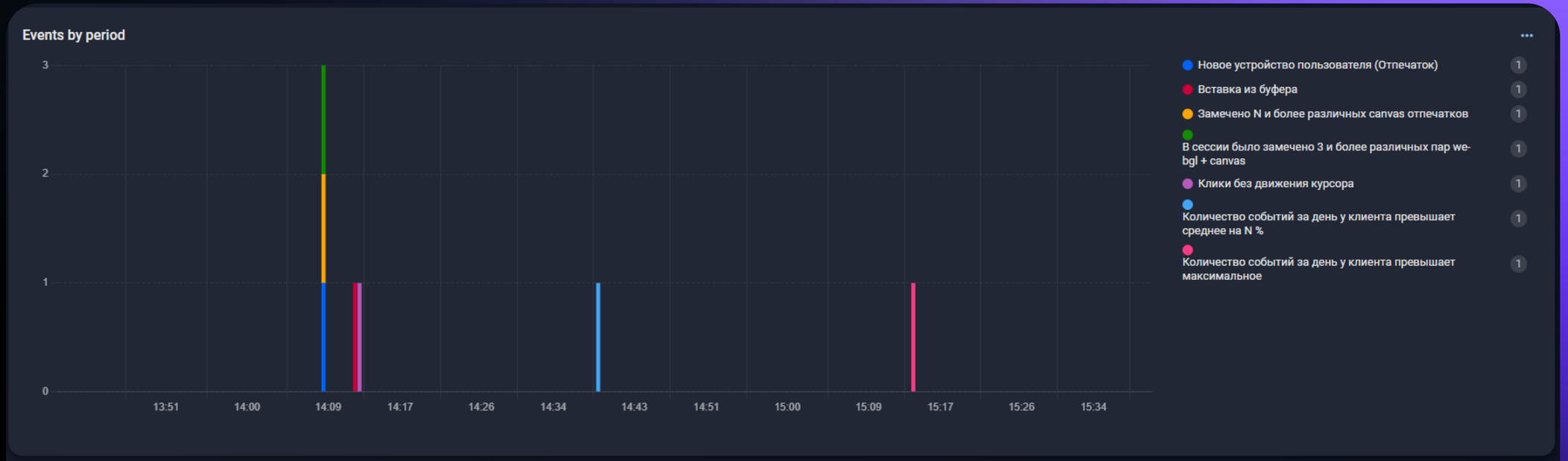


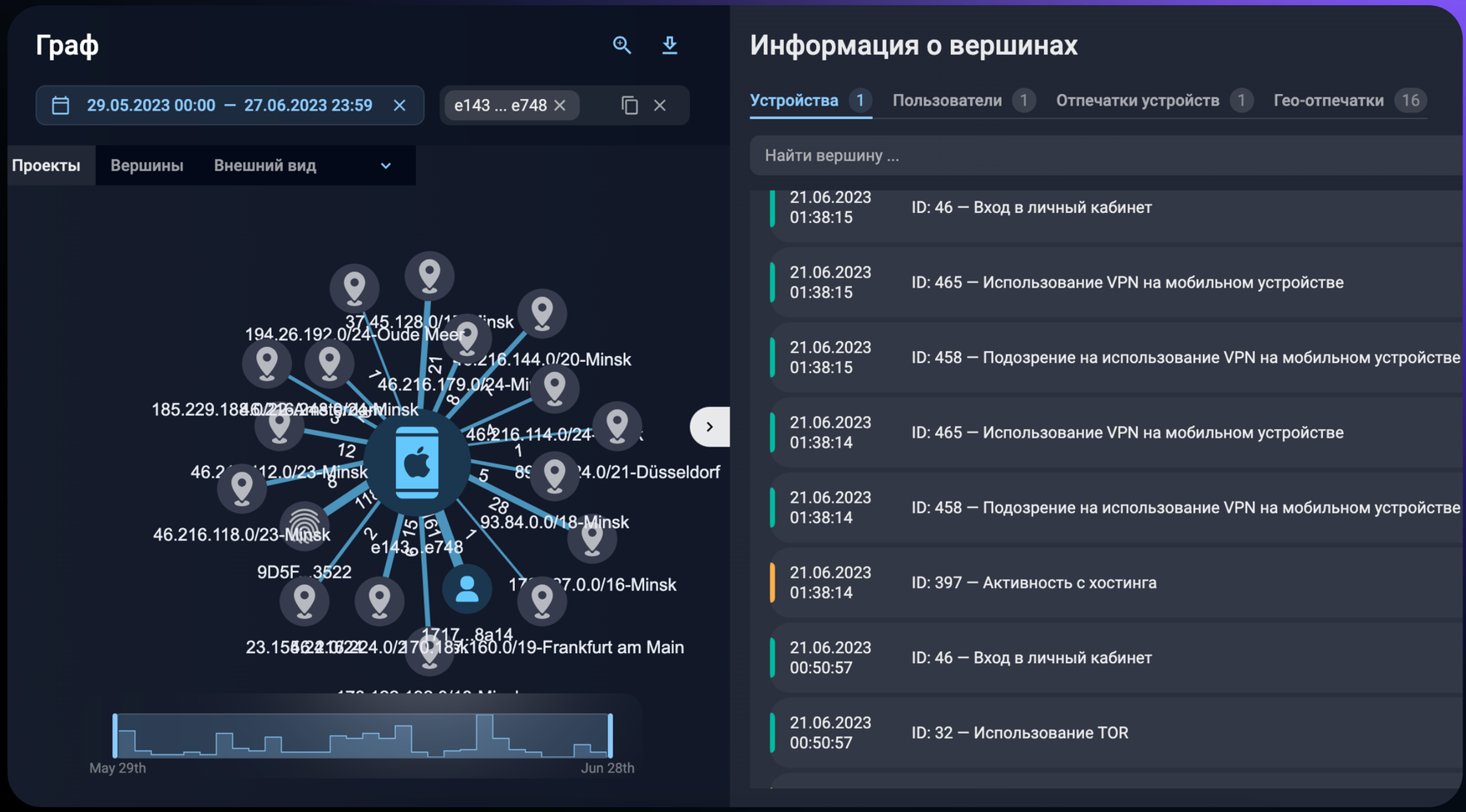
Таблица событий

Обнаружено событий: 7 Выгрузить

Время	Событие	Скоринг события	Global ID	Session ID	Дополнительный иден
2024.10.09 15:14:00	(ID: 1754) Количество событий за день у клиента превышает максимальное	0	16d5f44c-56ef-47b4-bb17-f3bb8e83c8cf	75ffab45-8603-11ef-bb60-8a1407da1fc0	—
2024.10.09 14:39:20	(ID: 1753) Количество событий за день у клиента превышает среднее на N %	0	16d5f44c-56ef-47b4-bb17-f3bb8e83c8cf	75ffab45-8603-11ef-bb60-8a1407da1fc0	—
2024.10.09 14:12:54	(ID: 385) Клики без движения курсора	0	16d5f44c-56ef-47b4-bb17-f3bb8e83c8cf	75ffab45-8603-11ef-bb60-8a1407da1fc0	—
2024.10.09 14:12:23	(ID: 129) Вставка из буфера	0	16d5f44c-56ef-47b4-bb17-f3bb8e83c8cf	75ffab45-8603-11ef-bb60-8a1407da1fc0	—

Использование средств анонимизации [hosting/VPN/Tor]

F6



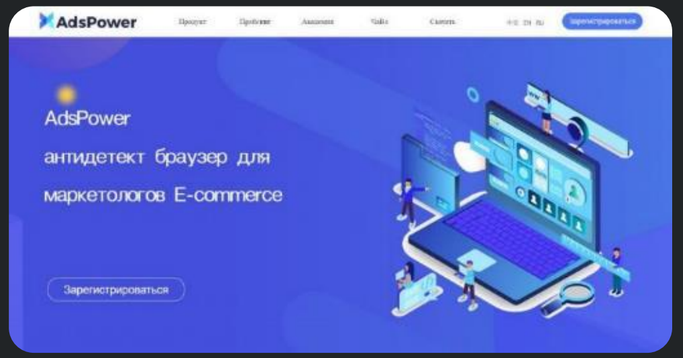
Root-доступ для подмены цифрового отпечатка, антидетект браузеры

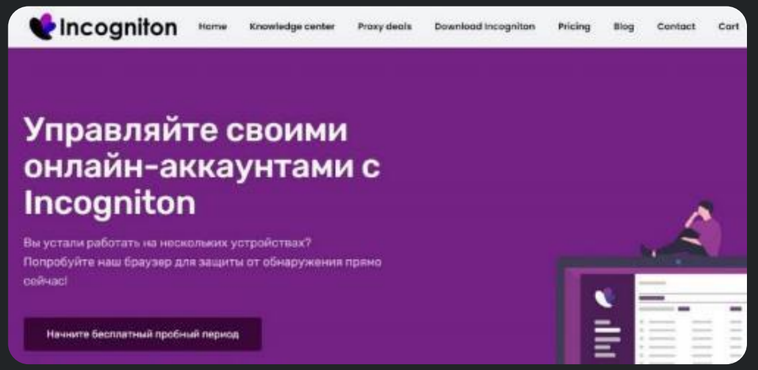
F6

Приложения, которые позволяют создавать и управлять большим количеством аккаунтов в параллель, использовать мультиаккаунтинг.

Аналогично клонированию приложений, зачастую используется для накруток, злоупотреблений и осуществления мошеннических действий.

- https://gologin.com
- https://incogniton.com
- https://www.clonbrowser.com
- https://multilogin.com
- https://indigobrowser.com
- https://beta.chebrowser.site
- https://antbrowser.pro
- https://antidetect.org
- https://ru.aezakmi.run
- https://ghostbrowser.com
- https://www.multibrowser.com
- https://kameleo.io
- https://sphere.tenebris.cc
- https://accovod.com
- https://www.ivanovation.ro/
- https://arbitrage-bets.com/
- http://samara-weblab.ru
- https://www.multiaccounter.com/
- http://lizard-program.ru/multi-browser.html
- http://ndalang.inflowtraffic.com
- https://cypher-antibrowser.net
- https://octobrowser.net
- https://www.adspower.net/
- https://undetectable.io
- https://fingerprints.bablosoft.com



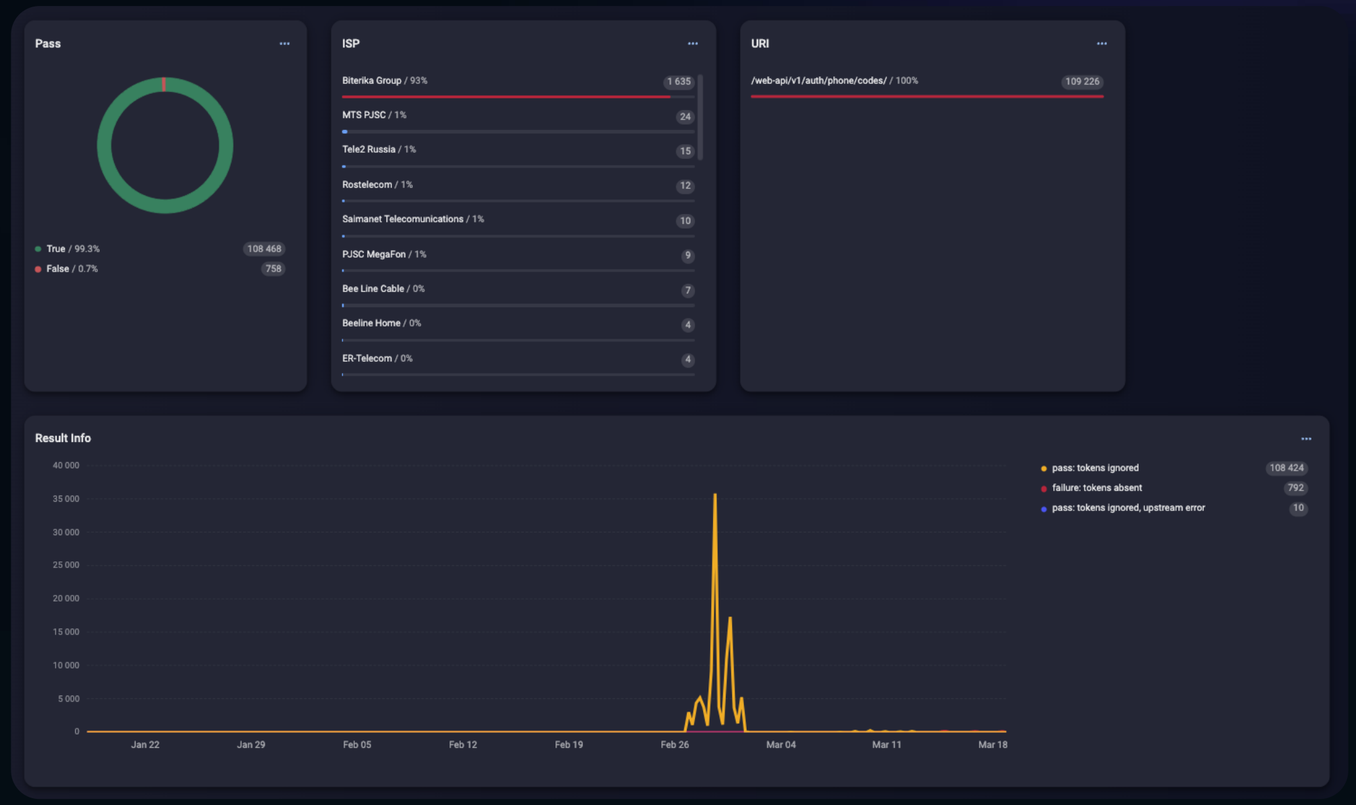


F6

Примеры атак

Статистика прямых запросов к API отправки SMS

Запросов обработанных Preventive proxy
за период с **26.02.2024** по **18.03.2024**



F6

Preventive Proxy - модуль в составе системы Fraud Protection. Preventive Proxy анализирует и применяет политики реагирования на бот-активность — выявляет автоматизированные средства для сбора данных и совершения действий на защищаемом ресурсе.

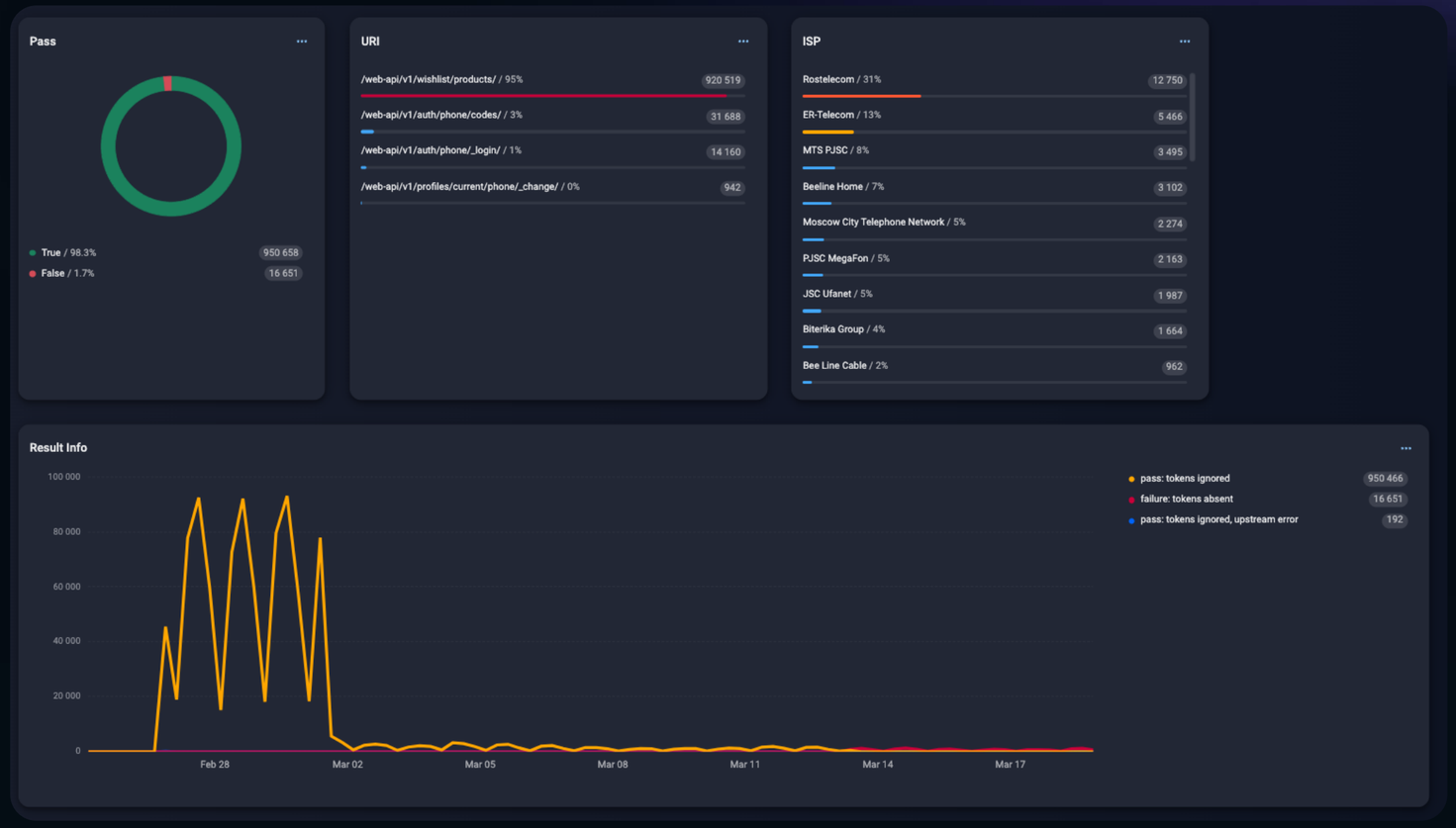
109 226

Прямых запросов с отсутствующими cookie GSSC/FGGS

Вердикт о наличии бот-активности может быть получен как через API, при обработке запросов на серверной стороне приложения, так и через файл cookie gssc (от англ. "Group-IB session score"), которая передается пользователю в веб- или мобильном приложении. Fraud Protection проверяет содержимое файла cookie gssc синхронно с обработкой пользовательского запроса без обращения к серверам Fraud Protection. Прямые запросы без gssc и fgssc являются прямым признаком нелетитимности запроса

Статистика прямых запросов к API

Запросов обработанных Preventive proxy за период с **26.02.2024** по **18.03.2024** к API предоставляющих определенные данные. Статистика доступна по ссылке.



F6

967 309

Прямых запросов с отсутствующими cookie GSSC/FGGS

Из аналитики исключены запросы с User-Agent содержащих информацию мобильных операционных систем, т.е. приведены данные сгенерированные в веб-канале, где всегда будут присутствовать cookie gssc/fgssc (подтверждение активной работы Web Snippet Fraud Protection)

Экономическая составляющая результата оценки нелегитимной активности

Приведена статистика явно поддающаяся экономической оценки

	Количество	Оценка потенциального ущерба ($)в месяц	Оценка потенциального ущерба ($)в год
Sms api	109 226*	2 184,52**	2 621 424**
Оценка возможных убытков системы лояльности	8 432***		84 320 ****
Итого			110 534,24

* количество запросов к /web-api/v1/auth/phone/codes/ с явным признаком нелегитимной деятельности, в которых отсутствовали cookie gssc/fgssc, за период времени 26.02.2024 -18.03.2024 только в веб-канале.

** оценочная стоимость затрат при использовании текущей системы защиты API отправки SMS-сообщений. Минимальная стоимость SMS без учета принадлежность к иностранным операторам сотовой связи, по данным сетевого ресурса **https://smsc.ru**

*** количество уникальных учетных записей использовавшихся в устройства с признаками мультиаккаунтинга (множественной авторизации).

**** - оценочная сумма возможных начислений клиентам выплат по системе лояльности (для одной учетной записи в расчет бралась 1000 рублей), для приобретения сопутствующего товара при отсутствии текущий системы защиты.

Web scraping

F6

Инструменты скрапинга:

скрипты инициализирующие прямые запросы без использования WebDriver.

Выявляются и блокируются путем проверки наличия и легитимности токенов gssc и fgssc.

Русскоязычные облачные сервисы:

Xmldatafeed **Диггернаут** **Catalogloader**

скрипты использующие WebDriver, средства автоматизации (Selenium, PhantomJS*, OpenBullet, PrivateKeeper и т.д.), специализированные браузеры (антидетект браузеры) инструменты автоматизации (BAS, ZennoPoster).

детектирование и блокирование запросов осуществляется путем поведенческого анализа, анализа пользовательской среды и выявления технически аномалий.

* Устройство, использующее PhantomJS, устраняет свои следы путем очистки истории браузера, cookies и т.п., смены IP-адресов, за счет чего оно выглядит новым устройством

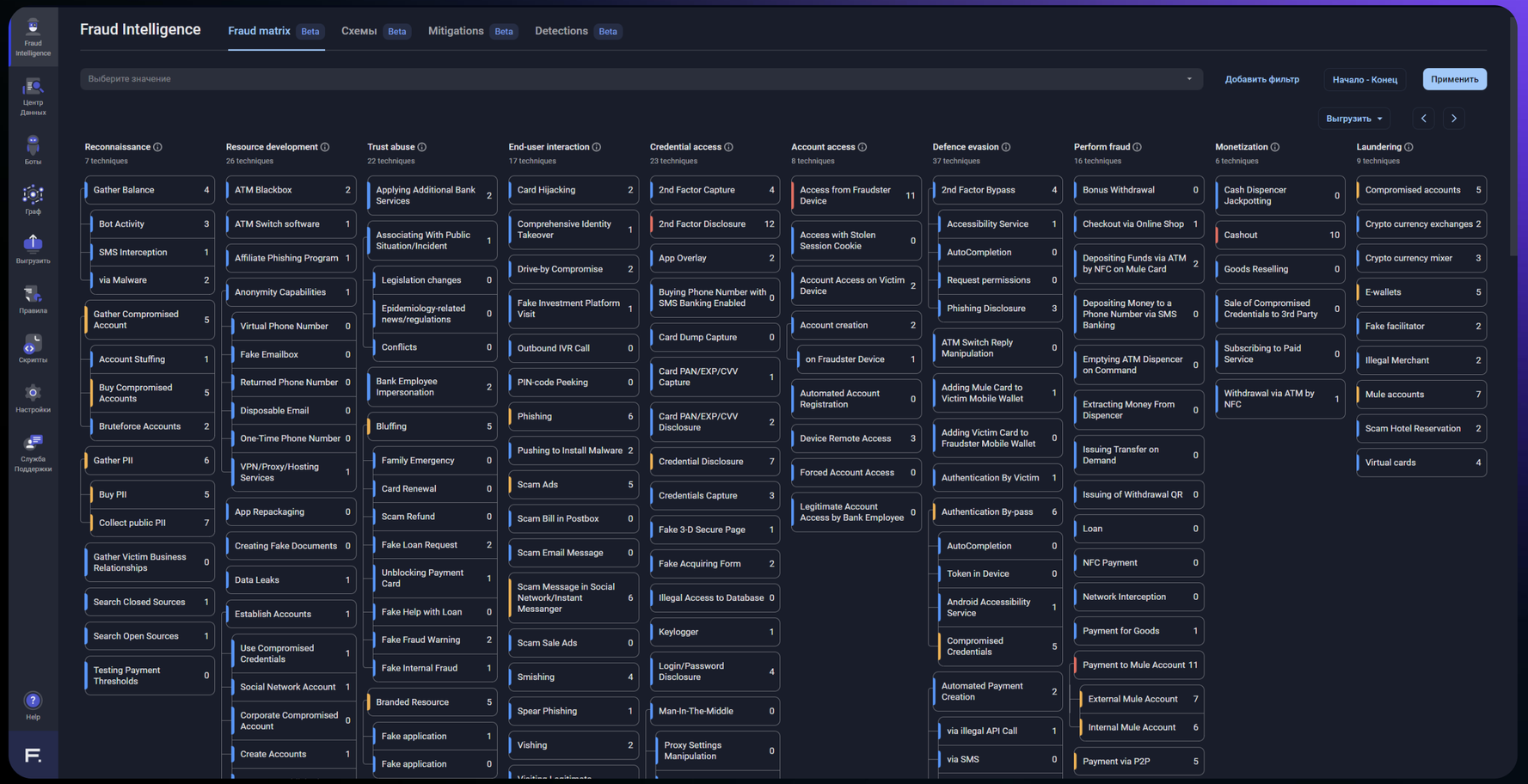
F6

Типизация мошенничества

Выявление мошенничества: знайте своих противников

F6

Fraud Intelligence – это матрица для структурирования, описания и накопления знаний о различных видах мошенничества и способах противодействия им.



Компании, интегрировавшие решение отмечают улучшение показателей бизнеса:

F6

До 30%

снижение убытков по сравнению с теми, кто отказался от получения актуальной киберразведки

До 50%

сокращение времени реагирования на инциденты

На 20%

повышение удовлетворенности клиентов за счет стабильной и надежной работы инфраструктуры

F6

Закажите бесплатный пилот прямо сейчас

Всего 1-2 месяца требуется для полной настройки решения
в инфраструктуре организации

f6.ru
info@f6.ru

f6.ru/blog
+7 495 984 33 64