Телефон: 8 (495) 532 28 73

mail@antifraud2.ru

www.antifraud2.ru

Сессионная антифрод система

WEB ANTIFRAUD

Сессионная антифрод система WEB ANTIFRAUD

Сессионная антифрод система WEB ANTIFRAUD предназначена для выявления мошенников и иной нежелательной активности среди пользователей интернет-сервисов.

Система основана на анализе параметров устройства пользователя, интернет-подключения и поведения пользователя при взаимодействии с сервисом заказчика.

Сессионный анализ позволяет оценивать уровень рисков сессии и выявлять риски до наступления нежелательного события (например, кражи средств со счета клиента в онлайн-банкинге). **Сессия** – каждое взаимодействие пользователя с сервисом, начиная с авторизации (ввод логина и пароля) и заканчивая выходом из личного кабинета.

Решаемые задачи

Проверка новых пользователей – оценка уровня риска новых пользователей при регистрации, подачи заявок без регистрации, оформлении новых заказов.

Защита учетных записей от кражи – выявление ситуаций, в которых существует вероятность доступа мошенников к аккаунту пользователя.

Защита мобильных приложений – выявление случаев модификации мобильных приложений, запуска на эмуляторах, множественных переустановок приложений и других рисков.

Определение реального IP адреса пользователя – в некоторых случаях при использовании прокси возможно раскрытие реального IP адреса пользователя.

Адаптивная аутентификация – определение необходимости запроса у пользователя дополнительного подтверждения (например, кода из смс) в зависимости от доверенности его окружения (устройство, локация и другие параметры).

Выявление фрода через мультиаккаунты – выявление связей между учетными записями, которые управляются одним человеком.

Выявление иных видов мошенничества – с помощью широкого спектра используемых технологий WEB ANTIFRAUD способен выявлять различные аномалии в технических и поведенческих данных пользователей.

Типы выявляемых рисков

WEB ANTIFRAUD выявляет широкий список аномалий в технических характеристиках устройства пользователя, поведенческие аномалии, определяет автоматизированную активность (в том числе продвинутых ботов), выявляет использование эмуляторов, наличие вредоносных программ (троянов) на устройстве, использование прокси, vpn, программ для удаленного доступа к устройству, связи между учетными записями и другие

типы рисков. Полный список выявляемых инцидентов доступен в технической документации (см. ниже).

Собираемые системой данные

Система собирает обезличенные технические и поведенческие данные. Система не собирает персональные данные. Информация об идентификаторах учетных записей пользователей (для их соотнесения с идентификаторами сессий) может быть зашифрована по согласованию с заказчиком.

Интеграция с проектом заказчика

Сайты – добавление JavaScript кода на значимые страницы сайта.

Мобильные приложения – добавление Mobile SDK для Android (Kotlin) и iOS (Swift).

Возможна, но не обязательна, интеграция Backend заказчика с Backend системы по API (Application Programming Interface, способ взаимодействия между программами). Backend интеграция позволяет системе выявлять дополнительные типы инцидентов.

Сложность интеграции зависит от архитектуры и реализации сервиса заказчика, поэтому в каждом случае необходима оценка способа интеграции с нашей стороны.

Интеграция со сторонним программным обеспечением

Система готова для интеграции со сторонним программным обеспечением (ПО), в том числе для обогащения собираемых сторонним ПО данных для принятия более эффективных решений. Сторонним ПО может выступать транзакционный антифрод, SIEM, Web Application Firewall и другое ПО.

Получение результатов работы системы

Аналитическая панель – интерфейс для ручного поиска данных аналитиком заказчика.

Backend API – получение данных программным способом по модели PULL (заказчик запрашивает данные) для автоматизированного принятия решений сервисом заказчика. Необходим для адаптивной аутентификации. Доступно несколько типов Backend API.

PUSH уведомления – отправка системой данных об инцидентах на API заказчика. Возможна доработка формата уведомлений под требуемый заказчику формат.

Система внесена в Реестр российского ПО

WEB ANTIFRAUD внесен в Реестр в 2022 году: https://reestr.digital.gov.ru/reestr/1258300/

Стоимость

Стоимость основана на количестве приобретаемых лицензий на ПО. Состоит из базового лимита лицензий, который оплачивается независимо от фактического использования, и дополнительного количества лицензий, которые являются превышением базового лимита за отчетный период.

Стоимость одной лицензии зависит от количества приобретаемых лицензий, сложности интеграции, решаемых заказчиком с помощью системы задач и других факторов, поэтому рассчитывается индивидуально.

Демонстрация и документация

По запросу предоставляется доступ к технической документации на систему (общие принципы работы, типы инцидентов, интеграция) и к тестовому стенду. Возможна демонстрация (создание тестового стенда) на инфраструктуре заказчика.

Контакты

Электронная почта: mail@antifraud2.ru

Телефон: 8 (495) 532 28 73

Сайт: https://www.antifraud2.ru