Описание функциональных характеристик ПО

Аннотация

Настоящий документ содержит сведения о функциональных характеристиках ПО “ИРИС (интернет риск скоринг)” (далее — ПО).

Описание и назначение ПО

ПО “ИРИС (интернет риск соринг)” (далее — программа, ПО) — программное обеспечение, представляющее собой облачный мониторинг, помогающий защитить маркетинговый бюджет и деньги клиентов от угроз.

ИРИС осуществляет непрерывный сессионный мониторинг, получая и анализируя информацию с устройств пользователя. Существуют различные способы получения данных и сигналов обратно от системы.

Наиболее распространенным вариантом использования является получение оповещений во время мониторинга транзакций с использованием серверного API - см. Серверно-ориентированный API, метод score_session.

Если вы хотите избежать дополнительной связи между серверами, или например, интегрировать антифрод с WAF, вы можете использовать механизмы интеграции на стороне пользователя - зашифрованные cookie или токены.

ПО позволяет :

- получение уведомлений о подозрительной активности на сервисе;
- анализ сессий пользователей, в том числе активных сессий;
- формирование отчетности об активности пользователей на сервисе клиента.

Функциональные характеристики:

- Выдача рекомендации по адаптивной аутентификации.
- Выдача текстового пояснения к результатам скоринга.
- Сбор следующих данных с мобильного устройства пользователя компонентом SDK (если у приложения есть необходимые разрешения):
- Идентификаторы устройства;
- Параметры сетевого соединения;
- Модель и имя устройства;
- Параметры процессора устройства;
- Параметры дисплей устройства;
- Наличие на устройстве Root/Jailbreak;
- Параметры установленной сим-карты;
- Список установленных приложений;
- Данные по кликам на экран;

- Данные с акселерометра и гироскопа.
- Сбор следующих данных с браузера с помощью JavaScript:
- Информация о браузере пользователя;
- Операционная система;
- Часовой пояс клиента;
- Языковые настройки;
- Параметры экрана монитора;
- Список установленных плагинов клиента в браузере;
- Список установленных шрифтов клиента;
- Данные по движению и кликам мыши в браузере;
- Возможность сбора цифровых отпечатков и характеристик пользовательских устройств, зафиксированных в онлайн сессиях пользователя.
- Возможность определения устройств, с которых осуществляется доступ в защищаемое приложение под множеством различных учетных записей.
- Наличие базы данных репутации IP-адресов, предназначенная в том числе для выявления использования адресов определенных категорий, имеющих повышенный уровень риска (VPN, VPS, Proxy, TOR).
- Возможность определения факта наличия на устройстве пользователя средства удаленного управления (RDP, VNC, TeamViewer и т. д.).
- Возможность определение факта использование средств для автоматизированной работы с ПО заказчика (ботов).
- Возможность получения информации о сессиях и алертах по API по HTTPS.
- Возможность получения информации о сессии по идентификатору.
- Возможность поиска сессий пользователя за период по идентификатору учетной записи.
- Возможность простановки идентификатора учетной записи на клиентской стороне для сопоставления потоков данных.
- Наличие рабочего места фрод-аналитика в виде тонкого клиента (выполнено по веб-технологии).

- Капча - определение реального пользователя от бота.

- Мониторинг и аудит сайтов мерчантов для оценки соответствия MCC, выявления фрод-признаков, репутационного и технического риска.

Основные компоненты платформы

К основным функциональным компонентам платформы относятся:

1. Модуль онлайн-скоринга. Позволяет получать информацию о сессиях и алертах по API.
2. Модуль интерфейса фрод-офицера. Позволяет просматривать информацию о сессиях и алертах по через веб-интерфейс.В веб интерфейс входит:

- Алерты:

Вкладка позволяет просматривать информацию об Алертах.Они указывают на то, что с сеансом происходит что-то подозрительное.
Поля:

  - t_ms: u64 - серверное время, когда был сгенерирован алерт;

- session_id: String - идентификатор сессии;
- name: String - название алерта, например “BOT” или “SUSPICIOUS_IP”;
- message: String - произвольный текстовый комментарий с дополнительной;
- информацией об алерте, должен бытьудобочитаемым для человека;
- confidence: Float - показатель уверенности от 0 до 1.

● Сессии:

На данной вкладке пользователь может проверить информацию о сессии.

● Активные сессии:

Вкладка позволяет просматривать информацию о сессии, которая произошла в недавнем времени.

● Скоринг:

Отображение запросов заказчиков на проверку сессии.

● Графики:

На данной вкладке происходит отображение аналитики различной информации.

3. Клиентский модуль сбора данных для веб сайтов и мобильных приложений. Позволяет собирать необходимую информацию с устройств пользователей.

Инструкция по эксплуатации интерфейса

Задача: “Просмотр Алерты”

Условия, при соблюдении которых возможно выполнение операции: Успешная регистрация в системе.

Подготовительные действия: Не требуются.

Затрачиваемые ресурсы: 1 минута.

Основные действия в требуемой последовательности:

1. Пользователь на панели управления переходит по вкладке “Алерты”. После чего появляется список.
2. При необходимости Пользователь может воспользоваться строкой поиска, введя имеющиеся данные:
   - ●Поиск по session_id;
   - ●Поиск по user_id;
   - ●Поиск по IP-адресу;
   - ●Также пользователь может установить лимит Алертов.
3. После чего пользователь нажимает на изображение лупы, для получения информации.Наименование алертов означает:
   - ●Название: ACCOUNT_TAKEOVER

Платформы: все

Необходимость передачи user_id: да

Описание: вероятно, другой человек пытается получить доступ к учетной записи с идентификатором user_id. Обратите внимание, что этот алерт работает только в том случае, если вы задали user_id в SDK, чтобы мы могли создать профиль поведения. Также мы используем только информацию о поведении для обнаружения атаки, это означает, что

злоумышленник может использовать то же самое устройство, что и легитимный пользователь (например, физически украсть его или использовать инструмент удаленного доступа). Такой подход улучшает качество обнаружения угроз.

Уровень опасности: высокий.

- Название: BOT

Платформы: все
Необходимость передачи user_id: нет
Описание: вероятно, пользователь не является живым человеком. Этот алерт включает в себя несколько подтипов: воспроизведение сеанса, сканирование системы безопасности, поисковые боты, автоматизация с использованием скриптов или сложных ботов. В случае срабатывания данного алерта, рекомендуется проверять данный сеанс с помощью капчи.
Уровень опасности: высокий.

- Название: COPY_PASTE

Платформы: web
Необходимость передачи user_id: нет
Описание: пользователь вставил данные в поле ввода вместо того, чтобы вводить их. Этот алерт удобен для целей тестирования.
Уровень опасности: низкий.

- Название: DEV_TOOLS

Платформы: web
Необходимость передачи user_id: нет
Описание: активна консоль разработчика в браузере, пользователь является разработчиком или проводит разведку перед атакой. Этот алерт удобен для целей тестирования.
Уровень опасности: низкий.

- Название: MULTI_ACCOUNT

Платформы: все.
Необходимость передачи user_id: да
Описание: для этого пользователя существует множество учетных записей (‘user_id’). Основан на отпечатке устройства, IP- адресе и поведении.
Уровень опасности: средний.

- Название: SUSPICIOUS_IP

Платформы: все
Необходимость передачи user_id: нет
Описание: IP-адрес пользователя присутствует в одном или нескольких черных списках, таких как TOR, VPN, прокси, рассылки спама и т.д. или имеет плохую репутацию.
Уровень опасности: низкий.

- Название: SUSPICIOUS_DEVICE

Платформы: Android, iOS
Необходимость передачи user_id: нет
Описание: рутованное или взломанное мобильное устройство и/или имеет плохую репутацию.
Уровень опасности: средний.

- Название: SCREENSHOT Платформы: Android, iOS

Необходимость передачи user_id: нет
Описание: пользователь сделал скриншот.
Может быть связано с социальной инженерией / мошенничеством с приложениями.
Уровень опасности: низкий.

● Название: PHISHING

Платформы: web.

Необходимость передачи user_id: нет

Описание: обнаружен необычный домен, возможно, кто-то готовит или совершает фишинговую атаку. Обратите внимание,что этот алерт является адаптивным, если вы добавляете новый законный домен, для первых сеансов может быть ложноположительный результат.

Уровень опасности: средний.

● Название: SESSION_HIJACK

Платформы: все

Необходимость передачи user_id: да

Описание: одновременные сеансы для одного и того же пользователя. Это может быть захват учетной записи или совместное
использование.

Уровень опасности: средний.

● Название: NEW_COUNTRY

Платформы: все

Необходимость передачи user_id: да

Описание: пользователь совершил вход из нетипичной для себя страны.

Уровень опасности: низкий.

● Название: NEW_CITY

Платформы: все

Необходимость передачи user_id: да

Описание: пользователь совершил вход из нетипичного для себя города.

Уровень опасности: низкий.

● Название: NEW_DEVICE

Платформы: все

Необходимость передачи user_id: да

Описание: пользователь совершил вход из нетипичного для себя устройства.

Уровень опасности: низкий.

● Также существует особый тип алерта, который называется “GOOD”.

Он сигнализирует о том, что поведенческий отпечаток пользователя совпадает с его предыдущими сессиями и /или пользователь успешно прошел капчу и не является ботом. Вы можете использовать этот алерт, чтобы установить приоритет этому пользователю во время DDoS-атаки, упростить процесс аутентификации и т.д.

4. Действие завершается при необходимости копированием показанной информации.

Задача: “Просмотр информации о Сессии”

Условия, при соблюдении которых возможно выполнение операции: Успешная регистрация в системе.

Подготовительные действия: Не требуются.

Затрачиваемые ресурсы: 1 минута.

Основные действия в требуемой последовательности:

1. Пользователь на панели управления переходит по вкладке “Сессии”. После чего появляется список.
2. При необходимости Пользователь может воспользоваться строкой поиска, введя имеющиеся данные:
    - Поиск по session_id;
    - Поиск по user_id;
    - Поиск по IP-адресу;
    - Поиск по application_id;
    - Поиск по device_id;
    - Также пользователь может установить лимит Сессий.
3. После чего пользователь нажимает на изображение лупы, для получения информации.
4. Действие завершается при необходимости копированием показанной информации.

Задача: “Просмотр информации о запросах клиента на проверку сессии”
Условия, при соблюдении которых возможно выполнение операции: Успешная регистрация в системе.
Подготовительные действия: Не требуются.
Затрачиваемые ресурсы: 1 минута.
Основные действия в требуемой последовательности:
1. Пользователь на панели управления переходит по вкладке “Сессии”. После чего появляется список.
2. При необходимости Пользователь может воспользоваться строкой поиска, введя имеющиеся данные:
    - Поиск по session_id;
    - Поиск по user_id;
    - Поиск по event_id;
    - Также пользователь может установить лимит Событий скоринга.
3. После чего пользователь нажимает на изображение лупы, для получения информации.
4. Действие завершается при необходимости копированием показанной информации

Задача: “Просмотр аналитики”
Условия, при соблюдении которых возможно выполнение операции: Успешная регистрация в системе.
Подготовительные действия: Не требуются.
Затрачиваемые ресурсы: 1 минута.
Основные действия в требуемой последовательности:
1. Пользователь на панели управления переходит по вкладке “Графики”. После чего появляется список.
2. В списке пользователь может выставить фильтр:
    - Период (10,30,40 дней);
    - Аналитика (Общая или по платформам).
3. После чего появятся графики.

Информация для контактов

Для контактов с командой разработчиков просьба обращаться по следующим контактам:

Тел.: +7985 970 44 94
e-mail: Tsavina@technoscore.ru
Фактический адрес разработчиков и тех поддержки:11113 Москва Вн.Тер. Муниципальный округ Перово Ш. Энтузиастов д 52 стр 32