**Модуль анализа клиентских сессий BotShield платформы SolarCloud**

**Оглавление**

1. Назначение и решаемые задачи ................................................................................3

1.1. Описание назначения ..........................................................................................3

1.2. Описание функциональных возможностей и решаемых задач.......................3

1.2.1. Настройки проекта ........................................................................................6

1.3. Условия эксплуатации.........................................................................................8

1.3.1. Требования к серверу приложения..............................................................8

1.3.2. Требования к автоматизированному рабочему месту пользователя .......8

**1. Назначение и решаемые задачи**

**1.1. Описание назначения**

Модуль анализа клиентских сессий предназначен для классификации трафика на уровне запросов к веб-приложению, допуска к веб-приложению легитимных клиентов и блокировки автоматизированных ботов. Платформа SolarCloud включает подсистему анализа клиентских сессий - BotShield. Клиент, подключаясь к веб-ресурсу, передаёт информацию о поддерживаемых алгоритмах шифрования в сетевом пакете, а также протоколов шифрования SSL/TLS. Некоторые алгоритмы шифрования характерны для клиентских браузеров, другие - для библиотек, позволяющих выполнять автоматизированные запросы, которые могут выполняться как для полезных действий, так и в интересах злоумышленников. Облачный сервис BotShield представляет собой комплексное решение, предназначенное для оценки клиентских сессий веб-сайтов и интернет-ресурсов от вредоносных ботов и автоматизированных атак. Применение такой системы позволяет сделать оценку каждого клиентского запроса к веб ресурсу для дальнейшего решения по блокировке конкретного запроса.

**1.2. Описание функциональных возможностей и решаемых задач**

**Основные функции модуля:**

* Оценка клиентских запросов в режиме потока;
* Оценка нелегитимности клиентской сессии;
* Принятие решения о блокировке на основе оценки запросов;
* Логирование запросов и их оценок.

**1.2.1. Настройки проекта**

* Пороги классификации. Модуль выдаёт вердикт в диапазоне от 0 (легитимный пользователь) до 1 (автоматизированный бот). Установкой порогов можно регулировать агрессивность модуля (например, сессии ниже 0.2 полагать легитимными, выше 0.8 – вредоносными).

**1.3. Условия эксплуатации**

**1.3.1. Требования к серверу приложения**

Для установки модуля анализа требуются следующие минимальные характеристики:

- 4-ядерный процессор с тактовой частотой 2.2 ГГц;

- объем оперативной памяти – 8 ГБ;

- минимальный объем жесткого диска – 100 ГБ SSD/ SAS HDD;

- поддерживаемые операционные системы.

Требования к программному обеспечению сервера:

- Операционная система – Linux Debian 12 (с доступом администратора) ;

Также на серверной части должно быть настроено подключение к внутренней сети компании.

**1.3.2. Требования к автоматизированному рабочему месту пользователя**

Требования к аппаратному обеспечению:

- Персональный компьютер с подключением к сети.