ОБНОВЛЕНО 16 МАР

База вредоносных сигнатур

DosGate ведет собственную обновляющуюся базу вредоносных сигнатур которая поддерживается внутренней командой аналитики ServicePipe и обновляется каждый час. База вредоносных сигнатур применяется на решении в автоматическом или полу-автоматическом режиме

Содержимое Базы Данных

- Настроенные профили и контрмеры (пресеты)
- Вредоносные TLS-отпечатки
- IPv4/IPv6-адреса участвующие в ДДоС-атаках
- IPv4/IPv6-адреса участвующие в вредоносной автоматизации (парсинг, взлом)

Доставка обновлений

- API
- Через веб-интерфейс DosGate
- JSON-файлы
- Через приватный репозиторий

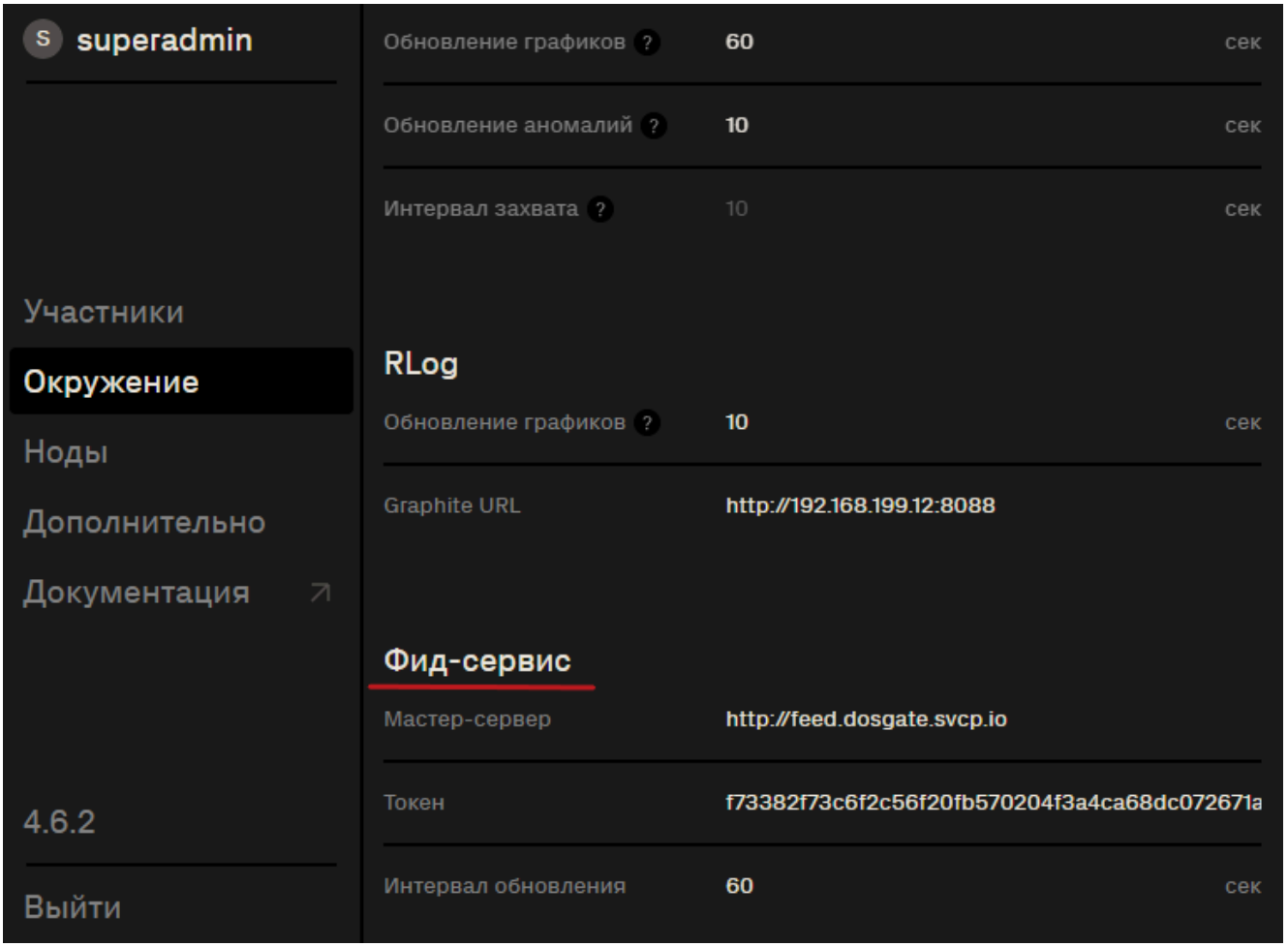
Подключение базы вредоносных сигнатур

- База вредоносных сигнатур распространяет компоненты-пресеты (готовые легитимные и вредоносные сигнатуры) для защиты сетевых сегметов и сервисов, а также вредоносные IP-списки. Она подключается и настраивается к веб-интерфейсу Spider через настройки окружения
- Содержимое базы вредоносных сигнатур уникально для каждого заказчика
- База вредоносных сигнатур поддерживается в Spider с версии 3.9.7

Шаг 1

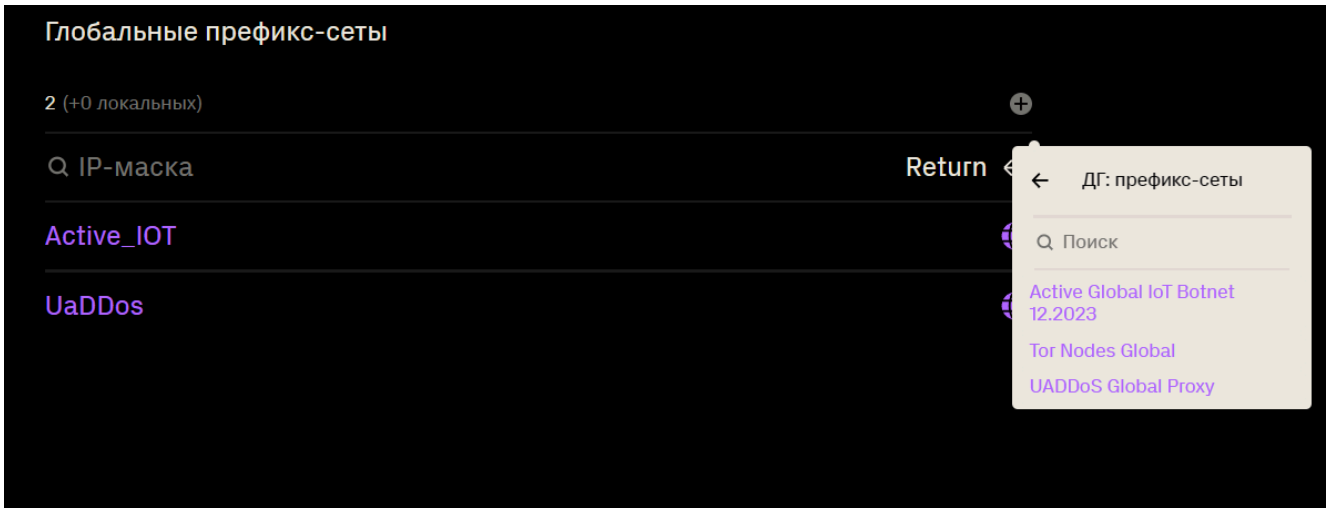
Получите от вендора ссылку на мастер-сервер базы вредоносных сигнатур и ключ

Шаг 2



Укажите ссылку и ключ в настройках окружения Spider. Также, укажите интервал обновления в секундах

Шаг 3



Компоненты-пресеты сразу появятся в вкладке пресетов. IP-списки нужно будет создать в глобальных префикс-сетах. После создания IP-списки будут обновляться сразу в уже созданном префикс-сете и создавать их повторно не потребуется

Все синхронизируемые с базой вредоносных сигнатур сущности помечаются фиолетовым цветом. Их нельзя изменить, но можно дублировать для дальнейшего изменения