ОБНОВЛЕНО 18 МАР

FlowCollector

FlowCollector — интеллектуальная система анализа потокового трафика, предназначенная для раннего выявления DDoS-атак и сетевых аномалий. Обеспечивает высокоскоростную агрегацию и обработку потоковых данных, выявляя подозрительную активность и автоматически инициируя защитные меры. Используется как самостоятельный детектор или как часть комплексной системы с DosGate.

Архитектура FlowCollector

FlowCollector реализует три ключевых направления работы:

- приём и агрегация потоковых данных (NetFlow v10 (IPFIX), NetFlow v9, sFlow, IMON);
- пороговая детекция трафика с применением векторных фильтров;
- формирование управляющих действий при обнаружении аномалий.

Потоковые записи обрабатываются в режиме реального времени. На основе указанных порогов и векторов производится вычисление нагрузки по IP-адресам, подсетям и направлениям. При превышении порогов система может сформировать маршрут очистки и направить трафик в защитный контур (например, через DosGate), а также зафиксировать событие для отчётности и анализа.

Модуль Data Explorer — хранит ретроспективные данные о трафике и событиях, обеспечивает быстрый поиск и анализ для последующего аудита или отладки порогов.

Возможности системы:

- **Детекция и противодействие DDoS-атакам**
  FlowCollector выявляет аномалии сетевого трафика на ранней стадии. В зависимости от конфигурации, возможны следующие действия: перенаправление трафика на системы фильтрации, генерация BGP FlowSpec или BGP Blackhole.
- **Поддержка потоковых протоколов**
  Поддерживает NetFlow v10 (IPFIX), NetFlow v9, sFlow, IMON и анализ зеркалированного трафика. Удобно встраивается в инфраструктуру любого уровня.
- **Высокопроизводительная обработка трафика**
  Одна нода обрабатывает до 250 000 flow в секунду при минимальной задержке.
- **Интеграция с системой фильтрации**
  При детектировании аномалии FlowCollector может перенаправлять трафик в DosGate с помощью отправки BGP анонсов для фильтрации DDoS-атаки. Управление DosGate и FlowCollector осуществляется через единый веб-интерфейс.

- **Аналитика и ретроспективный анализ**
  FlowCollector формирует и сохраняет отчёты с подробной информацией по каждой детектированной аномалии. С помощью модуля Data Explorer доступен полный набор метаданных из потоков NetFlow v10 (IPFIX), NetFlow v9, sFlow и IMON для ретроспективного анализа сетевой активности.
- **Техподдержка 24/7/365**
  Клиенты получают круглосуточную поддержку с реакцией до 5 минут по SLA.