ОБНОВЛЕНО 16 МАР

Что нового в FlowCollector

Раздел содержит изменения в системе FlowCollector. Обновления веб-интерфейса SP Spider вынесены отдельно.

- История версий SP Spider

Версия 1.6

Дата релиза: 30.09.2025

Новые возможности

FlowSpec-правила
Добавлены предустановленные FlowSpec-правила — механизм распространения фильтрационных политик на маршрутизаторы через BGP Flow Specification.

Фильтр источников по ifIndex для flow-протоколов
Точная фильтрация источников по интерфейсу.

Поддержка NetFlow v9
Приём и обработка потоков NetFlow v9.

Поддержка flow протокола IMON
Добавлена совместимость с протоколом IMON.

Опция disable для источников
Возможность отключить источник трафика на уровне конфигурации.

Улучшения

- Сделан исполняемым по умолчанию скрипт *bin/create_hugepages.sh*.
- Исключена запись *if_rx_octets* в режиме *save-flow*.
- В API **/managed-object/config** добавлен статус для каждого профиля.
- Параметр *rate* перенесён из **packet-counters** в секции **dpdk** и **ipfix**.

- Реализовано автоматическое переподключение к хранилищу потоков ClickHouse.

Версия 1.5

Дата релиза: 30.06.2025

Новые возможности

Автоматическое объединение локальных аномалий
Локальные аномалии могут объединяться в глобальную при выполнении заданных критериев.

Поддержка sFlow
Приём и обработка sFlow.

Авторизация к ClickHouse по логину и паролю
Поддержка user/pass в подключениях.

IPFIX: поля переменного размера
Поддержка variable-size полей.

Накопительная валидация опций в YAML
Ошибки по нескольким опциям собираются и показываются вместе.

Новые системные метрики по потокам
Добавлены группы метрик для `lcore-flow-rx/*`, `lcore-flow-worker/*`, а также агрегаты `flow/*`, `flow-ipfix/*`, `flow-sflow/*` (приём, обработка, передача, дропы).

Исправления

- Пропуск некорректных файлов профилей при старте. Повреждённые файлы не блокируют запуск.
- Корректное завершение детекций при остановке *DetectionService*.
- Удалён неиспользуемый параметр *metrics.interval*.
- Унифицированы значения временных интервалов в конфигурации.
- Удалены устаревшие ветки системных метрик: `ipfix-packets-pool/*`, `ipfix-packets-ring/*`, `lcore-rx-ipfix/*`, `lcore-worker-ipfix/*`.

Версия 1.4

Дата релиза: 11.03.2025

Новые возможности

Поддержка BGP FlowSpec
Реализована генерация событий BGP FlowSpec в ответ на обнаружение сетевых аномалий, что позволяет автоматически блокировать порты, используемые в атаках.

Функционал Router ID
Добавлена поддержка Router ID для группировки источников NetFlow с общими или индивидуальными счетчиками, что предотвращает ошибки, вызванные обработкой дублирующихся потоков.

Хранение SNMP в ClickHouse
Теперь данные SNMP сохраняются в ClickHouse рядом с NetFlow и используются в Data Explorer для классификации интерфейсов и анализа направлений сетевого трафика.

Поддержка IPv6 для ICMP Flood
Добавлена полная поддержка IPv6 для детекции атаки ICMP-flood.

Интеграция с NATS
Реализована поддержка NATS для передачи информации и событий о сетевых аномалиях, что повысило производительность системы.

Новые векторы детекции аномалий

- Детекция атаки HTTPS-flood
- Детекция атаки GRE-flood

Улучшения производительности

Запись метрик напрямую в ClickHouse
Метрики теперь записываются непосредственно в ClickHouse, что значительно повысило производительность параллельной записи метрик и статистики.

Оптимизация механизма детекции аномалий
Улучшена общая производительность системы, протестирована обработка атак на 2 миллиона IP-адресов одновременно.

Оптимизация обработки NetFlow

- Все входящие потоки NetFlow теперь сохраняются в ClickHouse для анализа в Data Explorer.
- Реализовано сжатие NetFlow-данных старше 24 часов для экономии места.
- Добавлена возможность произвольного поиска данных в SP Spider.

Улучшение обработки зеркалированного трафика
Общие оптимизации производительности.

Автоматическое распределение нагрузки по CPU
Оптимизирована работа сервиса Analyzer, теперь ресурсы автоматически распределяются между всеми ядрами процессора.

Повышение эффективности записи отчетов
Увеличена скорость записи отчетов и точность фиксируемых данных.

Исправления ошибок и мелкие улучшения

- Исправлена ошибка зависания маршрутов GoBGP.
- Поддержка 32-битных значений в IPFIX для совместимости со старыми или менее продвинутыми маршрутизаторами.
- Добавлены новые системные метрики: В FlowCollector появились метрики для отладки, включая количество экспортируемых метрик и число защищаемых хостов под анализом.
- Мелкие исправления ошибок и улучшения удобства использования.

Версия 1.0

Ручное создание дампов трафика
Добавлена возможность создавать дампы трафика в режиме port mirroring через API и Telegram-бота.

Новый формат оповещений Telegram и SMTP
Оповещения содержат ссылку на отчёт по аномалии.

Оптимизация производительности
Внесены общие улучшения работы системы.

Исправления ошибок
Исправлены выявленные ошибки.

Версия 0.6.94

Отчёты по аномалиям
Добавлен дашборд reports с подробными отчётами по каждой аномалии.

Интеграция с GoBGP
Добавлена поддержка отправки анонсов через GoBGP.

Автоматическая запись дампов трафика
Реализована запись дампов при аномалии в режиме port mirroring.

Новый формат Telegram-оповещений
Поддержана отправка дампов сразу после записи.

Дашборд Top-12 IP addresses
Добавлен новый дашборд по ведущим IP-адресам.

Версия 0.6.9

Поддержка Mellanox
Добавлена совместимость с сетевыми картами Mellanox.

Увеличение производительности
Общая оптимизация работы системы.

Версия 0.6.8

Отчёты по аномалиям
Добавлена генерация отчётов по каждой аномалии с детальной информацией о трафике.

SMTP-оповещения о начале аномалии
Добавлена поддержка SMTP-уведомлений.