

Интеграция с MP SIEM

Для того, чтобы реализовать синхронизацию правил корреляции/нормализации, необходимо произвести интеграцию Системы с MP SIEM. Для этого выполните следующие действия:

Шаг 1. Подключитесь к серверу, на котором развернута Система и перейдите в директорию **[LogIQ]/services/venus/**.

Шаг 2. Отредактируйте секцию **mpsiem_default** в файле **production.yml**, указав следующие данные:

- **hostname:** укажите IP-адрес **MPSIEM-Server**;
- **username:** укажите логин учетной записи с полными правами доступа к **MPSIEM Knowledge Base**;
- **password:** укажите пароль учетной записи с полными правами доступа к **MPSIEM Knowledge Base**.

Шаг 3. После того, как вы внесли изменения в файл, перезапустите все службы LogIQ, а затем вручную запустите синхронизацию в разделе **Настройки → Компоненты системы** веб-интерфейса.

ID статьи: 198

Последнее обновление: 23 дек., 2024

Обновлено от: Егоров В.

Ревизия: 1

База знаний LogIQ -> Документация -> Система хранения и обработки данных «LogIQ». Версия 2.3.0 -> LogIQ. Руководство администратора -> Синхронизация компонентов системы -> Интеграция с MP SIEM

<https://docs.axel.pro/entry/198/>