Интеграция с MP SIEM

Для того чтобы реализовать синхронизацию правил корреляции/нормализации, необходимо настроить интеграцию Логикор с MP SIEM.

При развертывании системы интеграция настраивается с помощью следующих параметров в файле **/etc/logiq/config.yml**:

```
saturn:
  manual_set_endpoints:
    mpsiem_rabbitmq: "localhost" # Укажите адрес rabbitmq MaxPatrol SIEM (ip либо FQDN, без указания порта)
  vault:
    secret_data:
      saturn:
        mpsiem_rabbitmq_username: "siem" # можно удалить после первого деплоя
        mpsiem_rabbitmq_password: "CHANGEME" # можно удалить после первого деплоя

venus:
  manual_set_endpoints:
    mpsiem_ptkb: "localhost" # Укажите адрес PTKB MaxPatrol SIEM (ip либо FQDN, без указания порта)
  vault:
    secret_data:
      venus:
        mpsiem_ptkb_username: "Administrator" # можно удалить после первого деплоя
        mpsiem_ptkb_password: "CHANGEME" # можно удалить после первого деплоя
```

Если при развертывании системы интеграция с MP SIEM не была настроена, ее можно выполнить вручную после установки. Для этого выполните следующие действия:

Шаг 1. Для синхронизации правил нормализации и корреляции настройте подключение к PTKB MP SIEM. В файл **/opt/logiq/services/venus/production.yml** добавьте:

```
mpsiem_default:
  hostname: "siem_ip_address"  # Укажите адрес PTKB MaxPatrol SIEM (ip либо FQDN, без указания порта)
  username: username  # Укажите пользователя PTKB MaxPatrol SIEM
  password: "CHANGEME"
  tables_used: []
```

Шаг 2. Также настройте подключение к RabbitMQ MP SIEM. Для этого в файл **/opt/logiq/services/saturn/config.yml** добавьте:

```
mpsiem_default:
  hostname: "siem_ip_address" # Укажите адрес rabbitmq MaxPatrol SIEM (ip либо FQDN, без указания порта)
  username: username # пользователь rabbitmq MaxPatrol SIEM
  password: "CHANGEME"
```

Шаг 3. Перезапустите сервисы Венера и Сатурн.

После перезапуска сервисов необходимо дождаться автоматической синхронизации правил или запустить ее вручную в интерфейсе системы на вкладке **Компоненты системы**.

По итогам синхронизации в веб-интерфейсе системы на вкладке **Конфигурационные файлы** бакета **saturn-pipeline** в директории **mpsiem_tags/siem_filter** появятся файлы **norm_rules_siem.yml** и **siem_filtration_rules.yml**. Необходимо настроить их использование в пайплайнах.

Шаг 4. В файле **parse/autonormalizer/_main.conf** замените:

- До:

  rules_filepath => "/usr/share/logstash/conf.d/mpsiem_tags/siem_filter/norm_rules_basic.yml"

- После:

  rules_filepath => "/usr/share/logstash/conf.d/mpsiem_tags/siem_filter/norm_rules_siem.yml"

Шаг 5. В файле **mpsiem_tags/_main.conf** замените:

- До:

  rules_filepath => "/usr/share/logstash/conf.d/mpsiem_tags/siem_filter/filtration_rules_basic.yml"

- После:

  rules_filepath => "/usr/share/logstash/conf.d/mpsiem_tags/siem_filter/siem_filtration_rules.yml"

ID статьи: 1639
Последнее обновление: 29 мая, 2026
Обновлено от: Михалева А.
Ревизия: 1