Table of Contents

Table of Contents 1
Настройка аналитики 2
Настройка аналитики (описание) 3

Настройка аналитики

Настройка аналитики (описание)

Documentation:
Product: SIEM
Version: 7.1.x

UserGate SIEM позволяет проводить анализ журналов событий безопасности, получаемых с настроенных сенсоров. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов. Подробнее об архитектуре и принципах работы функциональности SIEM читайте в разделе Аналитика Руководства администратора SIEM.

В интерфейсе CLI возможно создавать и настраивать правила аналитики и действия реагирования. С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные действия реагирования (реакцию) системы на создаваемые срабатывания. Все это позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Правила аналитики и действия реагирования в CLI создаются и настраиваются на уровне **analytics**.

Правила аналитики

С помощью правил аналитики происходит обработка событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников.

Для создания правила аналитики предназначена команда:

Admin@nodename# create analytics analytics-rules <parameters>

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	**on**/**off** — Включение/отключение правила аналитики для работы в режиме реального времени.
name	Название правила аналитики.
description	Описание правила аналитики.
threat-level	Уровень угрозы, который будет отображаться при срабатывании правила. • **informational**: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **low**: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **medium**: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. • **high**: события, требующие исследования и принятия мер. • **critical**: события, требующие исследования и срочного принятия мер.
priority	Показывает приоритет, установленный для срабатывания правила аналитики: • **low**: срабатывания данных правил обладают низким приоритетом реагирования. • **normal**: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. • **important**: на срабатывания данных правил необходимо обратить внимание и предпринять меры. • **critical**: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.

Параметр	Описание
alert-category	Отображает категорию, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: • **security**: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. • **availability**: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. • **performance**: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний могут быть созданы в библиотеке **Категории срабатывания**. Подробнее читайте в разделе Настройка категорий срабатывания.
timezone	Указывает на часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.
response-actions	Выбор действий реагирования, которые будут выполнены автоматически при срабатывании правила аналитики. Подробнее о создании действий реагирования и их настройке читайте в разделе Действия реагирования.
conditions	Указание условий срабатывания правила.

Условия срабатывания, которые указываются при создании правила аналитики, имеют следующие параметры настройки:

Параметр	Описание
name	Название условия правила аналитики.
description	Описание условия правила аналитики.
condition-time-enabled	Включить/отключить ограничение времени выполнения условия. При включении ограничения времени правило аналитики сработает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.
condition-time	Указывает на отрезок времени, за который условие должно выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание времени выполнения условия доступно при активированном параметре **condition-time-enabled**.
break-query-enabled	Включить/отключить использование запроса остановки в правиле аналитики.
break-query	SQL-подобный поисковый запрос остановки выполняется вместе с запросом условия. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы (задаётся аналогично запросу фильтра). Если при выполнении анализа найдётся хотя бы одна запись, соответствующая заданному запросу остановки, до того, как будет найдено заданное количество событий, соответствующих условию правила аналитики, то правило аналитики не сработает, а счётчик количества записей, найденных до выполнения запроса остановки, будет обнулён.
filter-query	Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно просмотреть в разделе Поиск и фильтрация данных. Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH. Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax.
group-by	Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания. О параметрах, по которым возможна группировка, читайте в разделе Поиск. При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра **pattern-repeats**.

Параметр	Описание
pattern-repeats	Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром **condition-time-enabled** или без него.

Для правил аналитики также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действия реагирования

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. UserGate SIEM позволяет гибко настраивать правила, используя переменные, относящиеся к категориям срабатывания правил аналитики.

Для создания действия реагирования предназначена команда:

Admin@nodename# create analytics response-actions <parameters>

Далее необходимо указать следующие параметры:

Параметр	Описание
enabled	on/off — Включение/отключение правила реагирования.
name	Название правила реагирования.
description	Описание правила реагирования.
action	Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики. Для выбора доступны следующие виды реагирования: • **send-email**: отправка письма на выбранные почтовые адреса. Настройка действия **Отправить email** будет рассмотрена далее в разделе Действие типа send-email. • **send-message**: отправка сообщения на указанные номера телефонов. Настройка действия **Отправить сообщение** будет рассмотрена далее в разделе Действие типа send-message. • **webhook**: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия **Webhook** будет рассмотрена далее в разделе Действие типа webhook. • **create-incident**: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия **Создать инцидент** читайте в разделе Настройки инцидентов. • **send-command-to-connector**: отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Действие типа послать send-command-to-connector. • **send-command-to-endpoint**: отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Действие типа send-command-to-endpoint.
enable-logging	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий SIEM.
grouping	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: • **never** — никогда. • **period** — при настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. • **number** — при настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
time-period	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.
alerts-number	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по их количеству.

Для действий реагирования также доступны команды **set** (редактирование), **show** (просмотр) и **delete** (удаление).

Действие типа send-email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Настройка профилей оповещений.
sender	Имя отправителя письма.
subject	Тема письма.
emails	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в библиотеке элементов. О добавлении почтовых адресов читайте в разделе Настройка почтовых адресов.
template	Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Действие типа send-message

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
notification-profile	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Настройка профилей оповещений.
sender	Имя отправителя письма.
phones	Список номеров телефонов получателей. Получатели должны быть добавлены в библиотеке элементов. О добавлении телефонных номеров читайте в разделе Настройка номеров телефонов.
template	Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
url	Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила.
template	Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Для тестирования webhook можно воспользоваться сервисом https://webhook.site. Для этого необходимо перейти на сайт Webhook.site и скопировать сгенерированную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле **url** параметра **action**.

Действие типа send-command-to-connector

В качестве одного из действий реагирования может быть настроена отправка команды на коннектор.

Если в качестве действия реагирования настроена передача команды для исполнения на коннекторе, то необходимо указать следующие параметры:

Наименование	Описание
connectors	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики. Коннектор должен быть заранее добавлен и настроен. Подробнее читайте в разделе Коннекторы. **Важно!** Могут выбраны только коннекторы с одинаковой группой команд.
command	Определение команды, которая будет передана на коннектор для выполнения; представлены команды группы, указанной для выбранных коннекторов. В случае наличия в команде переменных, будут отображены дополнительные поля для указания их значений. Подробнее о командах читайте в разделе Настройка команд.

Действие типа send-command-to-endpoint

В качестве одного из действий реагирования может быть настроена отправка команды на конечное устройство с установленным ПО UserGate Client. Доступны следующие команды:

- **block** — блокировка доступа к сети Интернет.
- **kill** — завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

В параметре **template** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле **template** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка email, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **create incident**, то текст будет отображён в описании инцидента.