

Table of Contents

Table of Contents	1
Аналитика	2
Общие сведения	3
Управление правилами аналитики	4
Поиск событий	6
Управление действиями реагирования	9
Управление срабатываниями правил аналитики	12
Просмотр подробной информации о срабатывании	13
Просмотр списка процессов конечных устройств	14
Использование списков из библиотек в поисковых запросах	15
Отправка уведомлений UserGate SIEM через Telegram	17

Documentation: 

Product: SIEM

Version: 7.x

Technology: SIEM

UserGate SIEM получает данные журналов событий безопасности [от модуля log-collector](#) и [от подключенных сенсоров](#) и записывает эти данные в единое хранилище для последующего анализа.

Администраторы могут управлять полученными событиями безопасности в разделе **Аналитика**. Для этого на соответствующих вкладках раздела вы можете:

- [настраивать правила аналитики](#);
- [выполнять поиск событий по заданным параметрам](#);
- [создавать действия реагирования для срабатываний правил аналитики](#);
- [управлять срабатываниями правил аналитики](#);
- [просматривать подробную информацию о срабатываниях правил аналитики](#);
- [просматривать список процессов конечных устройств](#).

Version: 7.x
Documentation: ☒
Product: SIEM
Technology: SIEM

События в UserGate SIEM хранятся в виде записей. Каждое событие (например, попытка входа в систему, изменение файла или сетевая активность) представляет собой отдельную запись. Для выявления взаимосвязи между событиями выполняется их корреляция на основе правил аналитики. Это позволяет обнаружить инциденты ИБ, которые могут быть пропущены при анализе каждого события в отдельности.

Правило аналитики содержит набор критериев и условий, по которым UserGate SIEM обнаруживает последовательности событий (корреляцию) в исторических данных из хранилища, а также в потоке данных реального времени, и генерирует [записи о срабатываниях](#) для оповещения администраторов об инцидентах ИБ. Правило аналитики также может определять [действия реагирования](#), которые следует выполнить UserGate SIEM при срабатывании этого правила, например, отправить уведомления по выбранному каналу связи или зарегистрировать инцидент безопасности для последующего анализа и расследования администратором.

По способу создания правила аналитики в UserGate SIEM делятся [на пользовательские правила](#), создаваемые администраторами в веб-консоли устройства, и [системные правила](#), которые вы можете импортировать из библиотеки правил аналитики для дальнейшего использования.

Работа с правилами аналитики

Список всех доступных правил аналитики отображается в разделе **Аналитика → Правила аналитики**.

Для каждого правила в таблице отображаются следующие параметры.

Параметр	Описание
Уровень угрозы	Уровень опасности угрозы (от 1 до 5, где 1 — очень низкий уровень), который определяет степень потенциального ущерба ИТ-инфраструктуре при срабатывании правила аналитики. Этот уровень также определяет интервал запуска правила
Название	Название, указанное при создании правила
Приоритет	Приоритет срабатывания правила аналитики: Низкий — имеет низкий уровень важности и не требует незамедлительного реагирования; Нормальный — требует обратить внимание и при необходимости принять соответствующие меры; Важный — требует обратить внимание и принять соответствующие меры; Критический — требует незамедлительного реагирования.
Категория срабатывания	Тип инцидента ИБ, на который указывает срабатывание правила аналитики. По умолчанию доступны следующие категории: Security — инциденты, приводящие к ослаблению безопасности информационных систем; Availability — инциденты, приводящие к ухудшению доступности информационных систем; Performance — инциденты, приводящие к снижению производительности информационных систем. Примечание Вы можете создавать дополнительные категории срабатываний правил аналитики в разделе «Настройки» → «Библиотеки» → «Категории срабатываний».
Условия	Условия срабатывания правила аналитики
Действия реагирования	Действия, которые выполняются при срабатывании правила аналитики

Вы можете управлять правилами аналитики в таблице: включать и отключать их состояние, а также удалять эти правила. Для этого необходимо выбрать нужные правила, удерживая клавишу Ctrl или Shift, и нажать соответствующую кнопку в панели инструментов.

Для дальнейшего анализа вы можете экспортировать данные о выбранных правилах и срабатываниях этих правил в файл формата BIN (по кнопке **Экспорт**). Кроме того, вы можете загружать правила аналитики в UserGate SIEM в виде файлов формата BIN или YAML (по кнопке **Импорт → Бинарный** или по кнопке **Импорт → YAML** соответственно).

Также вы можете фильтровать правила в таблице по состоянию. Так, например, можно просмотреть только правила во включенном состоянии, применив фильтр **Показать включенные**.

Для выбранного правила в таблице доступны следующие действия:

- изменение параметров правила по кнопке **Редактировать**;
- создание копии правила по кнопке **Копировать**;
- [просмотр списка срабатываний правила](#) по кнопке **Показать срабатывания**.

Все правила аналитики, находящиеся в таблице во включенном состоянии, используются для обработки данных, поступающих в UserGate SIEM в режиме реального времени. Запуск каждого правила выполняется с интервалом, соответствующим уровню опасности угрозы по срабатыванию этого правила (очень низкий, низкий, средний, высокий или очень высокий). Вы можете изменять интервалы запуска правил аналитики в окне конфигурации, доступном по кнопке **Настроить** в панели инструментов.

Конфигурация правил аналитики

Интервалы работы правил в режиме реального времени, мин

5

очень высокий:

2

4

высокий:

6

3

средний:

8

2

низкий:

14

1

очень низкий:

18

Сохранить

Отмена

Кроме того, вы можете запускать выбранное в таблице правило аналитики для обработки исторических данных по кнопке **Запустить сейчас**. В параметрах запуска правила необходимо указать период получения данных для обработки. Если требуется выполнить анализ всех данных из хранилища, необходимо снять флажок **Указать диапазон времени**. Для проверки работы правила вы можете установить флажок **Тестовый запуск**, при этом записи о

срабатывании правила генерироваться не будут.

Создание правила аналитики

Чтобы создать правило аналитики:

1. В разделе **Аналитика** → **Правила аналитики** нажмите **Добавить**.

2. На вкладке **Общие** выполните следующие действия:

- Включите правило аналитики. Включенное правило используется для обработки данных, поступающих в режиме реального времени.
- Укажите название и при необходимости описание правила аналитики.
- Выберите уровень опасности угрозы по срабатыванию правила аналитики (от 1 до 5, где 1 — очень низкий уровень угрозы).
- Выберите приоритет срабатывания правила аналитики.
- Выберите категорию срабатываний правила аналитики.
- Выберите часовой пояс правила аналитики (по умолчанию — UTC+0).
- Если требуется, чтобы для срабатывания правила аналитики все условия выполнялись в течение определенного времени, установите флажок **Ограничить общее время условий** и в поле **Общее время условий** укажите время в секундах.

3. На вкладке **Условия** нажмите **Добавить** и выполните следующие действия:

- Укажите название и при необходимости описание условия срабатывания правила аналитики.
- Если требуется, чтобы для срабатывания правила аналитики условие выполнялось в течение определенного времени, установите флажок **Ограничить время выполнения условия** и в поле **Время выполнения условия** укажите время в секундах.
- Если требуется, чтобы количество выполнений условия для срабатывания правила аналитики обнулялось по указанному запросу, установите флажок **Использовать запрос остановки** и в поле **Запрос остановки** введите выражение [на языке запросов](#). Для формирования запроса вы можете использовать доступные параметры и их значения, а также логические операторы и операторы сравнения.
- В поле **Запрос фильтра** введите условие срабатывания правила аналитики [с помощью языка запросов](#). В запросе вы можете указывать доступные параметры и их значения, а также логические операторы и операторы сравнения. Ниже в этом разделе приведены [примеры запросов для условий срабатывания правил](#).

Для формирования запроса вы также можете использовать оператор MATCH и синтаксис регулярных выражений библиотеки RE2. Описание библиотеки см. на сайте github.com в разделе компании Google.

Например, для обработки данных журнала событий конечных устройств можно ввести следующее условие:

```
source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'
```

Будет выполнен поиск событий из журнала Microsoft-Windows-Sysmon/Operational, связанных с запуском в командной строке Windows утилиты certreq.exe для отправки запроса на выпуск сертификата. Эти события могут указывать на попытки кражи или подделки сертификатов аутентификации злоумышленником.

- При необходимости укажите параметры, по которым будут сгруппированы срабатывания правила аналитики.
- В поле **Повторений шаблона** укажите количество выполнений условия для срабатывания правила аналитики.

ПримечаниеЕсли поле не отображается, необходимо увеличить размер окна свойств.

- Нажмите **Сохранить**.

Условие срабатывания правила аналитики отобразится в таблице на вкладке **Условия**. При необходимости вы можете добавить дополнительные условия срабатывания правила, повторив шаг 3 инструкции.

Порядок расположения условий в таблице соответствует порядку их применения в правиле аналитики при обработке событий. При необходимости вы можете изменять порядок с помощью кнопок **Наверх**, **Выше**, **Ниже**, **Вниз**.

4. При необходимости на вкладке **Действия реагирования** выберите действия, которые следует выполнять при срабатывании правила аналитики.

Вы можете выбирать действия из списка по кнопке **Добавить** [или создавать новые](#) по кнопке **Создать и добавить новый объект**.

5. При необходимости по кнопке **Запустить сейчас** запустите правило аналитики для обработки исторических данных из хранилища.

6. Нажмите **Сохранить**.

Примеры запросов для условий срабатывания правил

Ниже приведены примеры запросов, которые можно использовать при добавлении условий срабатывания правил аналитики, для выявления инцидентов ИБ в инфраструктуре организации.

Обнаружение брутфорса

Подбор множества паролей к одной учетной записи (брутфорс) можно обнаружить с помощью анализа событий, связанных с аутентификацией пользователей в системе. Для этого в условиях срабатывания правил аналитики вы можете использовать запросы следующего типа.

Пример запроса:

```
source = 'endpoint events log' AND logEventId = 4625 AND data MATCH 'Failure Reason:(\s*)Unknown user name or bad password.'
```

В журнале событий конечных устройств будет выполнен поиск записей о неудачной аутентификации в системе Windows по причине ввода неправильного логина или пароля. В качестве идентификатора события используется значение 4625, подробнее — [в документации Microsoft](#).

Пример запроса:

```
source = 'endpoint events log' AND logEventId = 4672
```

В журнале событий конечных устройств будет выполнен поиск записей, указывающих на вход в систему Windows пользователей с особыми (административными) привилегиями. В качестве идентификатора события используется значение 4672, подробнее — [в документации Microsoft](#).

Пример запроса:

```
source = 'endpoint events log' AND logEventId = 4624
```

В журнале событий конечных устройств будет выполнен поиск записей об успешном входе в систему Windows. В качестве идентификатора события используется значение 4624, подробнее — [в документации Microsoft](#).

Обнаружение изменения владельца файла

Для обнаружения подозрительной активности, связанной с изменением прав доступа к файлам в Unix-системах, вы можете использовать следующий запрос в условии срабатывания правила аналитики:

```
source = 'syslog' AND data ~ 'COMMAND=/bin/chown root' AND applicationName = 'sudo'
```

Среди данных, полученных от syslog-сервера, выполняется поиск записей об изменении владельца файла на пользователя root.

Поиск событий

Documentation: 
Product: SIEM
Version: 7.x
Technology: SIEM

В разделе **Аналитика → Поиск** отображаются записи о событиях безопасности, полученные из собственных журналов UserGate SIEM, а также из журналов [подключенных сенсоров](#).

В таблице событий вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки);
- просматривать подробную информацию о событии (по нажатию на иконку записи журнала);
- изменять формат отображения данных по кнопкам **Переключить в текстовый вид** и **Переключить в табличный вид** внизу таблицы.

Фильтрация данных о событиях

По умолчанию в таблице отображаются данные о событиях, полученные за все время. Вы можете изменить период отображения данных с помощью предустановленных значений. Для этого в раскрывающемся списке, доступном по кнопке **Все время** в панели инструментов, необходимо выбрать один из периодов.

Данные в таблице событий можно фильтровать с помощью специальных выражений [на языке запросов](#). Для формирования запроса вы можете использовать доступные параметры и их значения, а также логические операторы и операторы сравнения. Кроме того, вы можете добавлять запросы по ссылкам в таблице событий. Так, например, по нажатию на значение IP-адреса источника в строку фильтрации добавляется соответствующий запрос с IP-адресом источника взаимодействия (например, `ipSource = '203.0.113.1'`).

Также в запросе вы можете использовать оператор `MATCH` и синтаксис регулярных выражений библиотеки RE2. Описание библиотеки см. на сайте [github.com](#) в разделе компании Google.

Вы можете использовать запросы в строке фильтрации в качестве условий срабатывания новых правил аналитики. Для этого необходимо ввести запрос и в панели инструментов нажать кнопку **Добавить правило**. Дальнейшие действия аналогичны [созданию правила аналитики](#). Также вы можете добавлять запросы для условий срабатывания правил аналитики, созданных ранее. Для этого необходимо ввести запрос и в панели инструментов нажать кнопку **Добавить условие**.

Кроме того, вы можете сохранять примененные фильтры по кнопке **Сохранить как**. Список сохраненных фильтров доступен по кнопке **Популярные фильтры**. Также для дальнейшего анализа вы можете скачать отфильтрованные данные таблицы в виде CSV-файла по кнопке **Экспортировать в CSV**.

Просмотр записи о событии

Запись о событии в таблице может содержать данные, приведенные в таблице ниже. Наличие того или иного параметра зависит от журнала, из которого получено событие.

Параметр	Описание
Узел	Имя устройства
Время	Дата события
Время первого события	Дата и время первого срабатывания правила
Время последнего события	Дата и время последнего срабатывания правила
Источник	Журнал, из которого получено событие
Важность	Присвоенная событию степень важности. Могут быть указаны следующие значения: • Критичные; • Ошибки; • Предупреждения; • Информационные
Компонент	Компонент устройства
Тип события	Тип события
Пользователь	Имя пользователя
Модуль	Модуль устройства
Учет изменений	Тип изменений
Данные	Описание события
Информация	Детали события
Правило	Название правила
Действие	Действие при срабатывании правила
Приложение	Название приложения в системной библиотеке
Угроза приложения	Уровень опасности приложения
Сетевой протокол	Сетевой протокол
Протокол прикладного уровня	Протокол прикладного уровня и его версия
Категории сайтов	Категория URL
Угроза URL-категории	Уровень опасности категории URL
Причины	Причины, указанные в журнале веб-доступа (например, причина блокировки)
HTTP-метод	Метод HTTP-запроса

Параметр	Описание
Код ответа HTTP	Код HTTP-ответа
Тип контента	MIME-тип запроса
URL	URL-адрес ресурса
Реферер	Заголовок Referer в запросе
Операционная система	Тип ОС источника запроса
User-agent	User-Agent браузера
Сигнатуры COB	Название сигнатуры COB
Угроза сигнатуры	Уровень угрозы сигнатуры COB
Зона источника	Название сетевой зона источника
IP-источника	IP-адрес источника
Порт источника	Номер порта источника
MAC-источника	MAC-адрес источника
Зона назначения	Название сетевой зоны назначения
IP-назначения	IP-адрес назначения
Порт назначения	Номер порта назначения
MAC-назначения	MAC-адрес назначения
NAT-адрес источника	IP-адрес источника после NAT-трансляции
NAT-порт источника	Порт источника после NAT-трансляции
NAT-адрес назначения	IP-адрес назначения после NAT-трансляции
NAT-порт назначения	Порт назначения после NAT-трансляции
Байт отправлено/получено	Количество отправленных и полученных байтов соответственно
Пакетов отправлено/получено	Количество отправленных и полученных пакетов соответственно
Конечное устройство/сенсор	ID сенсора
Счетчик	Имя счетчика
Объект SNMP	Идентификатор SNMP-объекта (SNMP OID)
Тип SNMP-объекта	Тип SNMP-объекта
Статус	Статус выполнения запроса к сенсору WMI или SNMP
Ошибка	Код ошибки при выполнении запроса к сенсору WMI или SNMP
Протокол АСУ ТП	Протокол прикладного уровня АСУ ТП
Уровень лога	Уровень важности события Windows. Могут быть указаны следующие значения: • Error — события, указывающие на существенные проблемы, которые могут привести к потере функциональности или данных; • Warning — события, указывающие на проблемы, которые не требуют немедленного реагирования, но могут привести к ошибкам в будущем; • Information — информирующие события, которые не требуют немедленного реагирования; • Audit Success — события при успешном обращении к ресурсам; • Audit Failure — события при неуспешном обращении к ресурсам
Источник журнала событий	Источник события Windows
Категория лога	Категория события Windows
Категория задачи	Категория задачи Windows
Имя компьютера	Имя источника события
Код события лога	Код события Windows
Идентификатор события лога	ID события Windows

Параметр	Описание
Тип события лога	Тип события Windows, которому соответствует определенный уровень важности события (см. параметр Уровень лога). Параметр относится к записям журнала событий конечных устройств. Могут быть указаны следующие значения: 1 — ошибка; 2 — предупреждение; 3 — сведения; 4 — аудит успеха; 5 — аудит отказа
Строка вставки	Данные события Windows после обработки
Файл журнала лога	Журнал Windows. Могут быть указаны следующие значения: Application — журнал приложений, содержащий события приложений и служб; Security — журнал безопасности, содержащий события системы аудита; System — системный журнал, содержащий события драйверов устройств; CustomLog — пользовательский журнал событий, содержащий события, зарегистрированные определенными приложениями
Команда	Код функции ACU ТП
Адрес регистра	Адрес регистра ACU ТП
Номер ASDU	Адрес ASDU (COA) для протокола IEC-104
Идентификатор устройства	ID устройства из базы данных OPC-сервера для протокола OPC UA
Имя переменной	Имя переменной для обмена данными в режиме реального времени по протоколу MMS
Хэш	Хеш-сумма приложения
Объект	Категория события syslog
Критичность	Уровень важности события syslog
Идентификатор процесса	ID процесса

Technology: SIEM

Version: 7.x

Documentation: 

Product: SIEM

В разделе **Аналитика → Действия реагирования** отображается список действий, которые выполняет UserGate SIEM при срабатывании того или иного правила аналитики. Действия реагирования назначаются каждому правилу аналитики при его создании.

Вы можете управлять действиями реагирования в списке: создавать, изменять, копировать и удалять действия реагирования, а также включать и отключать их. Для этого используются соответствующие кнопки в панели инструментов. Также вы можете фильтровать действия реагирования в списке по их состоянию. Так, например, можно просмотреть только включенные действия реагирования, применив фильтр **Показать включенные**.

При создании действия реагирования для выбора доступны следующие действия:

- отправка уведомлений по каналу связи:
 - [на электронную почту](#);
 - [номер телефона](#);
 - [URL-адрес](#) (с помощью механизма webhook);
- [регистрация инцидента](#);
- [отправка команды на коннектор](#);
- [отправка команды на конечное устройство](#).

Создание действия реагирования

Чтобы создать действие реагирования:

1. В разделе **Аналитика → Действия реагирования** нажмите **Добавить**.

Откроется окно создания действия реагирования.

2. На вкладке **Общие** выполните следующее:

- Включите действие реагирования.
- Укажите название и при необходимости описание действия реагирования.
- Выберите действие, которое следует выполнять при срабатываниях правила аналитики:
 - отправлять уведомления о срабатывании на указанные адреса электронной почты;
 - отправлять уведомления о срабатывании на указанные номера телефонов;
 - отправлять уведомления о срабатывании с помощью механизма webhook на указанный URL;
 - регистрировать инцидент;
 - отправлять команду на выбранный коннектор;
 - отправлять команду на конечное устройство.
- Если требуется журналировать данные действия реагирования, установите флажок **Записывать в журнал правил**. Записи о выполнении действия реагирования будут отображаться в журнале событий UserGate SIEM в разделе **Журналы и отчеты → Журналы**.
- Если требуется выполнять действие реагирования для группы срабатываний, настройте группировку срабатываний правила аналитики по одному из следующих параметров:
 - **Никогда**. По умолчанию группировка отключена.
 - **За период времени**. Действие реагирования будет выполнено, если в течение указанного времени правило аналитики работает хотя бы один раз.
 - **По количеству срабатываний**. Действие реагирования будет выполнено после указанного количества срабатываний правила аналитики.
 - **В существующий инцидент**. Параметр доступен только при выборе действия **Создать инцидент**. По первому срабатыванию правила аналитики будет зарегистрирован инцидент, а все последующие срабатывания правила будут добавляться в этот инцидент в виде новых записей в блоке **Срабатывания**.

3. На вкладке **Действие** укажите параметры, соответствующие действию, выбранному на шаге 2. Ниже приведены параметры для каждого действия.

Для отправки уведомлений на электронную почту укажите следующие параметры:

- [Профиль оповещения SMTP](#), который будет использоваться для отправки уведомлений.
- Адрес электронной почты отправителя.
- Тему уведомлений.
- Группы адресов электронной почты получателей уведомлений. По кнопке **Добавить** вы можете выбрать [группы адресов](#), созданные в разделе **Настройки → Библиотеки → Почтовые адреса**. Также вы можете создавать новые группы адресов по кнопке **Создать и добавить новый объект**.

Для отправки уведомлений на номер телефона укажите следующие параметры:

- [Профиль оповещения SMPP](#), который будет использоваться для отправки уведомлений.
- Имя отправителя уведомлений.
- Группы номеров телефонов получателей уведомлений. По кнопке **Добавить** вы можете выбрать [группы номеров телефонов](#), созданные в разделе **Настройки → Библиотеки → Номера телефонов**. Также вы можете создавать новые группы номеров телефонов по кнопке **Создать и добавить новый объект**.

Для отправки уведомлений на URL с помощью webhook:

Укажите URL-адрес веб-ресурса, на который будут отправляться уведомления.

Примечание Вы можете протестировать отправку уведомлений с помощью сервиса [webhook.site](#). Для этого в качестве URL необходимо указать адрес, сгенерированный сервисом, например <https://webhook.site/7e8d2095-02d0-41aa-a7c9-588552c515d1>. Кроме того, для отправки уведомлений вы можете [настроить интеграцию UserGate SIEM с Telegram](#).

Для регистрации инцидента укажите следующие параметры:

- Название инцидента.
- Тип инцидента.
- Приоритет инцидента.
- Ответственного за расследование инцидента.
- Наблюдателей за состоянием инцидента.

Если в инцидент требуется добавлять последующие срабатывания правила аналитики, установите флажок **Добавлять срабатывания**.

Если к инциденту требуется прикрепить PCAP-файл, сгенерированный по срабатыванию правила аналитики, установите флажок **Приложить файлы PCAP**.

Для отправки команды на коннектор укажите следующие параметры:

- Устройства, на которые будет отправляться команда. С помощью кнопки **Добавить** вы можете выбрать [коннекторы](#), добавленные в разделе **Настройки → Сенсоры → Коннекторы**. Следует выбирать только коннекторы с одинаковой группой команд.
- Команду для устройств. В раскрывающемся списке выберите [команду из группы](#), указанной для коннекторов. Если команда [содержит переменные](#), укажите их значения в отобразившихся полях.

Для отправки команды на конечное устройство выберите одну из следующих команд:

- Отключить от сети.** Ограничение доступа конечного устройства в интернет.
- Завершить процесс.** Завершение на конечном устройстве процесса по его идентификатору, полученному после выполнения [запроса правила аналитики](#).

4. На вкладке **Шаблон** введите описание шаблона, который будет использоваться для уведомлений по выбранному каналу связи, а также для описания инцидента.

ПримечаниеЭтот шаг инструкции следует выполнять, если в качестве действия на шаге 2 вы выбрали регистрацию инцидента или отправку уведомлений по электронной почте, номеру телефона или URL-адресу (с помощью webhook).

В описании шаблона вы можете указывать переменные, относящиеся к срабатыванию правила аналитики, их необходимо вводить прописными буквами в формате {имя переменной}, например {ANALYTICS_RULE_NAME}. [В таблице ниже](#) приведены переменные, которые вы можете использовать.

5. Нажмите **Сохранить**.

Созданное действие реагирования отобразится в списке действий раздела.

Переменные в командах и в шаблонах уведомлений

Если в запросе правила аналитики указаны переменные, вы можете использовать их в командах и в шаблонах уведомлений [при создании действия реагирования](#). Такие переменные перечислены в таблице ниже.

Переменная	Описание
{ANALYTICS_RULE_NAME}	Название правила аналитики
{ANALYTICS_RULE_DESCRIPTION}	Описание правила аналитики
{NAME}	Название срабатывания правила аналитики
{TIME}	Время срабатывания правила аналитики
{TRIGGERED_ALERTS_NUMBER}	Количество срабатываний правила аналитики
{FIRST_TRIGGERED_ALERT_TIME}	Время первого срабатывания правила аналитики
{LAST_TRIGGERED_ALERT_TIME}	Время последнего срабатывания правила аналитики
{TRIGGERED_ALERTS_NAMES}	Список названий срабатываний правила аналитики, если срабатывания сгруппированы по параметру
{FIRST_EVENT_TIME}	Время первого события, на которое сработало правило аналитики
{LAST_EVENT_TIME}	Время последнего события, на которое сработало правило аналитики
{THREAT_LEVEL}	Уровень опасности угрозы по срабатыванию правила аналитики
{CATEGORY}	Категория срабатывания правила аналитики
{PRIORITY}	Приоритет срабатывания правила аналитики
{ADMINISTRATOR_NAME}	Администратор, создавший правило аналитики
{USER_NAME}	Имя пользователя, под учетной записью которого сработало правило аналитики
{SOURCE_ZONE}	Зона источника подключения
{DESTINATION_ZONE}	Зона назначения подключения
{SOURCE_COUNTRY}	Страна источника подключения
{DESTINATION_COUNTRY}	Страна назначения подключения
{SOURCE_IP}	IP-адрес источника подключения
{SOURCE_PORT}	Порт источника подключения
{DESTINATION_IP}	IP-адрес назначения подключения
{DESTINATION_PORT}	Порт назначения подключения

Переменная	Описание
{SOURCE_ZONE_ALL}	Зоны источников событий, на которые сработало правило аналитики
{DESTINATION_ZONE_ALL}	Зоны назначения событий, на которые сработало правило аналитики
{SOURCE_COUNTRY_ALL}	Страны источников событий, на которые сработало правило аналитики
{DESTINATION_COUNTRY_ALL}	Страны назначения событий, на которые сработало правило аналитики
{SOURCE_IP_ALL}	IP-адреса источников событий, на которые сработало правило аналитики
{SOURCE_PORT_ALL}	Порты источников событий, на которые сработало правило аналитики
{DESTINATION_IP_ALL}	IP-адреса назначения событий, на которые сработало правило аналитики
{DESTINATION_PORT_ALL}	Порты назначения событий, на которые сработало правило аналитики

Documentation: 
Product: SIEM
Version: 7.x
Technology: SIEM

В разделе **Аналитика → Срабатывания** отображаются срабатывания правил аналитики.

В таблице срабатываний вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Фильтрация данных о срабатываниях

Вы можете фильтровать данные в таблице, выбрав один из следующих режимов:

- **Простой** — фильтрация с помощью доступных параметров. Например, по дате и времени срабатывания, идентификатору срабатывания, сработавшему правилу аналитики, а также приоритету этого правила. Для выбора параметров используются соответствующие кнопки в панели инструментов. В раскрывающемся по кнопке **Еще** списке вы также можете выбирать дополнительные параметры фильтрации, устанавливая соответствующие флажки.
- **Расширенный** — фильтрация с помощью специальных выражений [на языке запросов](#). Для формирования запроса вы можете использовать доступные параметры и их значения, а также логические операторы и операторы сравнения.

Кроме того, вы можете сохранять примененные фильтры по кнопке **Сохранить как**. Список сохраненных фильтров доступен по кнопке **Популярные фильтры**. Также для дальнейшего анализа вы можете скачать отфильтрованные данные таблицы в виде CSV-файла по кнопке **Экспортировать в CSV**. Для сброса примененных фильтров доступна кнопка **Сброс**.

Просмотр записи о срабатывании

Запись о срабатывании в таблице содержит следующие данные.

Параметр	Описание
Узел	Имя устройства
Время	Время срабатывания правила
Идентификатор срабатывания	Идентификатор срабатывания правила
Время первого события	Дата и время первого срабатывания правила
Время последнего события	Дата и время последнего срабатывания правила
Количество событий	Количество всех событий, на которые сработало правило
Правило	Название правила аналитики
Категория срабатывания	По умолчанию для срабатываний доступны следующие категории: • Security — срабатывания категории указывают на инциденты, приводящие к ослаблению безопасности информационных систем; • Availability — срабатывания категории указывают на инциденты, приводящие к ухудшению доступности информационных систем; • Performance — срабатывания категории указывают на инциденты, приводящие к снижению производительности информационных систем Вы можете создавать дополнительные категории срабатываний правил аналитики в разделе Настройки → Библиотеки → Категории срабатываний
Приоритет	Приоритет срабатывания, указанный при создании правила аналитики: • Низкий — имеет низкий уровень важности и не требует незамедлительного реагирования; • Нормальный — требует обратить внимание и при необходимости принять соответствующие меры; • Важный — требует обратить внимание и принять соответствующие меры; • Критический — требует незамедлительного реагирования
Конечное устройство/сенсор	ID сенсора
Имя компьютера	Имя источника события
Пользователь	Имя пользователя
Сигнатуры COB	Название сигнатуры COB
Зона источника	Название сетевой зона источника
IP-источника	IP-адрес источника
Порт источника	Номер порта источника
Зона назначения	Название сетевой зоны назначения
IP-назначения	IP-адрес назначения
Порт назначения	Номер порта назначения

Вы также можете просматривать основную информацию о срабатывании в его карточке, которая открывается по нажатию на иконку срабатывания.

Действия со срабатыванием

С выбранным срабатыванием в таблице вы можете выполнять следующие действия:

- Добавлять срабатывание в зарегистрированный ранее инцидент (по кнопке **Добавить в инцидент**).
- Просматривать основную информацию о срабатывании в его карточке (по кнопке **Показать**).
- Просматривать подробную информацию о срабатывании на отдельной вкладке раздела **Аналитика** (по кнопке **Показать подробно**). При выборе инцидента в списке вам также доступна регистрация нового инцидента по кнопке **Создать новый инцидент**.

Technology: SIEM
Documentation: 
Product: SIEM
Version: 7.x

В разделе **Аналитика** → **Подробности срабатывания** вы можете просматривать подробную информацию о каждом срабатывании правила аналитики. Для этого в блоке **Срабатывание** из выпадающего списка выберите идентификатор нужного срабатывания. Информация о срабатывании отобразится в таблице и в соответствующих блоках.

Вы можете управлять выбранным срабатыванием:

- Просматривать основную информацию о срабатывании в его карточке (по кнопке **Показать**).
- Просматривать срабатывание в таблице всех срабатываний (по кнопке **Показать срабатывания**).
- Добавлять срабатывание в зарегистрированный ранее инцидент (по кнопке **Добавить в инцидент**). При выборе инцидента в списке вам также доступна [регистрация нового инцидента](#) по кнопке **Создать новый инцидент**.

Documentation: 
Product: SIEM
Version: 7.x
Technology: SIEM

В разделе **Аналитика → Процессы конечных устройств** отображается информация о процессах устройств с установленным ПО UserGate Client. Например, информация о процессах запущенных приложений, о фоновых процессах устройств, а также о системных процессах Windows. Вы можете просматривать параметры запуска этих процессов, а также отслеживать цепочки их вызовов.

В левой части страницы в блоке **Лог процессов** отображается таблица процессов, в которой вы можете:

- изменять набор столбцов в контекстном меню **Столбцы**, доступном по нажатию справа от заголовка столбца;
- изменять ширину столбцов;
- изменять порядок следования столбцов, перемещая заголовок столбца;
- сортировать данные по нажатию на заголовки столбцов (не все столбцы поддерживают функцию сортировки).

Также вы можете фильтровать данные в таблице процессов, выбрав один из следующих режимов:

- **Простой** — фильтрация с помощью доступных параметров. Например, по дате и времени запуска процесса, конечному устройству, на котором запущен процесс, а также по названию запущенного приложения. Для выбора параметров используются соответствующие кнопки в панели инструментов.
- **Расширенный** — фильтрация с помощью специальных выражений [на языке запросов](#). Для ввода выражений используется строка запросов.

Запись о процессе в таблице содержит следующие данные:

- дату и время запуска процесса;
- название конечного устройства, на котором запущен процесс;
- название запущенного приложения;
- идентификатор процесса.

Для выбранной записи в таблице вы можете просматривать подробную информацию о процессе, а также его дерево процессов. Действия доступны в правой части страницы в блоке **Процесс** на вкладках **Информация о процессе** и **Дерево процессов** соответственно.

Product: SIEM
Version: 7.x
Technology: SIEM

В UserGate SIEM можно использовать списки из библиотек в поисковых запросах везде, где они есть: в правилах аналитики, в поиске, в журналах, в дашбордах, в пользовательских отчетах.

Данные в списки заносятся либо вручную (для локальных списков), либо пополняются через указанный в настройках внешний URL обновления (для обновляемых списков). Если в правилах аналитики в фильтрах условий срабатывания используются списки, то новые элементы поиска будут добавляться в правила динамически по мере их добавления в списки.

Функция поддерживается для следующих видов списков:

Тип списка	Поле в запросе
IP-адреса	ipSource, ipDest, natIpSource, natIpDest
Списки URL	url
Типы контента	mime
Useragent браузеров	userAgent
Категории URL	urlCategory
Текстовые списки	user, rule, zoneSource, zoneDest, macSource, macDest, applicationName, httpProtocol, httpMethod, referer, sensor, computerName, logFile, data, hash, cmdLine, device, service, image, originalFilename, parentImage, parentCommandLine, targetObject, targetFilename, scriptBlockText, queryName, queryResult, workstationName, logonId, imageLoaded, sourceImage, targetImage, customString1.. customString15

Для использования списка в запросах необходимо:

1. Создать список с включенной опцией **Использовать в поисковых запросах**.
2. Добавить в него элементы списка.
3. Добавить список в поисковый запрос.

Подробнее о поддерживаемых видах и типах списков читайте в разделе [Библиотеки](#). При активации в свойствах списка опции **Использовать в поисковых запросах** создается внутренний словарь БД с содержимым этого списка и обработчик событий изменения списка.

В поисковых запросах списки могут использоваться с операторами **IN** и **NOT IN**. Синтаксис: <field name> **IN** <list name>. При получении запросов значения из запроса сравниваются со значениями из словаря.

Для IP-листов запрос вида: *ipSource IN list_1* проверяет, находится ли ipSource в каком-либо из диапазонов IP-адресов из списка list_1.

Для useragent браузеров, типов контента, списков URL, категорий URL, текстовых списков запросы *userAgent IN list_1, mime IN list_2, url IN list_3, urlCategory IN games, signatureName IN list1* проверяют, равно ли значение поля какому-либо значению из списка.

Пример:

1. Создадим список вида IP-адреса со следующим содержимым:

2. Создадим список вида Useragent браузеров со следующим содержимым:

3. Добавим созданные списки в фильтр условия правила аналитики:

В результате работы правила произойдет срабатывание на основании выбранных фильтров со списками в условии срабатывания правила:

--	--

Version: 7.x
Technology: SIEM
Product: SIEM

UserGate SIEM может быть интегрирован с Telegram для отправки уведомлений событий информационной безопасности.

Для такой интеграции понадобятся несколько компонентов:

- Заранее созданный чат-бот и Telegram-канал, в который чат-бот будет отправлять уведомления из UserGate SIEM.
- Веб-сервер, который будет выступать связующим звеном между UserGate SIEM и Telegram.
- Созданное в UserGate SIEM действие реагирования, использующее метод webhook в качестве механизма отправки событий информационной безопасности, генерируемых в SIEM.

UserGate SIEM инициирует действие webhook, отправляя на веб-сервер данные, которые должны быть переданы в Telegram. Веб-сервер обрабатывает полученные данные и посредством чат-бота отправляет в Telegram-канал данные из UserGate SIEM.

1. Инструкцию по созданию чат-бота можно найти на сайте Telegram (<https://core.telegram.org/bots/tutorial>) или на других ресурсах в Интернете. Дополнительно нужно создать Telegram-канал и разрешить чат-боту минимальные привилегии - постить сообщения.

Результатом этого подготовительного шага должны быть:

- Токен чат-бота. Он будет передан в диалоге с BotFather при создании бота.
- Токен канала. Его можно получить, добавив в целевой канал специального бота @username_to_id_bot, либо в адресной строке браузера, например: <https://web.telegram.org/a/#-xxxxxxxxxxxxx>, где "-xxxxxxxxxxxxx" — токен канала.

2. Необходимо запустить веб-сервер, который будет обрабатывать данные из UserGate SIEM. Пример кода на FastAPI: <https://gitflic.ru/project/cisecs/telegram-bot-and-webhooks/>.

3. В UserGate SIEM на странице **Действия реагирования** в разделе **Аналитика** необходимо создать действие реагирования типа webhook:

На вкладке **Действие** прописать URL созданного веб-сервера, например:

На вкладке **Шаблон** создать шаблон сообщения, например:

Добавить созданное действие реагирования в правило аналитики:

