Table of Contents

Table of Contents 1
Аналитика 2
- Общие сведения 3
- Примеры настройки правила аналитики 8
- Поиск 9
- Действия реагирования 15
- Срабатывания 20
- Подробности срабатывания 22
- Процессы конечных устройств 23
- Использование списков из библиотек в поисковых запросах 24

Общие сведения

Documentation:
Technology: SIEM
Version: 7.1.x, 7.2.x
Product: SIEM

UserGate SIEM позволяет проводить анализ журналов событий безопасности, получаемых с настроенных сенсоров, таких как МЭ UserGate, конечные устройства UserGate Client, сторонние сетевые устройства, поддерживающие передачу данных по протоколу SNMP, сенсоры WMI. 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.

Первоначальной единицей информации, которая поступает в UserGate SIEM, является событие. **Событие** — это одна запись в журнале, например, единичное срабатывание правила СОВ на МЭ UserGate, блокировка доступа к запрещенному ресурсу (срабатывание блокирующего правила контентной фильтрации), успешная или неуспешная попытка доступа в консоль управления и другие подобные события, которые регистрируются на устройствах, подключенных к UserGate SIEM. Отдельное событие может не нести достаточно информации об угрозе ИБ, но несколько однотипных событий (например, неуспешных попыток доступа в консоль управления) или разных событий, зарегистрированных в определенной последовательности и поступивших из разных источников, могут представлять ценность в идентификации угрозы. Этот процесс называется корреляция событий. Группа событий, объединенная правилом аналитики (корреляции), представляет собой **Срабатывание**. Инженер безопасности проводит анализ срабатывания, изучает входящие в срабатывание события и при необходимости может создавать **Инцидент** компьютерной безопасности на основе одного или нескольких срабатываний.

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.

В разделе **Аналитика** веб-интерфейса администратора можно настроить правила аналитики, создать действия реагирования, просмотреть журнал срабатываний правил и подробности срабатывания. Данные функции будут рассмотрены далее в соответствующих главах: Действия реагирования, Срабатывания и Подробности срабатывания.

На вкладке **Правила аналитики** можно создавать правила обработки событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников. Правила могут работать в двух режимах: исторический режим (анализ событий за выбранный период) и режим реального времени.

Правила создаются нажатием кнопки **Добавить** на панели инструментов. В открывшемся окне свойств правила аналитики на вкладке **Общие** необходимо указать параметры настройки правила:

Наименование	Описание
Включено	Включение/отключение правила аналитики для работы в режиме реального времени.
Название	Название правила аналитики.
Описание	Опциональное описание правила аналитики.
Уровень угрозы	Уровень угрозы, который будет отображаться при срабатывании правила. Для выбора доступны следующие уровни: • **Очень низкий**: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **Низкий**: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. • **Средний**: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. • **Высокий**: события, требующие исследования и принятия мер. • **Очень высокий**: события, требующие исследования и срочного принятия мер.

Наименование	Описание
Приоритет	Приоритет, установленный для срабатывания правила аналитики: • **Низкий**: срабатывания данных правил обладают низким приоритетом реагирования. • **Нормальный**: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. • **Важный**: на срабатывания данных правил необходимо обратить внимание и предпринять меры. • **Критический**: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.
Категория	Категория, 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 во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**.
Часовой пояс	Часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.
Ограничить общее время условий	Включение/отключение ограничения времени выполнения всех условий в правиле. При включении ограничения общего времени правило аналитики сработает только в том случае, когда за указанный отрезок времени все условия, настроенные в правиле, выполнятся заданное количество раз.
Общее время условий, сек	Указание отрезка времени, за который все условия, указанные в правиле, должны выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание общего времени выполнения условий доступно при поставленном флажке **Ограничить общее время условий**.

На вкладке **Условия** в окне свойств правила аналитики необходимо указать условие/условия срабатывания правила. Если условий несколько, то они связаны между собой логическим « **И**» и выполняются сверху вниз. Т.е. правило сработает только в том случае, если будут выполнены все условия.

Условие можно создать нажатием кнопки **Добавить**. Далее необходимо указать следующие параметры:

Наименование	Описание
Название	Название условия правила аналитики.
Описание	Опциональное описание условия правила аналитики.
Ограничить время выполнения условия	Включение/отключение ограничения времени выполнения условия. При включении ограничения времени правило аналитики сработает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.

Наименование	Описание
Время выполнения условия	Указание отрезка времени, за который условие должно выполнится заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание времени выполнения условия доступно при поставленном флажке **Ограничить время выполнения условия**.
Использовать запрос остановки	Включение/отключение использования запроса остановки в правиле аналитики.
Запрос остановки	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.
Запрос фильтра	SQL-подобный поисковый запрос условия, который выполняется 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.* **Например**. Поисковый запрос: *source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'.* Данный запрос производит поиск в журнале событий конечных устройств, который берёт данные из журнала Microsoft-Windows-Sysmon/Operational. При нахождении события, которое соответствует созданию нового процесса, запускается поиск родительского процесса (т.е. процесса, который вызвал создание нового процесса) и поиск вызова команды *certreq* с параметрами. Часть запроса с оператором *MATCH* позволяет определить, что *certreq* запустили из *cmd* (командной строки). Таким образом определяется то, что у текущего процесса родительским был *cmd.exe*. Подробнее о синтаксисе Google/RE2 в операторе *MATCH*: https://github.com/google/re2/wiki/Syntax.
Группировать по	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 **Повторений шаблона**.
Повторений шаблона	Количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром **Ограничить время выполнения условия** или без него.

Кнопка **Запустить сейчас** внизу окна свойств правила аналитики производит запуск анализа событий за определённый период времени (работа в историческом режиме). В открывшемся окне необходимо задать временной диапазон анализа. Если флажок **Указать диапазон времени** не поставлен, то анализ по созданному правилу аналитики проводится по всей базе событий за всё время.

Также правило можно запустить без записи в журнал срабатываний, т.е. для проверки работоспособности правила или просмотра количества срабатываний. Для этого необходимо поставить флажок **Тестовый запуск**:

После завершения анализа, нажав кнопку **Показать срабатывания** в окне **Запуск правила аналитики**, можно перейти в журнал срабатываний и просмотреть информацию о срабатывании этого правила.

На вкладке **Действия реагирования** в окне свойств правила аналитики могут быть добавлены действия, которые будут выполнены автоматически при срабатывании правила аналитики. Действия реагирования могут быть созданы нажатием строки **Создать и добавить новый объект** или добавлены из списка существующих действий (нажатием кнопки **Добавить**):

Подробнее о действиях реагирования и их настройке читайте в разделе Действия реагирования.

Чтобы запустить правило в режиме реального времени необходимо нажать кнопку **Включить** на панели инструментов раздела аналитики. Кнопка **Отключить** завершает выполнение выбранного правила аналитики.

Созданные правила можно редактировать, удалять и копировать. Кнопка **Показать срабатывания** на панели инструментов раздела аналитики отобразит журнал с краткой информацией о всех срабатываниях выбранного правила. Также можно настроить отображение списка правил: отображать все правила, только включённые/выключенные правила.

Кнопка **Настроить** на панели инструментов раздела аналитики позволяет установить значения интервалов запуска правил аналитики, работающих в режиме реального времени, в зависимости от уровня критичности правила:

Для правил аналитики также доступны функции экспорта и импорта. Импорт правил производится в бинарном формате или формате YAML. Экспортировать правила можно только в бинарном формате; экспортируются выделенные правила или все созданные, если правила не были выбраны.

При настройке условий правил аналитики возможно производить группировку событий по параметрам, представленным в записях журналов SIEM, NGFW и конечных устройств. Список параметров, по которым возможна группировка событий, смотрите в таблице раздела Поиск.

Примеры настройки правила аналитики

Technology: SIEM
Version: 7.1.x
Product: SIEM
Documentation:

Рассмотрим несколько примеров настройки правил аналитики.

Пример 1. Поиск попыток брутфорса

Брутфорс (Brute force) — метод взлома учётных записей путём подбора паролей к ним. Суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью определения правильной.

После задания общих настроек, таких как название правила, описание, уровень угрозы, приоритет, категория срабатывания и часовой пояс, были заданы несколько условий.

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

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4625. Данный идентификатор события соответствует неудачной попытке авторизации учётной записи. Часть условия с оператором MATCH позволяет определить причину отказа в авторизации: неправильный логин или пароль.

Подробнее о событии 4625 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4625.

source = 'endpoint events log' AND logEventId = 4672

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4672. Данный идентификатор события соответствует успешной авторизации с назначением специальных привилегий текущему сеансу.

Подробнее о событии 4672 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4672.

source ='endpoint events log' AND logEventId = 4624

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4624. Данный идентификатор события соответствует успешному входу пользователя в систему.

Подробнее о событии 4624 читайте в соответствующей документации: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4624.

Пример 2. Обнаружение изменения владельца файла

В данном примере рассматривается написание правила аналитики с использованием источника событий syslog. Правило обнаруживает изменение владельца файла на root с помощью утилиты chown. Условие задается следующей строкой:

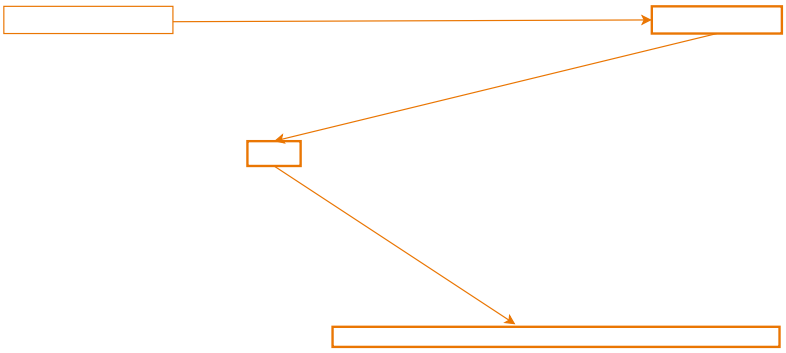
source = 'syslog' AND data ~ 'COMMAND=/bin/chown root' AND applicationName = 'sudo'

Поиск

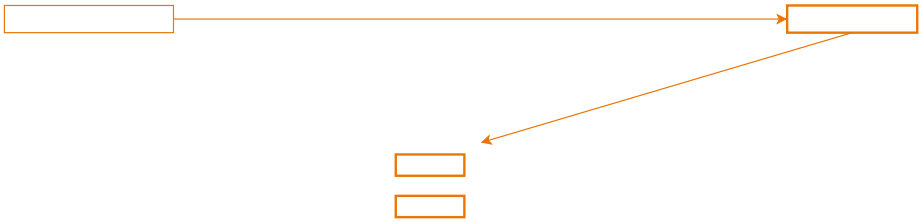
Technology: SIEM
Version: 7.2.x
Product: SIEM
Documentation: ☑

На вкладке **Поиск** отражён список всех событий журналов подключённых сенсоров и событий журналов UserGate SIEM. С использованием строки поиска можно производить поиск нужных событий. Строка поиска использует SQL-подобный поисковый запрос. 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.

С использованием кнопки **Добавить правило**, можно добавить новое правило аналитики, в котором в качестве запроса фильтра будет указан введённый поисковый запрос. Подробнее о правилах аналитики смотрите в разделе Аналитика.



Также, нажатием кнопки **Добавить условие**, по введённому поисковому запросу можно сформировать условие и добавить его в созданное ранее правило аналитики. При добавлении необходимо указать правило аналитики и имя условия:



Выбранное событие можно добавить в инцидент нажатием кнопки **Добавить в инцидент**. Подробнее об инцидентах читайте в главе Настройки инцидентов.

Существует 2 режима представления данных о событиях: табличный вид и текстовый вид. Для перехода в выбранный режим используются кнопки на нижней панели интерфейса: **Переключить в текстовый вид** или **Переключить в табличный вид**:

На вкладке **Поиск** можно увидеть следующую информацию о событиях.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Узел	node	Показано имя узла устройства NGFW или SIEM.
Время	date	Указано время события или срабатывания правила аналитики. Отображается в часовом поясе, настроенном на UserGate SIEM.
Время первого события	triggeredAlertFirstEventDate	Для журнала срабатываний: отображено время первого события, попавшего под срабатывание правила аналитики.
Время последнего события	triggeredAlertLastEventDate	Для журнала срабатываний: отображено время последнего события, попавшего под срабатывание правила аналитики.
Источник	source	Показан журнал, в который записано событие: журналы SIEM, NGFW, конечных устройств, срабатываний.
Важность	severity	Отражена категория события журналов событий NGFW, SIEM: • **Информационные**: как правило, не требуют внимания администратора. • **Предупреждение**: предупреждают о возможных проблемах. • **Ошибка**: сообщают об ошибках. • **Критические**: сообщают о серьёзных ошибках, которые могут повлиять на функциональность.
Компонент	component	Отражён компонент, в котором произошло событие (например: обновления, настройки, консольная авторизация, аналитика и т.п.). Относится к записям журнала событий NGFW и SIEM.
Тип события	event	Отображён тип события из журнала событий NGFW, SIEM (например: проверка, скачивание, установка обновлений, успешная/неуспешная авторизация, поиск параметров и т.п.).
Пользователь	user	Показано имя пользователя, с учётной записи которого был совершён вход в систему NGFW, SIEM, конечного устройства. Относится к записям журналов событий NGFW, SIEM и конечных устройств, веб доступа, трафика, СОВ, срабатываний.
Модуль	module	Указан модуль, в котором произошло событие (например: Web console, Core, VPN сервер и т.п.). Относится к записям журнала событий NGFW, SIEM.
Учёт изменений	changeTracker	Указан тип изменений (журнал событий SIEM, NGFW). Возможные типы изменений пользователь может задать самостоятельно.
Данные	data	Представлена подробная информация о событии. Относится к записям журналов событий конечных устройств и Syslog.
Информация	details	Представлена подробная информация о событии из журнала событий SIEM и NGFW.
Правило	rule	Отображено название правила аналитики, межсетевого экрана, контентной фильтрации, АСУ ТП или СОВ.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Действие	action	Отображено действие, настроенное в правилах межсетевого экрана, контентной фильтрации, АСУ ТП или СОВ: • **Разрешить** (allow/pass/allow_webaccess): действие, настроенное в правилах межсетевого экрана, СОВ или контентной фильтрации. • **Безопасный поиск** ('safe browsing'). • **Captive-портал** ('captive portal'). • **Предупредить** (warning): действие, настроенное в правилах контентной фильтрации. • **Уведомление** (alert): относится к DoS защите на зоне. • **NAT** (nat). • **DNAT** (dnat). • **Порт-форвардинг** ('port forwarding'). • **Policy-based routing** ('policy based routing'). • **Network mapping** ('network mapping'). • **Запретить** (deny/drop/deny_webaccess): действие, настроенное в правилах межсетевого экрана, СОВ или контентной фильтрации. • **Расшифровать** (decrypt): действие, настроенное в правилах инспектирования. • **Журналировать** (log): действие, настроенное в правилах СОВ. • **Пропускать** (pass): действие, настроенное в правилах АСУ ТП. • **Блокировать** (drop): действие, настроенное в правилах АСУ ТП.
Приложение	application	Название приложения. Относится к записям журнала трафика, СОВ, Syslog, журналов правил и приложений конечных устройств.
Угроза приложения	applicationThreat	Уровень угрозы приложения. Относится к записям журнала веб-доступа, трафика и СОВ.
Сетевой протокол	networkProtocol	Показан транспортный протокол подключения, использующийся для доступа к ресурсу. Относится к записям журналов трафика, СОВ, журнала правил конечных устройств.
Протокол прикладного уровня	httpProtocol	Указана версия HTTP протокола. Относится к записям журнала веб-доступа.
Категории сайтов	urlCategory	Отображены категории, к которым относится сайт. Относится к записям журнала веб-доступа и журнала правил конечных устройств.
Угроза URL-категории	urlCategoryThreat	Уровень угрозы категории URL. Параметр относится к записям журнала веб-доступа.
Причины		Отображены причины из журнала веб-доступа (например: причина блокировки).
HTTP метод	httpMethod	Отображен метод HTTP (основная операция над ресурсом). • **OPTIONS**: используется для определения возможностей веб-сервера или параметров соединения для конкретного ресурса. • **GET**: используется для запроса содержимого указанного ресурса. • **HEAD**: аналогичен методу GET, за исключением того, что в ответе сервера отсутствует тело. • **POST**: применяется для передачи пользовательских данных заданному ресурсу. • **PUT**: используется для загрузки содержимого запроса на указанный в запросе URI. • **PATCH**: аналогично PUT, но применяется только к фрагменту ресурса. • **DELETE**: удаляет указанный ресурс. • **TRACE**: возвращает полученный запрос так, что клиент может увидеть, какую информацию промежуточные серверы добавляют или изменяют в запросе. • **CONNECT**: преобразует соединение запроса в прозрачный TCP/IP-туннель. Относится к записям журнала веб-доступа.
Код ответа HTTP	statusCode	Отображён код состояния, являющийся частью первой строки ответа от сервера при запросах по протоколу HTTP. Относится к записям журнала веб-доступа.
Тип контента	mime	Показан тип контента. Является записью журнала веб-доступа и журнала правил конечных устройств.
URL	url	Показан URL-адрес ресурса, к которому было выполнено обращение. Относится к записям журнала веб-доступа.
Реферер	referer	Отображён URL-адрес предыдущей страницы (если есть). Относится к записям журнала веб-доступа.
Операционная система	operatingSystem	Отображён тип операционной системы устройства пользователя. Относится к записям журнала веб-доступа и СОВ.
User-agent	userAgent	Указан Useragent пользовательского браузера. Относится к записям журнала веб-доступа.
Сигнатуры	signature	Отображено имя сработавшей сигнатуры системы обнаружения вторжений (СОВ). Является параметром журнала СОВ.
Угроза сигнатуры	signatureThreat	Уровень угрозы сигнатуры. Относится к записям журнала СОВ.
Зона источника	zoneSource	Указана зона источника. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ.

Наименование в базе данных	Наименование в поисковом запросе	Описание
IP источника	ipSource	Показан IP-адрес источника трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств.
Порт источника	portSource	Отображён номер порта источника, через который осуществляется подключение. Относится к записям журналов веб-доступа, трафика, СОВ, журнала правил конечных устройств.
MAC источника	macSource	Показан MAC-адрес источника. Относится к записям журналов трафика и СОВ.
Зона назначения	zoneDest	Отображена зона назначения. Относится к записям журналов веб-доступа, трафика, СОВ, журнала правил конечных устройств.
IP назначения	ipDest	Показан IP-адрес назначения трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств.
Порт назначения	portDest	Указан номер порта назначения, используемый транспортным протоколом. Относится к записям журналов веб-доступа, трафика, АСУ ТП, СОВ, журнала правил конечных устройств.
MAC назначения	macDest	Показан MAC-адрес назначения. Относится к записям журналов трафика и СОВ.
NAT адрес источника	natIpSource	Отображён NAT IP-адрес источника (если настроены правила NAT). Относится к записям журнала трафика.
NAT порт источника	natPortSource	Отображён NAT порт источника (если настроены правила NAT). Относится к записям журнала трафика.
NAT адрес назначения	natIpDest	Отображён NAT IP-адрес назначения (если настроены правила NAT). Относится к записям журнала трафика.
NAT порт назначения	natPortDest	Отображён NAT порт назначения (если настроены правила NAT). Относится к записям журнала трафика.
Байт отправлено/получено	bytesSent/bytesRecv	Отображён отправленный/полученный объём информации. Относится к записям журналов трафика и веб-доступа.
Пакетов отправлено/получено	packetSent/packetRecv	Показано количество отправленных/полученных пакетов. Относится к записям журналов трафика и веб-доступа.
Конечное устройство/сенсор	sensor	Отображено имя конечного устройства/сенсора. Относится к записям журнала событий конечных устройств.
Счётчик	counter	Название счётчика, добавленного в WMI и SNMP сенсор. Относится к записям журнала событий конечных устройств.
Объект SNMP	snmpObject	Указан идентификатор SNMP объекта (SNMP OID). Относится к записям журнала событий конечных устройств.
Тип SNMP объекта	snmpObjectType	Указан тип SNMP объекта. Относится к записям журнала событий конечных устройств.
Статус	status	Отображён результат выполнения WMI или SNMP запроса (OK или Error). Относится к записям журнала событий конечных устройств.
Ошибка	error	Показана ошибка WMI или SNMP, возникшая в результате выполнения запроса. Относится к записям журнала событий конечных устройств.
Протокол АСУТП	scadaProtocol	Указан протокол SCADA (Supervisory Control And Data Acquisition - диспетчерское управление и сбор данных). • **IEC 104** (ГОСТ Р МЭК 60870-5-104). • **Modbus**. • **DNP3** (Distributed Network Protocol). • **MMS** (Manufacturing Message Specification). • **OPC UA** (Open Platform Communications Unified Architecture). Относится к записям журнала АСУ ТП.
Уровень лога	logLevel	Указан тип события: • **Audit Success** (успешный аудит): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам. • **Audit Failure** (неуспешный аудит): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам. • **Error** (ошибка): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных. • **Information** (сведения): информационные события, которые, как правило, не требуют внимания администратора. • **Warning** (предупреждение): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем. Относится к записям журнала событий конечных устройств.
Источник журнала событий	logEventSource	Отображено название программного обеспечения, которое сформировало запись события в журнал. Относится к записям журнала событий конечных устройств.
Категория лога	logCategory	Указана категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Категория задачи	taskCategory	Показана категория задачи. Является записью журнала событий конечных устройств.
Имя компьютера	computerName	Представлено полное имя конечного устройства. Относится к записям журналов событий конечных устройств, Syslog.
Код события лога	logEventCode	Отображён код события лога, соответствующий определённому событию. Является записью журнала событий конечных устройств.
Идентификатор события лога	logEventId	Показан идентификатор события лога, который определяет первичный идентификатор события. Относится к записям журнала событий конечных устройств.
Тип события лога	logEventType	Отображён тип события лога. Он представлен параметрами, каждый из которых соответствует уровню лога: • 1 — уровень лога: error. • 2 — уровень лога: warning. • 3 — уровень лога: information. • 4 — уровень лога: audit success. • 5 — уровень лога: audit failure. Относится к записям журнала событий конечных устройств.
Строка вставки	insertionString	Отображены данные блока EventData события Windows. Относится к записям журнала событий конечных устройств.
Файл журнала лога	logFile	Показана информация из журнала событий конечных устройств, т.е. информация о важных программных и аппаратных событиях. Типы журналов: • **Application** (файл журнала приложений): для событий приложений и служб. • **Security** (файл журнала безопасности): для событий системы аудита. • **System** (файл системного журнала): для событий драйверов устройств. • **CustomLog**: журнал содержит события, регистрируемые приложениями, которые создают пользовательский журнал. Использование пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения. Относится к записям журнала событий конечных устройств.
Команда	scadaCommand	Отображена команда управления АСУ ТП (например: чтение или запись). Относится к записям журнала АСУ ТП.
Адрес регистра	scadaAddress	Представлен адрес регистра, с которым необходимо провести операцию (запись или чтение). Относится к записям журнала АСУ ТП.
Номер ASDU	scadaAsdu	Показан адрес ASDU (COA - Common Object Address). Параметр относится к протоколу IEC-104. Относится к записям журнала АСУ ТП.
Идентификатор устройства	scadaDevice	Указан уникальный номер устройства, содержащийся в базе данных OPC-сервера. Параметр относится к протоколу OPC UA. Относится к записям журнала АСУ ТП.
Имя переменной	scadaVarname	Отображено имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS. Относится к записям журнала АСУ ТП.
Хэш	hash	Показан хэш приложения. Является параметром журнала приложений конечных устройств.
Объект	facility	Отображена категория события. Относится к записям журнала Syslog. Возможны следующие значения: • Сообщения ядра. • Сообщения пользовательские. • Почтовая система. • Системный сервис. • Безопасность/авторизация. • Сообщения syslog. • Система печати LPR. • Система сетевых новостей. • Подсистема UUCP. • Сервис времени. • Безопасность/аутентификация. • FTP сервис. • Система NTP. • Аудит. • Тревога. • Сервис времени 2. • Local 0 - Local7.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Критичность	syslogSeverity	Указана критичность событий журнала Syslog. • **Экстренная**: критическое состояние, которое сказывается на работоспособности системы. • **Тревога**: состояние, требующее незамедлительного вмешательства. • **Критическая**: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • **Ошибки**: несрочные сбои в системе. • **Предупреждения**: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • **Уведомительная**: события, которые относятся к необычному поведению системы, но не являются ошибками. • **Информативная**: информационные уведомления. • **Отладочная**: информация, полезная разработчикам для отладки приложений.
Идентификатор процесса	processId	Указан идентификатор процесса. Относится к записям журнала Syslog.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры:

Technology: SIEM
Version: 7.2.x
Product: SIEM
Documentation: ☑

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.

Действия могут быть созданы на вкладке **Аналитика → Действия реагирования**. При добавлении действия необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает/отключает правило реагирования.
Название	Отображает название правила реагирования.
Описание	Описывает правила реагирования. Данное поле необязательно для заполнения.
Действие	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: • **Отправить email**: отправка письма на выбранные почтовые адреса. Настройка действия **Отправить email** будет рассмотрена далее в разделе Отправить email. • **Отправить сообщение**: отправка сообщения на указанные номера телефонов. Настройка действия **Отправить сообщение** будет рассмотрена далее в разделе Отправить сообщение. • **Webhook**: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия **Webhook** будет рассмотрена далее в разделе Webhook. • **Создать инцидент**: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия **Создать инцидент** читайте в разделе Настройки инцидентов. • **Послать команду на коннектор** – отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Послать команду на коннектор. • **Послать команду на эндпоинт** – отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Послать команду на эндпоинт.
Записывать в журнал правил	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий SIEM, который можно просмотреть во вкладке **Журналы и отчёты → Журналы → Журнал событий** .
Группировать похожие срабатывания	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: • **Никогда**. • **За период времени**. При настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. • **По количеству срабатываний**. При настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
Период группировки	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.
Количество срабатываний	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по их количеству.

Созданные действия реагирования можно редактировать, удалять, копировать, включать, отключать. Также в списке действий реагирования можно отображать все действия, только включённые или только выключенные.

Отправить email

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

Наименование	Описание
Профиль оповещения	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Профили оповещений.
От	Имя отправителя письма.
Тема	Тема письма.
Почтовые адреса	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в разделе **Настройки → Библиотеки → Почтовые адреса** . О добавлении почтовых адресов читайте в разделе Почтовые адреса.

Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию, создается на вкладке **Шаблон**.

Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

Отправить сообщение

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

Наименование	Описание
Профиль оповещения	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Профили оповещений.
От	Имя отправителя письма.
Номера телефонов	Список номеров телефонов получателей. Получатели должны быть добавлены в списки в разделе **Настройки → Библиотеки → Номера телефонов** . О добавлении телефонных номеров читайте в разделе Номера телефонов.

Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию, создается на вкладке **Шаблон**.

Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд.

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.

Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию, создается на вкладке **Шаблон**.

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** во вкладке **Действия**.

Послать команду на коннектор

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
Коннекторы	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики. Коннектор должен быть заранее добавлен и настроен в разделе **Сенсоры --> Коннекторы** вкладки **Настройки** веб-интерфейса управления UserGate SIEM (для более подробной информации обратитесь к разделу Коннекторы). **Важно!** Могут быть выбраны только коннекторы с одинаковой группой команд.
Команда	Выбор 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 создании команд читайте в разделе Команды.

Пример создания правила аналитики с действием типа отправки команды на коннектор приведен в статье Как настроить правило аналитики SIEM.

Послать команду на эндпоинт

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

Доступны следующие команды:

- **Отключить от сети** – блокировка доступа к сети Интернет.
- **Завершить процесс** – завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

На вкладке **Шаблон** 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 на вкладке **Шаблон** 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 **Создать инцидент**, то текст будет отображён в описании инцидента.

Переменные для уведомлений и команд

ПримечаниеПоле чувствительно к регистру букв. Название переменных необходимо вводить прописными буквами в фигурных скобках (как представлено в таблице).
ПримечаниеИспользование переменных в командах и уведомлениях возможно в случае, если они были выбраны в разделе *Аналитика → Правила аналитики → Условия для группировки событий.*

Наименование	Описание
{ANALYTICS_RULE_NAME}	Название правила аналитики.
{ANALYTICS_RULE_DESCRIPTION}	Описание правила аналитики.
{NAME}	Название определённого срабатывания.
{TIME}	Время срабатывания правила аналитики.
{TRIGGERED_ALERTS_NUMBER}	Количество срабатываний.
{FIRST_TRIGGERED_ALERT_TIME}	Время первого срабатывания.
{LAST_TRIGGERED_ALERT_TIME}	Время последнего срабатывания.
{TRIGGERED_ALERTS_NAMES}	Список названий срабатываний, если используется группировка.
{FIRST_EVENT_TIME}	Время первого события, попавшего под срабатывание правила аналитики.
{LAST_EVENT_TIME}	Время последнего события, попавшего под срабатывания правила аналитики.
{THREAT_LEVEL}	Указанный уровень угрозы.
{CATEGORY}	Категория, к которой относится срабатывание.

Наименование	Описание
{PRIORITY}	Приоритет срабатывания правила аналитики.
{ADMINISTRATOR_NAME}	Имя администратора, которым было создано правило аналитики.
{USER_NAME}	Имя пользователя.
{SOURCE_ZONE}	Зона источника.
{DESTINATION_ZONE}	Зона назначения.
{SOURCE_COUNTRY}	Страна источника.
{DESTINATION_COUNTRY}	Страна назначения.
{SOURCE_IP}	IP-адрес источника.
{SOURCE_PORT}	Порт источника.
{DESTINATION_IP}	IP-адрес назначения.
{DESTINATION_PORT}	Порт назначения.
{SOURCE_ZONE_ALL}	Зоны источников всех событий, сформировавших срабатывание.
{DESTINATION_ZONE_ALL}	Зоны назначения всех событий, сформировавших срабатывание.
{SOURCE_COUNTRY_ALL}	Страны источников всех событий, сформировавших срабатывание.
{DESTINATION_COUNTRY_ALL}	Страны назначения всех событий, сформировавших срабатывание.
{SOURCE_IP_ALL}	IP-адреса источников всех событий, сформировавших срабатывание.
{SOURCE_PORT_ALL}	Порты источников всех событий, сформировавших срабатывание.
{DESTINATION_IP_ALL}	IP-адреса назначения всех событий, сформировавших срабатывание.
{DESTINATION_PORT_ALL}	Порты назначения всех событий, сформировавших срабатывание.

Срабатывания

Technology: SIEM
Version: 7.1.x
Product: SIEM
Documentation: ☑

На вкладке **Срабатывания** показан список срабатываний правил аналитики и отображена краткая информация о них. Срабатывание — это набор событий, объединенных правилом аналитики.

Можно увидеть следующую информацию о срабатываниях.

Наименование	Описание
Узел	Показан уникальный код, соответствующий устройству.
Время	Указаны дата и время срабатывания правила аналитики.
ID	Отображен идентификатор срабатывания.
Время первого события	Показано время первого события, попавшего под срабатывание правила аналитики.
Время последнего события	Показано время последнего события, попавшего под срабатывание правила аналитики.
Количество событий	Показано количество событий, попавших под срабатывание правила аналитики.
Правило	Отображено название правила аналитики, которое сработало.
Категория	Отображена категория, 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 правил аналитики могут быть созданы во вкладке **Настройки** в разделе **Библиотеки → Категории срабатываний**.
Приоритет	Показан приоритет срабатывания, указанный при настройке правила аналитики: • **Низкий**: данные правила обладают низким приоритетом реагирования. • **Нормальный**: на данные правила необходимо обратить внимание и, возможно, предпринять меры. • **Важный**: на данные правила необходимо обратить внимание и предпринять меры. • **Критический**: данные правила требуют незамедлительного реагирования. Установленный приоритет указывает на важность срабатывания.
Пользователь	Указано имя пользователя.
Сигнатуры	Отображено имя сработавшей сигнатуры СОВ.
Зона источника	Отображена зона, из которой происходит подключение.
IP источника	Показан IP-адрес источника.
Порт источника	Указан порт источника.
Зона назначения	Отображена зона назначения.
IP назначения	Показан IP-адрес назначения.
Порт назначения	Указан порт назначения.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Доступны два режима поиска: простой и расширенный. Простой режим использует графический интерфейс; расширенный поиск предназначен для формирования более сложных фильтров поиска с использованием специального языка запросов, о синтаксисе которого написано в разделе Поиск и фильтрация данных.

Нажатием кнопки **Сохранить как** можно сохранить настроенный фильтр. Список сохранённых фильтров поиска можно просмотреть, нажав на кнопку **Популярные фильтры**.

Чтобы посмотреть карточку срабатывания (краткую информацию о выбранном срабатывании), необходимо нажать кнопку **Показать**.

Нажатие кнопки **Показать подробно** произведёт перевод на вкладку Подробности срабатывания, где отображена подробная информации о выбранном срабатывании. О вкладке **Подробности срабатывания** читайте в соответствующей главе Подробности срабатывания.

Выбранное срабатывание правила аналитики можно добавить в инцидент нажатием одноимённой кнопки **Добавить в инцидент**.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Подробности срабатывания

Technology: SIEM
Version: 7.1.x
Product: SIEM
Documentation: ☑

На данной вкладке отображена подробная информация о срабатывании правила аналитики и отображаются все события, попавшие в данное срабатывание.

Данные могут быть представлены в табличном или текстовом виде. Переключение между режимами осуществляется нажатием кнопок **Переключить в текстовый вид** или **Переключить в табличный вид**, находящихся внизу экрана.

Представлена следующая информация о срабатывании.

Наименование	Описание
Срабатывание	Показан идентификатор срабатывания.
Время	Указано время срабатывания правила аналитики. Отображается в часовом поясе, настроенном на UserGate SIEM.
Приоритет	Отображён установленный при настройке приоритет срабатывания. • **Низкий**: данные правила обладают низким приоритетом реагирования. • **Нормальный**: на данные правила необходимо обратить внимание и, возможно, предпринять меры. • **Важный**: на данные правила необходимо обратить внимание и предпринять меры. • **Критический**: данные правила требуют незамедлительного реагирования.
Правило	Показано название правила аналитики, которое сработало.
Поиск инцидента	Нажатие данной кнопки производит поиск инцидента, в котором используется данное срабатывание.
Список событий	Показаны события, которые попали в данное срабатывание.

Нажатие кнопки **Показать срабатывания** произведёт перевод на вкладку **Срабатывания**, где будет отображён список срабатываний выбранного правила аналитики.

Процессы конечных устройств

Technology: SIEM
Version: 7.1.x
Product: SIEM
Documentation: ☑

На вкладке **Процессы конечных устройств** отображён список процессов устройств с установленным ПО UserGate Client. Она позволяет отследить цепочку вызова процессов, а также разобраться в параметрах запуска и просмотреть полезную информацию о файле. Вкладка представлена двумя панелями: **Лог процессов** и **Процесс**.

На панели **Лог процессов** отображён список процессов конечных устройств (процессы запущенных приложений, фоновые процессы, процессы Windows), передающих информацию на SIEM. Для просмотра доступна следующая информация:

- Дата и время запуска.
- Название конечного устройства.
- Приложение.
- Идентификатор процесса.

Для удобства записи могут быть отфильтрованы по различным критериям, например, таким, как диапазон дат, название приложения, идентификатор процесса и т.п. Фильтрация также возможна с использованием расширенного поиска для формирования сложных фильтров; в режиме расширенного поиска используется специальный язык запросов, синтаксис которого рассмотрен далее в разделе Поиск и фильтрация данных.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Выделив процесс можно просмотреть дерево процесса и подробную информацию о нём. Дерево процесса и подробная информация будут отображены на панели **Процесс**.

Использование списков из библиотек в поисковых запросах

Technology: SIEM
Version: 7.2.x, 7.3.x
Product: SIEM

В SIEM начиная с версии ПО 7.2.0 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 (доступно с версии ПО 7.3.0)	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: