NTechnology | SIEM

Руководство по созданию запросов

НЦОТ

Содержание

1.Общая информация о системе

1.1 О документе

Этот документ содержит информацию о стандартных запросах в системе, предназначенной для сбора и анализа событий информационной безопасности (Security Information and Event Management system) «NTechnology SIEM» (далее – NT SIEM).

Руководство предоставляет рекомендации по правильному формированию запросов для обеспечения их корректной интерпретации и обработки системой. В документе также представлены примеры запросов и результаты их применения.

Комплект документации NT SIEM включает в себя следующие документы:

– Этот документ;

– Руководство по установке – содержит информацию для внедрения продукта в инфраструктуре организации: инструкции по установке, первоначальной настройке и удалению продукта;

– Руководство пользователя – содержит справочную информацию и инструкции по настройке и администрированию продукта. Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности;

– Руководство по написанию правил – содержит рекомендации по созданию правил нормализации, агрегации, корреляции и обогащению событий.

1.2 О NT SIEM

NT SIEM – это система, которая осуществляет сбор, хранение и анализ событий, исходящих от сетевых устройств, средств защиты информации, баз данных, ключевых корпоративных ресурсов, инфраструктуры систем и приложений.

1.3 Краткое описание возможностей системы

Система NT SIEM предоставляет следующие основные функциональные возможности:

- Сбор журналов событий с различных источников;
- Визуализация данных в виде графиков, диаграмм в форме дашбордов;
- Анализ журналов событий в соответствии с правилами нормализации, корреляции, агрегации и обогащения;
- Формирование инцидентов на основе процессов агрегации, обогащения и корреляции;
- Управление инцидентами информационной безопасности;
- Хранение событий и инцидентов информационной безопасности;

- Фильтрация по различным параметрам событий и инцидентов, в том числе с использованием избранных запросов для быстрого доступа к фильтрам по событиям;
- Использование готовой базы правил, а также возможность создания собственных правил и табличных списков;
- Мониторинг состояния системы;
- Отправка уведомлений пользователям в рамках веб-приложения и по электронной почте;
- Формирование и выгрузка отчетов за определенный период времени;
- Осуществление интеграций, в том числе и с SOAR-системами;
- Мониторинг активов.

2. Запросы для фильтрации данных на страницах системы

2.1 Фильтрация на группе страниц «База правил»

По умолчанию в пользовательском интерфейсе NT SIEM на группе страниц «База правил» данные отображаются от более новых к более старым. Для фильтрации правил необходимо в поле поиска задать запрос и нажать на кнопку 🔍. Отобразится таблица правил, соответствующих условиям вашего запроса.

Поиск осуществляется с помощью предикатов. Простой предикат в языке запросов, используемом на группе страниц «База правил», – это логическое выражение, получаемое после объединения поля правила (табл.1) и его значения с помощью оператора сравнения (табл. 2). Значение соответствует типу данных поля правила. Простой предикат формируется в соответствии с синтаксисом, при этом между полем, оператором и значением могут быть пробелы:

Выражение `<Поле><Оператор><Значение>`.

Предикат в языке запросов, используемом в группе страниц «База правил», может использоваться как самостоятельное условие запроса или как часть условия. Условие запроса, состоящее из нескольких предикатов, формируется с помощью логических операторов и скобок. Логические операторы (табл. 3) соединяют предикаты, а скобки определяют порядок выполнения операций в запросе.

Все поля, операторы и значения регистрозависимы, то есть при обработке запроса система проверяет регистр символов. Между полями, операторами и значениями не должно быть пробелов.

`<Поле>` – имя поля правила. В случае, если в названии поля есть ошибка или значение поля не соответствует типу данных поля, результат будет некорректный либо результат запроса будет отсутствовать.

Таблица 1 – Поля правил, по которым можно фильтровать данные

Поле	Описание	Пример запроса
Правила корреляции, агрегации		
id	Идентификатор правил корреляции и агрегации	`id=001`
filename	Название файла	`filename=0015-NT_rules.xml`
groups	Группы используются для	`groups=syslogerrors`

Поле	Описание	Пример запроса
	классификации. Каждое правило должно принадлежать к какой-либо группе. По умолчанию, каждое правило может быть причислено к одной из групп: `syscheck`, `attack`, `syslog`	
level	Уровень критичности	`level=7`
mitre	Систематизированное описание техник (приёмов) и тактик, которые используют злоумышленники при атаках на организации (см. документацию Mitre ATT&CK)	`mitre~T1003`

relative_dirname	Имя каталога	Два варианта запроса:
		`relative_dirname=etc/rules`
		
		`relative_dirname=ruleset/rules`

status	Поле, описывающие доступность или недоступность	`status=enabled` `status=disabled`
Правила нормализации		
details.order		`details.order=level`
filename	Название файла	`filename=0006-json_decoders.xml`
name	Название правила нормализации	`name!=apparmor`
relative_dirname	Имя каталога	`relative_dirname=etc/decoders` `relative_dirname=ruleset/decoders`
Табличные списки		
filename	Название файла	`filename=audit-keys`

Поле	Описание	Пример запроса
relative_dirname	Имя каталога	`relative_dirname=etc/lists`

`<Значение>` – значение поля правила. Если необходимо провести поиск по значению из без пробела, дополнительное форматирование не требуется для поиска не требуется. Пример:

`id=001` или `groups=syslog`

Таблица 2 – Операторы сравнения для фильтрации на странице «База правил»

Оператор	Описание	Синтаксис
=	Сравнение на равенство. Если равенство верное, то получится результат ИСТИНА, если нет – ЛОЖЬ	<Поле> **=** <Значение>
!=	Сравнение на неравенство, ИСТИНА система выдаст, если значения будут не равны.	<Поле> **!=** <Значение>
<	Сравнение на строгое неравенство (меньше). Принимает значение ИСТИНА, когда правый операнд больше левого.	<Поле> **<** <Значение>
>	Сравнение на строгое неравенство (больше). Если левый операнд больше правого, то результат ИСТИНА.	<Поле> **>** <Значение>
~	Проверка вхождения указанного значения в значение поля.	<Поле> **~** <Значение>

Таблица 3 – Логические операторы для фильтрации на странице «База правил»

Оператор	Описание	Синтаксис
`or`	Логическое ИЛИ	<Предикат> **`or`** <Предикат>
`and`	Логическое И	<Предикат> **`and`** <Предикат>
()	Группировка операторов	(<Предикат>) **`or/and`** (<Предикат>)

Если необходимо провести проводите поиск по значению, а значение состоит из несколько частей и имеет пробел или содержит символ двойной кавычки «"», то требуется дополнительное форматирование. Значение должно быть заключено в пару

двойных кавычек "<Значение>", а символ двойной кавычки «"» заменен на символ «\"». Пример:

```
"never connected \"Windows\""
```

Примеры поиска с помощью предикатов.

Пример 1. Фильтровать по сущностям, чьи <group name> равны определенному <Значению>:

```
groups=syslog or groups=syslogerrors
```

Пример 2. Фильтровать правила, где <level> больше или равен определенному <Значению>:

```
level=7 or level>7
```

Пример 3. Фильтровать правила, на соответствие нормативным требованиям:

```
mitre~T1003
```

2.2 Фильтрация на странице «События»

В пользовательском интерфейсе NT SIEM в разделе «События» данные отображаются от более новых к более старым. Для фильтрации событий необходимо в поле поиска задать запрос и нажать на кнопку 🔍. Отобразится таблица с событиями, соответствующих условиям запроса.

Существует возможность создания запросов путем нажатия на значение полей в блоке с подробной информацией о событии (см. в Руководство Пользователя).

Запросы должны быть организованы в виде пар «ключ:значение». Для комбинирования нескольких условий используются логические операторы (табл. 5). Следует отметить, что для поиска можно использовать и операторы сравнения (табл.4).

Основной формат ввода состоит из пары, где ключ и значение разделены символом «:» без использования пробелов. Ключи и значения чувствительны к регистру.

Ключ представляет собой поле события. Может содержать латинские буквы, цифры, символы подчеркивания «_», точки «.», восклицательного знака «!» и символ «@». Ключ, в отличии от значения, допускает использование латинских букв. Например:

```
@timestamp
!rule.id
full_log
agent.id
```

Значение представляет собой данные, соответствующие ключу. Значения могут быть представлены или в кавычках «" "», или без них:

1. Если значение не включает в себя пробелы и спецсимволовы кроме «.», «-», «_», «*», «?», то кавычки «" "» можно опустить. Например:

```
agent.id:002
agent.ip:10.72.144.61
agent.name:unix_61
```

2. Если значение содержит пробел(-ы) и/или спецсимволы, кроме «.», «-», «_», «*», «?», то оно помещается в кавычки «" "». Например:

```
full_log:"Feb 11 10:41:49 Deactivated successfully."
rule.description: "Anomaly detection event."
```

В результате будет выполнен запрос на поиск событий, в описании которых содержится эта фраза в точной последовательности.

Таблица 4 – Операторы сравнения для фильтрации на странице «События»

Символ	Описание и синтаксис	Примеры
*	Используется для поиска с несколькими подстановочными знаками. В значении может использоваться только один спецсимвол «*» в формате текста без кавычек. Спецсимволу могут предшествовать цифры. Не рекомендуется использовать в начале поискового запроса.	Нужно найти все события, у которых идентификатор начинается с 50, например 505 или 506. `rule.id:50*`
?	Используется для поиска с одним подстановочным знаком. В значении может использоваться только один спецсимвол «?» в формате текста без кавычек. Не рекомендуется использовать в начале поискового запроса.	Нужно найти агенты с именами `siem31 … siem39`. Для замены одного знака используется символ «?». `agent.name:siem3?`
[]	Поиск по заданному диапазону, **включая** граничные значения. Должен состоять из двух значений, разделенных соединителем «TO». Ожидается, что значения не содержат пробелов.	Нужно найти все события с 510 по 550 включительно. `rule.id:[510 TO 550]`

Символ	Описание и синтаксис	Примеры
	Ключ:[значение_от `TO` значение_до]	
{}	Поиск по заданному диапазону, **исключая** граничные значения. Должен состоять из двух значений, разделенных соединителем «TO». Ожидается, что значения не содержат пробелов. Ключ:{значение_от `TO` значение_до}	Нужно найти все события с 510 по 550, не включая 510 и 550. `rule.id:{510 TO 550}`

Для объединения нескольких пар «ключ:значение» используются логические операторы (табл.5). Логический оператор ставится перед парой «ключ:значение», к которой он относится.

Следует обратить внимание, что **операторы регистрозависимы** и их следует писать заглавными буквами.

Таблица 5 – Логические операторы для фильтрации на странице «События»

Текстовый оператор	Символ	Описание	Синтаксис

OR	||	Логическое **ИЛИ**. Используется для объединения условий, где достаточно выполнения хотя бы одного из них.	Нужно найти правило 510 или 550.
			
			`rule.id:510 OR rule.id:550`
			`rule.id:510 || rule.id:550`

AND	&&	Логическое **И**. Используется для объединения условий, требующих одновременного выполнения.	Нужно найти правило 510 и с локацией «syscheck».
			
			`rule.id:510 AND location: "syscheck"`
			
			`rule.id:510 && location: "syscheck"`

NOT	-	Логическое **НЕ**. Используется для исключения определенных условий. Обратить внимание, что запрос с символом «-» следует писать без пробелов.	`location: syscheck NOT syslog`
			
			`location: "syscheck"-"syslog"`

Текстовый оператор	Символ	Описание	Синтаксис
	()	Используется для группировки операторов	`(rule.id:510 AND location: "syscheck") NOT rule.id:550`

При необходимости использования специальных символов, таких как: «+», «-» «&&», «||», «!», «(», «)», «{», «}», «[», «]», «^», «"», «~», «*», «?», «:», «\» следует использовать специальный синтаксис при помощи символа «\»:

```
\(1\+1\)\:2
```

Пример 1. Отфильтровать события по условию: событие пришло с агента с идентификатором начинается с «00_» и идентификатор трехзначный:

```
agent.id:00?
```

Пример 2. Отфильтровать события по условию: событие было проанализировано по правилу с идентификатором, начинающимся с 50 или равным 510:

```
rule.id:50* || rule.id:510
```

Пример 3. Отфильтровать события по условию: событие было проанализировано по правилу с идентификатором равным 510 или в диапазоне от 513 до 515 включительно:

```
rule.id:510 OR rule.id:[513 TO 515]
```

Пример 4. Отфильтровать события по условию: событие пришло в 14:27 10 февраля 2025 и не с агента с идентификатором равным 004:

```
@timestamp:"2025-02-10T14:27" NOT agent.id:004
```

Пример 5. Отфильтровать события по условию: событие с определенным описанием правила, по которому оно сработало:

```
rule.description:"Unknown problem somewhere in the system" - rule.gpg13:4.3
```

Пример 6. Отфильтровать события по условию: событие пришло в 14:27 10 февраля 2025 или с агента с идентификатором равным 004 и является нормализованым:

```
@timestamp:"2025-02-10T14:27" OR agent.id:004 && !rule.id:*
```

Группа невалидных запросов.

Пример 7. Отфильтровать события по условию: событие сработавшим по правилу начинающимся с «50» или с «asd». Запрос является невалидным, так как в значении более одного спецсимвола «*» и спецсимволу предшествуют не цифры:

```
rule.id:50* || rule.id:asd*
```

Пример 8. Отфильтровать события по условию: событие пришло 10 февраля в 20:32. Запрос является невалидным, так как в значении не заключено в кавычки (содержит пробелы и спецсимволы):

```
predecoder.timestamp:Feb 10 20:32:36
```

Пример 9. Отфильтровать события по условию: событие пришло от агента с идентификатором 001, 002, 003 или 004. Запрос является невалидным, так как диапазон указывается в «[]» или «{}» через «TO».

```
agent.id:001-004
```

Пример 10. Отфильтровать события по условию: событие пришло от агента с идентификатором 001, 002, 003 или 004. Запрос является невалидным, так как в диапазоне есть пробел. При использовании квадратных или фигурных скобок необходимо убдится, что они содержат только два значения, разделенных «TO».

```
rule.id:[513 TO 51 5]
```

Пример 11. Отфильтровать события по условию: событие с полным логом, содержащем данные. Запрос является невалидным, так как значение находится в одинарных кавычках, необходимо использовать двойные кавычки.

```
full_log:'Feb 11 10:41:49 Deactivated successfully.
```

Пример 12. Если в интерфейсе выбран тип событий «Нормализованные», а в строке поиска введен запрос «`rule.id:510 AND agent.name:"linux-002"`», то итоговый запрос будет иметь вид:

```
(rule.id:510 AND agent.name:"linux-002") AND
timestamp:[2025-02-12T00:00:00.000+03:00 TO 2025-02-
12T23:59:59.000+03:00] AND rule.level:*
```

Дополнительные фильтры типа событий и временной период не отображаются в поле ввода, но также участвуют в формировании запроса с одной особенностью. Они автоматически имеют соединитель «AND», и при их наличии все остальные фильтры автоматически оборачиваются в круглые скобки «()».

2.3 Фильтрация на страницах «Инциденты», «Активы», «Журнал действий пользователей»

Для фильтрации инцидентов, активов, логов пользователей необходимо задать в поле поиска запрос и нажать на кнопку . Далее отобразится таблица с данными, соответствующими условию запроса.

2.3.1 Быстрое создание запроса из карточки объекта.

На страницах «Инциденты» и «Активы» существует возможность создания запросов путем нажатия на значение полей в блоке с подробной информацией об объекте (см. Руководство Пользователя).

2.3.2 Ручной ввод запроса.

- Общий поиск.

Введите искомое значение поля в строку поиска, например, test1. Система найдет все записи, содержащие слово «test1» в любом из полей таблицы.

Для поиска точной фразы (несколько слов подряд) используйте двойные кавычки. Например, если введен запрос `"Account_was_successfully_logged"`, то система найдет только те записи, где эти три слова стоят вместе в таком же порядке.

- Поиск по названию поля.

Запросы могут быть организованы в виде пар «`ключ:значение`». Основной формат ввода состоит из пары, где ключ и значение разделены символом «:». Ключ представляет собой название поля таблицы. Значение представляет собой данные, соответствующие ключу. Значения могут быть представлены или в кавычках «" "», или без них.

Если нужно найти точное значение поля, необходимо заключать фразу в двойные кавычки. Например, если введен запрос `name:"Abnormal activity"`, то система найдет все записи, где в поле `name` присутствует фраза `Abnormal activity`.

Если запрос не заключон в кавычки, например `name:Abnormal activity`, то система находит записи, где поле `name` содержит слово `Abnormal` или где любое другое поле содержит слово `activity`. Таким образом, первое слово после двоеточия ищется в указанном поле. Все последующие слова (без кавычек) ищутся уже по всем полям (как в общем поиске).

Список всех доступных для поиска полей приведен в таблицах ниже.

Таблица 6 – Схема полей для поиска на странице «Инциденты»

Наименование для поиска	Наименование в пользовательском интерфейсе	Поле для сортировки
severity_name	Уровень критичности	+
status_name	Статус	+
name	Наименование инцидента	+
description	Описание инцидента	+

Наименование для поиска	Наименование в пользовательском интерфейсе	Поле для сортировки
key_value	Идентификатор инцидента	+
correlation_rule	Правило корреляции	+
source_ipv4	Адрес источника в формате ipv4	+
destination_ipv4	Адрес назначения в формате ipv4	+
created_at	Время создания	+
updated_at	Время обновления	+ (по умолчанию)
assigned_to_name	Ответственный пользователь	+

Таблица 7 – Схема полей для поиска на странице «Активы»

Наименование для поиска	Наименование в пользовательском интерфейсе	Поле для сортировки
name	Наименование	+ (по умолчанию)
ip	IP-адрес	+
system	Операционная система	+
importance_name	Значимость	+
inactivity_notification_period	Срок актуальности данных	+
last_connection_at	Дата последнего подключения	+
group_name	Наименование группы активов	+
is_monitored	Отслеживание актива	+
is_active	Состояние актива	-

Таблица 8 – Схема полей для поиска на странице «Журнал действий пользователей»

Наименование для поиска	Наименование в пользовательском интерфейсе	Поле для сортировки
timestamp	Время	-
user_ip	IP-адрес	-
user_login	Логин	-
method	Метод	-
path	Путь	-
status	Статус выполнения действия	-

Для комбинирования нескольких условий используются **регистрозависимые** операторы, представленные в таблице 9.

Таблица 9 – Операторы для фильтрации

Текстовый оператор	Символ	Описание	Синтаксис
OR	()	Логическое **ИЛИ**. Используется для объединения условий, где достаточно выполнения хотя бы одного из них.	`source_ipv4:"192.168.10.1" OR name:"Incident 1"`

AND	+	Логическое **И**. Используется для объединения условий, требующих одновременного выполнения. При этом оператор «AND» обладает приоритетом. Таким образом, оператор «+» помечает **обязательные** для выборки поля, остальные поля могут быть использованы для уточнения выборки.	`source_ipv4:"192.168.10.1" AND name:"Incident 1" OR name:"Abnormal activity"` эквивалентен запросу: `(source_ipv4:"192.168.10.1" AND name:"Incident") OR name:"Abnormal activity"`
			
			`source_ipv4:"192.168.10.1" + name:"Incident"`

	-	Логическое **НЕ**. Используется для исключения определенных условий. Обратить внимание, что запрос с символом «-» следует писать без пробелов.	`source_ipv4:"192.168.10.1" - name:"Incident 1"`
	()	Используется для группировки операторов.	`(source_ipv4:"192.168.10.1" OR name:"Incident 1") AND name:"Abnormal activity"`
	[]	Используется для поиска по заданному диапазону, **включая** граничные значения.	`created_at:[ 2025-11-15T11:03:54.139462Z TO 2025-11-16T11:03:54.139462Z ]`
	{}	Используется для поиска по заданному диапазону,	`created_at:{ 2025-11-15T11:03:54.139462Z TO`

Текстовый оператор	Символ	Описание	Синтаксис
		исключая граничные значения.	`2025-11-16T11:03:54.139462Z }`
	IN	Используется для объединения условий, где достаточно выполнения хотя бы одного из них. Способ заменить множество условий с оператором OR.	`name: IN [test1, test2, test3]`
	*	Используется для поиска по всем полями.	`* -source_ipv4:"1.1.1.1"`
	~	Используется для поиска по неточной фразе, позволяет установить соответствующее расстояние фразы в словах.	`description:"тест русском"~1`
	~	Используется для поиска по неточной фразе, позволяет установить соответствующее расстояние фразы в словах.	`description:"тест русском"~1`

Важно помнить, что при работе с временем необходимо использовать формат UTC, а также отделять временные метки пробелами с двух сторон.

При необходимости использования кавычек как части поискового запроса следует использовать специальный синтаксис при помощи символа «\»:

```
description:"Incident of type \"Significally dangerouse\" be careful"
```

Пример 1. Отфильтровать инциденты по условию: показать все инциденты, кроме тех, у кого адрес источника IP-адрес «1.1.1.1» и тех, у кого IP-адрес назначения «2.2.2.2»:

```
* -source_ipv4:"1.1.1.1" -destination_ipv4:"2.2.2.2"
```

Пример 2. Отфильтровать инциденты по условию: показать инцидент с ID «11»:

```
key_value:"11"
```

Пример невалидного запроса. Отфильтровать инциденты по условию: время создания от 15.11.2025 по 16.11.2025. Запрос является невалидным, так как диапазон указывается в «[]» или «{}» через «TO».

```
created_at:2025-11-15T11:00:00.0+03:00 - 2025-11-
16T11:00:00.0+03:00
```