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 страницах «События», «Инциденты», «Активы», «Журнал действий пользователей»

Для фильтрации событий, инцидентов, активов и журналов действий пользователей необходимо в поле поиска задать запрос и нажать на кнопку  или клавишу Enter. Далее отобразится таблица с данными, соответствующими условию запроса.

2.2.1 Быстрое создание запроса из карточки объекта.

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

2.2.2 Ручной ввод запроса.

Запросы организованы в виде пар `ключ:"значение"`. Основной формат ввода состоит из пары, где ключ и значение разделены символом «:» без использования пробелов. Ключ представляет собой название поля таблицы. Значение представляет собой данные, соответствующие ключу. Значения необходимо заключать в двойные кавычки «" "».

Например:

```
full_log:"Feb 11 10:41:49 Deactivated successfully"
rule_description:"Системный вызов к ядру."
```

Ключ может содержать латинские буквы, цифры, символ подчеркивания «_». Набор полей для фильтрации событий совпадает с полями, доступными в настройках отображения таблицы на странице «События» (за исключением поля `full_log`).

Для фильтрации инцидентов, активов и журнала действий пользователей полный список доступных полей приведен в таблицах ниже.

Таблица 4 – 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	+
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 5 – 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 6 – 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 объединения нескольких пар ключ:"значение" используются логические операторы (табл.7). Логический оператор ставится перед нужной парой и обязательно отделяется пробелами с обеих сторон.

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

Таблица 7 – Операторы для фильтрации

Текстовый оператор	Описание	Синтаксис
OR	Логическое **ИЛИ**. Используется для объединения условий, где достаточно выполнения хотя бы одного из них.	`rule.id:"510" OR rule.id:"550"`
AND	Логическое **И**. Используется для объединения условий, требующих одновременного выполнения. При этом оператор «AND» обладает приоритетом.	`rule.id:"510" AND location: "10.77.163.30"`
NOT	Логическое **НЕ**. Используется для исключения определенных условий.	`status_name:"New" NOT severity_name:"Low"`
()	Используется для группировки операторов.	`(source_ipv4:"192.168.10.1" OR name:"Incident 1") AND name:"Abnormal activity"`
*	Используется для поиска по всем полями.	`status_name:*`

Для фильтрации по всем значениям определенного поля необходимо использовать запрос в формате `ключ:*`. Такой запрос отобразит на странице все записи, содержащие указанное поле с любыми значениями. Например, запрос `rule_level:*` покажет все нормализованные события. А для отображения всех ненормализованных событий необходимо ввести запрос `NOT rule_level:*`

Если в значении ключа используются двойные кавычки " или обратный слеш \, их необходимо экранировать обратным слешем (\" или \\ соответственно).

Например, если ключ name имеет значение Инц123\идент \"/, то в запросе необходимо записать name:"Инц123идент \\\"\/".

Следует обратить внимание на то, что значения всегда нужно обворачивать в двойные кавычки.

Если в значении двойные кавычки стоят последние, то необходимо закрыть экранирование.

Например, если ключ group_name имеет значение Группа "Специальная", то в запросе необходимо записать group_name:"Группа \"Специальная\"/".

Пример1. Запрос `NOT source_ipv4:"10.77.163.10" NOT source_ipv4:"10.77.163.30"` исключает из выборки инциденты, у которых `source_ipv4` совпадает с `10.77.163.10` или `10.77.163.30`. В результате останутся только те записи, где источники отличаются от обоих указанных значений.

Пример 2. Запрос `severity_name:"Low" AND status_name:"New"` выполнит фильтрацию по двум полям одновременно. На странице отобразится список инцидентов, которые имеют низкий уровень критичности и находятся в работе.

Пример 3. Запрос `rule.id:"510" OR rule.id:"550"` найдет события, где `rule.id` равен 510 или 550.

Пример 4. Запрос `rule_id:"510" AND location: "10.77.163.30"` найдет события, где одновременно выполняются оба условия, а именно `rule_id` равен `510` и `location` равен `10.77.163.30`.

Пример 5. Запрос `dst_port:"42214" NOT rule_id:"300961"` найдет события, где `dst_port` равен `42214`, но при этом `rule_id` не равен `300961`

Пример 6. Запрос `rule_level:"6" AND (dst_port:"42214" OR dst_port:"42215»)` найдет события с `rule_level:"6"`, у которых `dst_port` равен `42214` или `42215`. Скобки гарантируют, что оператор OR будет обработан до применения внешнего оператора AND.