MaxPatrol VM версия 2.0

Синтаксис языка запросов PDQL

Дата редакции документа: 28.07.2023

Содержание

1. Об этом документе

Это руководство содержит информацию о языке Positive Data Query Language (далее также — PDQL). Язык PDQL разработан в Positive Technologies для написания запросов в процессе обработки активов и уязвимостей в Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM).

В руководстве описаны синтаксис, основные функции и операторы языка PDQL, приводятся примеры использования.

Руководство адресовано операторам, использующим MaxPatrol VM для управления информационными активами организации.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство оператора безопасности — содержит сценарии использования продукта для управления информационными активами организации.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.
- Руководство разработчика — содержит информацию о доступных в MaxPatrol VM функциях сервиса REST API.
- PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol VM.

2. Синтаксис языка PDQL для фильтрации активов

Этот раздел содержит информацию о синтаксисе языка PDQL для фильтрации активов.

Актив — это базовая единица MaxPatrol VM, которая представляет собой сканируемый сетевой узел.

В этом разделе

2.1. О фильтрации активов с помощью языка PDQL

Выполнение условия на языке PDQL позволяет отфильтровать активы. Для создания условия используются поля модели активов, поля из паспортов активов и их значения, псевдонимы, данные об уязвимостях, а также операторы и функции.

Результаты фильтрации могут использоваться для анализа IT-инфраструктуры предприятия и выпуска отчетов, а также при создании динамической группы активов.

В этом разделе

2.1.1. Фильтрация активов в таблице

Выполнение PDQL-запроса позволяет отфильтровать активы в таблице в соответствии с его условием. Вы можете создавать условие запроса вручную с помощью поля фильтрации или с помощью системного конструктора представления данных и всплывающих подсказок (см. Руководство оператора).

В таблице активов вы можете:

- выполнять быстрый поиск в строке поиска . Условие поиска может быть преобразовано в условие фильтрации;
- выбирать состав колонок по нажатию **Колонки** или с помощью выражения `Select(<Поле 1>, …, <Поле N>)`;
- фильтровать записи по нажатию **Фильтрация** или с помощью выражения `Filter(<Условие фильтрации>)`;
- фильтровать записи по времени по нажатию **Время** или с помощью выражений `Timepoint(<Условие фильтрации>)` и `Timeseries(<Условие фильтрации>)`. Для фильтрации используются моменты времени и периоды (см. раздел 2.1.3);
- группировать записи и анализировать данные по нажатию **Группировка и агрегация** или, например, с помощью выражения `Group(<Поле 1>, …, <Поле N>, <Математическая функция>(<Поле>))`. Для анализа данных используются математические функции (см. приложение Б);
- выбирать порядок сортировки по нажатию **Сортировка** или сортировать записи по возрастанию с помощью выражения `Sort(<Поле 1> ASC)` или по убыванию с помощью выражения `Sort(<Поле N> DESC)`;
- изменять регистр символов (см. раздел 2.1.5) и проводить вычисления по нажатию **Вычисляемые колонки** или с помощью выражения `Calc(<Условие>)`;
- ограничивать количество записей по нажатию **Ограничение** или с помощью выражения `Limit(<Количество записей в таблице>)`;
- отображать только уникальные записи по нажатию **Уникальность** или с помощью выражения `Unique()`;
- объединять результаты выполнения двух запросов (см. раздел 2.1.4) в одну таблицу по нажатию **Объединение** или с помощью выражения `Join(<Условие фильтрации> as <Псевдоним>, <Условие объединения>)` с использованием псевдонима запроса (см. раздел 2.7.3).

После фильтрации и выбора колонок таблицы вы можете выполнять остальные действия в любом порядке. Каждое последующее действие применяется к результату, полученному при выполнении предыдущего действия. При создании условия запроса вручную необходимо разделять действия с помощью пробелов и вертикальной черты (`" | "`).

Примеры

Запрос `Select(@Host, Host.OsName, Host.OsVersion) | Sort(Host.OsName ASC, Host.OsVersion ASC)` позволяет получить список всех узлов с информацией об имени и версии установленной на них операционной системы, а также отсортировать их по имени и по возрастанию номера версии операционной системы. Например, чтобы обновить версии операционных систем.

Запрос `Filter(NetworkDeviceHost) | Select(@NetworkDeviceHost, NetworkDeviceHost.ModelNumber) | Sort(@NetworkDeviceHost ASC)` позволяет получить список узлов (сетевых устройств) с информацией об их моделях.

Запрос `Select(@Host, Host.User.Name) | Filter(Host.User.Name) | Group(@Host) | Sort(@Host ASC)` позволяет получить список учетных записей на узлах.

Запрос `Select(@UnixHost, UnixHost.Groups.Name, UnixHost.Groups.Users) | Join(Select(@UnixHost, UnixHost.User.ID, UnixHost.User.Name) as U, @UnixHost = U.@UnixHost and UnixHost.Groups.Users = U.UnixHost.User.Name) | Select (@UnixHost, UnixHost.Groups.Name, U.UnixHost.User.ID, UnixHost.Groups.Users)` позволяет найти группы пользователей на узлах с операционной системой семейства Unix и вывести информацию о пользователях, состоящих в них.

Запрос `Select(WindowsHost.User<WindowsUser>.Name, WindowsHost.User<WindowsUser>.PasswordLastChanged as t) | Filter(t > Now() - 1M)` позволяет найти на узлах с операционной системой Windows учетные записи пользователей, у которых сменился пароль в течение последнего месяца.

Запрос `Select(Host.Softs.Name as name, Host.Softs.Version as version, Host.Softs.Vendor as vendor, Host.Softs.@Type as t) | Filter(t = 'Software') | select (name, version, vendor) | Unique()` позволяет вывести в таблице информацию о программном обеспечении, которое не поддерживается в системе.

2.1.2. Создание динамической группы активов

Выполнение PDQL-запроса позволяет отфильтровать активы в соответствии с его условием. Результаты фильтрации могут быть использованы для создания динамической группы активов (см. Руководство оператора).

Примеры

Запрос `Host.HostType = 'Server'` позволяет найти все сетевые узлы-серверы.

Запрос `not WindowsHost` позволяет найти все узлы с операционной системой не из семейства Windows.

Запрос `Host.OsName = 'Windows 7'` позволяет найти все сетевые узлы, на которых установлена операционная система Windows 7.

Запрос `UnixHost.Softs.Name like '%Apache%'` позволяет найти все узлы с операционной системой семейства Unix, на которых развернуты сервера Apache.

Запрос `Host.@Vulners.CVEs.Item = 'CVE-1999-1113'` позволяет найти все активы типа Host с уязвимостью CVE-1999-1113.

Запрос `not Host.@IpAddresses.Item in 203.0.113.0/20` позволяет найти все активы, не включенные в подсеть 203.0.113.0/20.

Запрос `WindowsHost.Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 3389]` позволяет найти все узлы, на которых установлена операционная система семейства Windows и у которых открыт TCP-порт 3389 (работает протокол удаленного рабочего стола Remote Desktop Protocol — RDP).

Запрос `Host [not Softs.Name = "Kaspersky"]` позволяет найти все узлы, на которых не установлено программное обеспечение семейства Kaspersky.

2.1.3. Фильтрация активов по времени

Для фильтрации активов по времени с помощью PDQL-запроса необходимо указать условие фильтрации в поле **Фильтр** или в поле **Указать на языке PDQL** (операция **Время** → окно **Данные за момент времени** (операция `timepoint`) или **Данные за период** (операция `timeseries`)).

> **Примечание.** Фильтрация по данным за период (операция `timeseries`) необходима для создания виджетов по активам с распределением по времени.

Для создания условия используются временные атрибуты активов (например, UnixHost.User<UnixUser>.PasswordLastChanged и WindowsHost.User<WindowsUser>.PwdLastSet), псевдонимы времени и операторы.

Кроме того, для создания условий фильтрации активов по времени можно использовать арифметические операции — сложение для периода в будущем (например, для поиска активов, которые скоро устареют) и вычитание для периода в прошлом (например, для поиска учетных записей, у которых недавно сменился пароль).

Синтаксис: `<Атрибут актива или его псевдоним> <Оператор> <Момент времени>() <Арифметическая операция> <Период>`

Моменты времени: пользовательское значение в формате DateTime, сейчас (Now), начало текущего часа (Startofhour), конец текущего часа (Endofhour), начало текущего дня (Startofday), конец текущего дня (Endofday), начало текущей недели (Startofweek), конец текущей недели (Endofweek), начало текущего месяца (Startofmonth), конец текущего месяца (Endofmonth), начало текущего года (Startofyear), конец текущего года (Endofyear).

Формат периода: `<Количество><Единица времени 1><Количество><Единица времени 2>… <Количество><Единица времени N>`

Формат единиц времени:

- год — `y`, `year`, `years`;
- месяц — `mo`, `month`, `months`;
- неделя — `w`, `week`, `weeks`;
- день — `d`, `day`, `days`;
- час — `h`, `hour`, `hours`;

— минута — `mi`, `minute`, `minutes`;

— секунда — `s`, `second`, `seconds`.

Единицы времени должны располагаться по убыванию, например `1year2months3weeks` или `4d 5h 6mi`.

> **Примечание.** Единицы времени регистронезависимы, то есть при обработке запроса система игнорирует регистр символов.

Примеры

Для поиска активов, которые устареют в течение недели, может использоваться условие `Select(@Host) | Filter (Host.@DeletionTime <= Now() + 7days)`.

Для поиска учетных записей, у которых за последний месяц сменился пароль, может использоваться условие `Select(UnixHost.User<UnixUser>.Name, UnixHost.User<UnixUser>.PasswordLastChanged as "Смена пароля") | Filter("Смена пароля" > Now() - 1Mo)`.

Для создания динамической группы и добавления в нее активов, которые появились в системе за последнюю неделю, может использоваться условие `Host.@CreationTime >= Now() - 1W`.

Для поиска активов высокой значимости с опасными уязвимостями может использоваться запрос `Filter(Host.@Importance in ['H', 'M']) | Timeseries(30d, 1d, Endofday()) | Filter(Host.@Vulners.CVSS2SCORE > 7) | Select(@Host, Host.@Time) | Group(Host.@Time, Count(*))`.

См. также

Псевдонимы времени (см. раздел 2.7.1.3)

Операторы (см. раздел 2.8)

Типы данных (см. приложение A)

2.1.4. Фильтрация активов с помощью объединения запросов

Для объединения результатов запросов используются:

— Запрос 1 — запрос, с результатом которого будет объединен результат другого запроса.

— Запрос 2 — запрос, результат которого будет объединен с результатом первого запроса.

— Если требуется, псевдоним запроса, который позволяет избежать повторения названий колонок таблиц с результатами выполнения запросов.

— Условие объединения, которое образуется с помощью предикатов равенства, соединенных с помощью логических операторов AND, OR и скобок (), определяющих порядок выполнения операций в запросе.

Синтаксис: `<Запрос 1> | Join(<Запрос 2> as <Псевдоним>, <Условие объединения>)`

См. также

Псевдонимы запросов для операции объединения (см. раздел 2.7.3)

Операторы (см. раздел 2.8)

Предикаты для создания условия фильтрации (см. раздел 2.2)

2.1.5. Изменение регистра данных об активах

Регистр данных об активах и о событиях может отличаться. Для их корректного сравнения в правилах корреляции и обогащения необходимо создавать табличные списки таким образом, чтобы поля данных об активах в них были в таком же регистре, что и поля в данных о событиях.

Для изменения регистра данных об активах с помощью PDQL-запроса необходимо указать выражение в поле **Фильтр** или в поле **Выражение** (операция **Вычисляемая колонка**). Для приведения к верхнему регистру используется операция `upper`, к нижнему — операция `lower`.

Синтаксис: `Calc(<Операция изменения регистра>(<Поле>) as <Псевдоним>)`

После выполнения операции в конец таблицы добавляется колонка с названием <Псевдоним>, значения из которой можно использовать при создании табличных списков.

Примеры

```
Filter(Host.HostRoles.Role = 'Domain Controller') | Select(Host.Fqdn,
Host.@IpAddresses as ip, Host.@Id as id) | Calc(lower(Host.FQDN) as fqdn) |
select(fqdn, ip, id))
```

2.2. Предикаты для создания условия фильтрации

Для формирования условия фильтрации активов используются предикаты — логические выражения на языке PDQL.

Для создания предикатов могут использоваться:

— объекты и атрибуты модели активов (см. раздел 2.3);

— данные паспортов активов (см. раздел 2.5);

— данные об уязвимостях (см. раздел 2.6);

— псевдонимы (см. раздел 2.7).

Также для создания некоторых предикатов могут использоваться операторы (см. раздел 2.8).

При создании предикатов для фильтрации по времени значения для поля `time` могут быть заданы в форматах:

— `YYYY-MM-DD'T'HH:MM:SS`;

— `YYYY-MM-DD'T'HH:MM`;

— `YYYY-MM-DD`.

Предикат может использоваться как самостоятельное условие фильтрации или как часть условия. Условие фильтрации, состоящее из нескольких предикатов, формируется с помощью логических операторов AND, OR и NOT и скобок (). Логические операторы соединяют предикаты, а скобки определяют порядок выполнения операций в запросе.

Также предикаты можно вкладывать друг в друга для создания более сложных условий фильтрации активов. Вложенное условие формируется с помощью квадратных скобок [ ].

> **Примечание.** При выборе состава колонок таблицы активов операнды в предикатах должны быть одного типа, например @WindowsHost, WindowsHost.@CumulativeVulnerability, WindowsHost.@UpdateTime, WindowsHost.Groups.Name.

Пример:

Запрос `Host[HostRoles.Role = 'File Service' and OsCandidates.Family = 'Windows' and OsName != 'Windows 7']` позволяет найти все файловые службы на операционных системах, отличных от Windows 7.

Предикат существования

Предикат существования используется для поиска активов, у которых есть атрибут, указанный в условии фильтрации.

Примеры:

Предикат `Host` задается для поиска всех сетевых узлов.

Предикат `Host<WindowsHost>` задается для поиска всех сетевых узлов, на которых установлена операционная система семейства Windows.

Предикат `WindowsHost.Softs<KasperskySecurityCenter>.Plugins` задается для поиска всех сетевых узлов, на которых установлена операционная система семейства Windows, а также программное обеспечение Kaspersky Security Center с плагинами.

Предикат равенства

Предикат равенства используется для указания названий колонок, по которым происходит объединение результатов при создании условия объединения запросов (см. раздел 2.1.4).

Этот предикат образуется с помощью оператора равенства (=), который объединяет два названия колонок из разных таблиц с результатами выполнения запросов для поиска активов. Для исключения повторения названий столбцов таблицы активов используются псевдонимы (см. раздел 2.7.3).

Примечание. Колонки таблиц, содержащие псевдоним @<Актив>, сравниваются по ID актива.

Прочие предикаты

Кроме того, условие фильтрации активов может содержать предикаты сравнения (образуются с помощью операторов сравнения), вхождения (образуются с помощью оператора `IN`), а также предикаты, образованные с помощью других операторов (см. раздел 2.8).

В этих предикатах первый предикат задается так же, как в предикате существования, а значение (или диапазон значений, сеть, шаблон) может быть только соответствующего типа данных.

См. также

Данные об уязвимостях (см. раздел 2.6)

2.3. Объекты модели активов

В MaxPatrol VM реализована модель активов: все собранные сведения об активах представлены в виде объектов. С помощью набора этих объектов может быть охарактеризован любой актив. Объекты модели имеют атрибуты, которые могут быть использованы при формировании условия фильтрации активов на языке PDQL.

Примечание. Все атрибуты объектов модели активов регистронезависимы, то есть при обработке PDQL-запроса система игнорирует регистр символов.

2.4. Пользовательские поля модели актива

В MaxPatrol VM при импорте активов вы можете добавлять в модель активов пользовательские поля и их значения (см. Руководство оператора). Вы можете использовать эти поля при формировании условия фильтрации активов на языке PDQL.

Примечание. Поля активов и их значения могут быть указаны в условии фильтрации на языке PDQL в любом регистре.

2.5. Данные паспорта актива

В MaxPatrol VM для каждого актива предусмотрен паспорт. В паспорте актива отображаются его название и текстовое описание, а также установленные значения метрик CVSS. При формировании условия фильтрации активов на языке PDQL могут быть использованы название актива и его текстовое описание.

Примечание. Название актива и его текстовое описание могут быть указаны в условии фильтрации на языке PDQL в любом регистре.

2.6. Данные об уязвимостях

В MaxPatrol VM для актива могут быть указаны уязвимости. Каждой уязвимости присваивается идентификатор в соответствии с классификацией уязвимостей Common Vulnerabilities and Exposures (CVE).

Идентификатор уязвимости может быть использован при формировании условия фильтрации активов на языке PDQL.

> **Примечание.** Идентификатор уязвимости может быть указан в условии фильтрации на языке PDQL в любом регистре.

Кроме того, фильтрация и настройка представления данных об активах и уязвимостях на этих активах могут осуществляться с помощью псевдонимов для полей уязвимости (см. раздел 2.7.1.6).

2.7. Псевдонимы

В MaxPatrol VM предусмотрены стандартные псевдонимы, которые объединяют похожие атрибуты объектов модели активов, имена и описания активов и другие данные об активах. Такие псевдонимы могут использоваться при создании запросов для фильтрации активов в таблице, для настройки представления данных об активах и для объединения активов в динамические группы.

Кроме того, можно указывать пользовательские псевдонимы для более понятного отображения информации в таблице активов, а также для запросов при операции объединения.

> **Примечание.** Псевдонимы могут быть указаны в любом регистре.

В этом разделе

2.7.1. Стандартные псевдонимы

Для удобства создания условия фильтрации активов на языке PDQL, а также для изменения представления данных об активах могут использоваться предусмотренные в MaxPatrol VM стандартные псевдонимы. Некоторые псевдонимы также могут использоваться для объединения активов в динамические группы.

В этом разделе

2.7.1.1. Общие псевдонимы активов

Для всех активов должны быть указаны их основные атрибуты. Фильтрация активов, настройка представления данных о них, а также создание динамических групп активов могут осуществляться с помощью псевдонимов для таких атрибутов.

Псевдоним актива

Для понятного отображения актива при выборе колонок в таблице, при сортировке и группировке активов могут использоваться псевдонимы:

— для узлов — `@HOST`;

— для служб каталогов Active Directory — `@ACTIVEDIRECTORY`.

Внимание! Активы такого типа доступны в таблице активов после создания динамической группы активов с фильтром `ActiveDirectory`.

Поиск активов осуществляется по одному из параметров: отображаемому имени актива, идентификатору, типу актива или типу устройства.

Псевдоним имени

Для поиска активов может использоваться псевдоним `@NAME`. Поиск осуществляется по атрибуту модели активов DisplayName (отображаемое имя актива).

Псевдоним идентификатора

Для поиска активов может использоваться псевдоним `@ID`. Поиск осуществляется по атрибуту модели активов GUID (идентификатор).

Псевдоним типа актива

Для поиска активов может использоваться псевдоним `@TYPE`, с помощью которого можно обращаться к разным атрибутам актива. При создании динамической группы активов поиск осуществляется по полному или краткому наименованию типа, при выборе колонок в таблице активов — по краткому наименованию (если есть конфликты, то по полному). При настройке представления данных об активах в таблице поиск осуществляется по значению типа актива, отображаемому в ячейке таблицы активов.

Кроме того, для поиска по полному наименованию типа актива в доменной модели может использоваться псевдоним `@FULLTYPE`.

Псевдоним типа актива для импорта

Для импорта активов используется псевдоним `@TYPEALIAS`. Заполняется на основании значения из списка (см. приложение В), в случае отсутствия значения — `@CoreHost`.

Псевдоним типа устройства

Для поиска активов может использоваться псевдоним `@DEVICETYPE`. Поиск осуществляется по атрибуту модели активов DeviceType (тип устройства, данные для отрисовки графического отображения актива).

Псевдоним описания

Для поиска активов может использоваться псевдоним `@DESCRIPTION`. Поиск осуществляется по атрибуту модели активов Description (описание актива).

Псевдоним значимости

Для активов в паспорте может быть указана значимость — High (высокая), Medium (средняя), Low (низкая) или Undefined (не определена). Для поиска активов может использоваться псевдоним `@IMPORTANCE`. Поиск осуществляется по атрибуту модели активов Importance (значимость актива).

> **Примечание.** Псевдоним значимости не может использоваться для объединения активов в динамическую группу.

Псевдоним интегральной уязвимости

Для поиска активов может использоваться псевдоним `@CUMULATIVEVULNERABILITY`. Поиск осуществляется по атрибуту модели активов CumulativeVulnerability (интегральная уязвимость актива).

> **Примечание.** Псевдоним интегральной уязвимости не может использоваться для объединения активов в динамическую группу.

2.7.1.2. Псевдонимы адресов узлов

Для узлов могут быть указаны адреса, а также адреса их целей при межсетевом взаимодействии. Для фильтрации, настройки представления данных в таблице и для создания динамических групп активов могут использоваться псевдонимы адресов и списков адресов.

Псевдоним IP-адреса узла

Для активов типа Host могут быть указаны IP-адреса. Для поиска активов по IP-адресам может использоваться псевдоним `@IPADDRESSES`. Он объединяет разные атрибуты объектов модели активов, например Host.IpAddress и Host.Interfaces.L3Settings.Address.Address.Address. Запрос `Host.@IpAddresses contains 192.0.2.10` позволяет найти активы с IP-адресом 192.0.2.10, а запрос `Host.@IpAddresses intersect [192.0.2.10, 192.0.2.12]` позволяет найти активы, у которых есть хотя бы один из IP-адресов: 192.0.2.10 или 192.0.2.12.

Также для поиска активов по IP-адресам может использоваться псевдоним `@IPADDRESSES.ITEM`. Запрос `Host.@IpAddresses.Item in 192.0.2.0/24` позволяет найти все активы из подсети 192.0.2.0—192.0.2.255.

> **Примечание.** Псевдоним `@IPADDRESSES.ITEM` может использоваться в условии фильтрации активов только до выбора полей.

Псевдоним MAC-адреса узла

Для активов типа Host может быть указан MAC-адрес. Для поиска активов по MAC-адресам может использоваться псевдоним `@MACADDRESSES`. Он объединяет разные атрибуты объектов модели активов, например Host.MacAddress, Host.Interfaces.L2Settings.MacAddress; Host<Computer>.NetworkCard.Mac. Кроме того, для поиска активов по MAC-адресам может использоваться псевдоним `@MACADDRESSES.ITEM`.

> **Примечание.** Псевдоним @MACADDRESSES.ITEM может использоваться в условии фильтрации активов только до выбора полей.

Псевдоним списка IP-адресов узлов

Для активов типа Host могут быть указаны IP-адреса. Для поиска активов по списку адресов может использоваться псевдоним `@IPLIST` для объединения значений атрибутов модели активов IpAddresses. Адреса должны быть разделены с помощью вертикальной черты с пробелами (`" | "`).

Псевдоним списка MAC-адресов узлов

Для активов типа Host могут быть указаны MAC-адреса. Для поиска активов по списку адресов может использоваться псевдоним @MACLIST для объединения значений атрибутов модели активов MacAddresses. Адреса должны быть разделены с помощью вертикальной черты с пробелами (`" | "`).

Псевдоним списка IP-адресов целей

Для цели межсетевого взаимодействия может быть указан IP-адрес. Для поиска активов по спискам IP-адресов их целей может использоваться псевдоним `@IPENDPOINTLIST`. Адреса должны быть разделены с помощью вертикальной черты с пробелами (`" | "`).

Псевдоним списка MAC-адресов целей

Для цели межсетевого взаимодействия может быть указан MAC-адрес. Для поиска активов по спискам MAC-адресов их целей может использоваться псевдоним `@ETHERNETIPENDPOINTLIST`. Адреса должны быть разделены с помощью вертикальной черты с пробелами (`" | "`).

2.7.1.3. Псевдонимы времени

Для фильтрации, настройки представления данных в таблице и для создания динамических групп активов могут использоваться псевдонимы времени.

Примечание. Время в системе соответствует часовому поясу UTC+0.

Псевдоним времени создания актива

Для актива в паспорте может быть указан момент его создания, то есть дата и время, когда данные об активе появились в системе. Для поиска активов по времени создания может использоваться псевдоним `@CREATIONTIME`.

Псевдоним времени последнего обновления актива

Информация об активах может обновляться в процессе сбора данных. Для поиска активов по времени последнего обновления может использоваться псевдоним `@UPDATETIME`.

Псевдоним времени удаления актива

В паспорте актива, который долгое время не обновлялся, может быть указано предполагаемое время его устаревания, то есть удаления данных о нем из системы. Для поиска активов по предполагаемому времени устаревания может использоваться псевдоним `@DELETIONTIME`.

Псевдоним времени последнего аудита актива

Для поиска активов по времени последнего сбора с них данных модулем Audit может использоваться псевдоним `@AUDITTIME`.

Псевдоним времени последнего пентеста

Для поиска активов по времени последнего сбора с них данных модулем Pentest может использоваться псевдоним `@PENTESTTIME`.

Псевдоним для расчета актива на момент времени

Для выбора даты и времени для расчета данных об активе может использоваться псевдоним `@TIME`, для расчета на предыдущий момент времени —— `@PREVIOUSTIME`.

2.7.1.4. Псевдонимы инфраструктур

Для фильтрации, настройки представления данных в таблице и для создания динамических групп активов могут использоваться псевдонимы параметров инфраструктур, к которым принадлежат активы.

Псевдоним инфраструктуры

Для поиска активов может использоваться псевдоним `@SCOPE`, с помощью которого можно обращаться к параметрам инфраструктуры — идентификатору и названию. При выборе колонок таблицы активов и сортировке поиск осуществляется по имени инфраструктуры, а при группировке — по ее идентификатору.

Псевдоним идентификатора инфраструктуры

Для поиска активов по идентификатору инфраструктуры, к которой он принадлежит, может использоваться псевдоним `@SCOPE.ID`.

Псевдоним названия инфраструктуры

Для поиска активов по названию инфраструктуры, к которой он принадлежит, может использоваться псевдоним `@SCOPE.NAME`.

2.7.1.5. Псевдонимы групп активов

Активы могут быть помещены в группы. Для фильтрации активов и для настройки представления данных об активах в таблице могут использоваться псевдонимы параметров групп активов.

> **Примечание.** Группа «Все активы» не учитывается при фильтрации и настройке представления данных об активах в таблице с помощью псевдонимов групп активов.

> **Примечание.** Псевдонимы групп активов не могут использоваться для объединения активов в динамическую группу.

Псевдоним группы

Для поиска активов может использоваться псевдоним `@GROUPS`, с помощью которого можно обращаться к параметрам группы — идентификатору, названию и типу (динамическая или статическая). При выборе колонок таблицы активов фильтрация осуществляется по названию группы и ее типу, при сортировке — по названию; группировка осуществляется по идентификаторам групп активов.

Псевдоним идентификатора группы

Для поиска активов по идентификатору группы, в которой он расположен, может использоваться псевдоним `@GROUPS.ID`.

Псевдоним названия группы

Для поиска активов по названию группы может использоваться псевдоним `@GROUPS.NAME`.

Псевдоним типа группы

Для поиска активов по типу группы может использоваться псевдоним `@GROUPS.TYPE`.

Псевдоним пути к группе

Для поиска активов по пути к группе, в которой они расположены, может использоваться псевдоним `@GROUPS.PATH`. В качестве псевдонима может использоваться только полный путь к группе. Группы в пути должны быть разделены с помощью косой черты (/), например Group A/Group B/Group C/My Group.

2.7.1.6. Псевдонимы уязвимостей

Уязвимости на активах могут рассматриваться как виртуальные объекты типа Vulners. Фильтрация активов, настройка представления данных о них, а также создание динамических групп активов могут осуществляться с помощью псевдонимов для полей уязвимости.

Псевдонимы уязвимостей позволяют отобразить в таблице активов уязвимости на текущем узле актива и вложенных узлах. Для отображения уязвимостей только на текущем узле актива вы можете добавить к псевдониму префикс `NODE`, например `@NODEVULNERS.NAME`.

Общие псевдонимы

Для поиска активов по уязвимостям может использоваться псевдоним `@VULNERS`, с помощью которого можно обращаться к полям объекта Vulners (названию и описанию).

Для поиска активов по названиям уязвимостей может использоваться псевдоним `@VULNERS.NAME`.

Для поиска активов по описаниям уязвимостей может использоваться псевдоним `@VULNERS.DESCRIPTION`.

Для поиска активов по уровню опасности уязвимости может использоваться псевдоним `@VULNERS.SEVERITYRATING`. Кроме того, для поиска по максимальному уровню опасности среди всех уязвимостей на активах может использоваться псевдоним `@VULNERABILITYSEVERITYRATING`.

> **Примечание.** Псевдоним `@VULNERS.SEVERITYRATING` не может использоваться для создания динамической группы активов.

Для поиска активов по времени обнаружения уязвимости может использоваться псевдоним `@VULNERS.DISCOVERYTIME`.

Для поиска активов по способу устранения уязвимости может использоваться псевдоним `@VULNERS.HOWTOFIX`.

Для поиска активов по ссылкам на информацию об уязвимости может использоваться псевдоним `@VULNERS.LINKS`.

Для поиска активов по дате публикации уязвимости может использоваться псевдоним `@VULNERS.ISSUETIME`.

Для поиска активов по уязвимостям с отметкой «важная» может использоваться псевдоним `@VULNERS.ISDANGER`.

Для поиска активов по уязвимостям с пользовательскими метками может использоваться псевдоним `@VULNERS.TAGS`.

Для поиска активов по отдельным меткам уязвимостей может использоваться псевдоним `@VULNERS.TAGS.ITEM`.

Для поиска активов по возможности пентест-проверки для обнаружения уязвимостей может использоваться псевдоним `@VULNERS.HASPENTESTCHECK`.

Для поиска активов по уязвимостям их операционных систем может использоваться псевдоним `@NODEVULNERS`.

Для поиска активов по уязвимостям с определенным типом последствий эксплуатации уязвимостей может использоваться псевдоним `@VULNERS.IMPACT`.

Псевдонимы идентификаторов уязвимости

Для поиска активов по идентификатору уязвимостей может использоваться псевдоним `@VULNERS.ID`.

Для поиска активов по идентификаторам уязвимостей в базе Common Vulnerabilities and Exposures (CVE) может использоваться псевдоним `@VULNERS.CVES`. Кроме того, может использоваться псевдоним `@VULNERS.CVES.ITEM`. Например, запрос `@Vulners.Cves.Item like '%14833%'` позволяет найти активы, на которых обнаружена уязвимость CVE-2019-14833.

Базу уязвимостей см. на сайте mitre.org.

Для поиска активов по уникальному идентификатору в базе данных уязвимостей Knowledge Base в MaxPatrol VM может использоваться псевдоним `@VULNERS.KB`.

Для поиска активов по идентификатору уязвимости может также использоваться псевдоним `@VULNERS.IDS`, с помощью которого можно обращаться к любым идентификаторам уязвимостей в публичных базах данных (например, в CVE и банке данных угроз ФСТЭК), кроме идентификатора в Knowledge Base .

Псевдонимы оценок и векторов уязвимости по стандарту CVSS

Для поиска активов по общей оценке уязвимости может использоваться псевдоним `@VULNERS.SCORE`, а также псевдонимы `@VULNERS.CVSS2SCORE` и `@VULNERS.CVSS3SCORE`.

> **Примечание.** Псевдоним общей оценки уязвимости не может использоваться для объединения активов в динамическую группу.

Для поиска активов по базовой оценке уязвимости могут использоваться псевдонимы `@VULNERS.CVSS2BASESCORE` и `@VULNERS.CVSS3BASESCORE`; по временной оценке — псевдонимы `@VULNERS.CVSS2TEMPORALSCORE` и `@VULNERS.CVSS3TEMPORALSCORE`; по контекстной оценке — псевдонимы `@VULNERS.CVSS2ENVIRONMENTALSCORE` и `@VULNERS.CVSS3ENVIRONMENTALSCORE`.

> **Примечание.** Псевдоним контекстной оценки уязвимости не может использоваться для объединения активов в динамическую группу.

Для поиска активов по базовым метрикам уязвимости могут использоваться псевдонимы `@VULNERS.CVSS2BASEVECTOR` и `@VULNERS.CVSS3BASEVECTOR`, по временным метрикам — псевдонимы `@VULNERS.CVSS2TEMPORALVECTOR` и `@VULNERS.CVSS3TEMPORALVECTOR`, по контекстным метрикам — псевдонимы `@VULNERS.CVSS2ENVIRONMENTALVECTOR` и `@VULNERS.CVSS3ENVIRONMENTALVECTOR`. Если для уязвимости указан базовый вектор (совокупность базовых метрик), для поиска активов по общему вектору уязвимости могут использоваться псевдонимы `@VULNERS.CVSS2VECTOR` и `@VULNERS.CVSS3VECTOR`.

> **Примечание.** Псевдонимы контекстных метрик уязвимости и вектора уязвимости не могут использоваться для объединения активов в динамическую группу.

Описание оценок, метрик и векторов уязвимостей по стандарту CVSS см. на сайте first.org.

Псевдонимы статусов

Для поиска активов по статусам уязвимостей может использоваться псевдоним `@VULNERS.STATUS`.

Для поиска активов по времени последнего изменения статуса уязвимости может использоваться псевдоним `@VULNERS.STATUSUPDATETIME`.

Если в карточке уязвимости на активе есть дополнительная информация, то могут использоваться псевдонимы:

- `@VULNERS.STATUSREASON` для поиска активов по уточнению к статусу уязвимости;
- `@VULNERS.STATUSCOMMENT` для поиска активов по комментарию к статусу уязвимости;
- `@VULNERS.FIXTYPE` для поиска активов по типу устранения уязвимости;
- `@VULNERS.LASTFIXTIME` для поиска активов по времени последнего устранения уязвимости;
- `@VULNERS.DUETIME` для поиска активов по времени, до которого уязвимость должна быть устранена или исключена.

Псевдонимы метрик

Для поиска активов по метрикам уязвимостей может использоваться псевдоним `@VULNERS.METRICS`. Если в карточке уязвимости есть информация о конкретных метриках, то могут использоваться псевдонимы этих метрик:

- если есть возможность эксплуатации уязвимости — псевдоним `@VULNERS.METRICS.EXPLOITABLE`;
- если уязвимость может быть устранена — псевдоним `@VULNERS.METRICS.HASFIX`;
- если есть возможность эксплуатации уязвимости по сети — псевдоним `@VULNERS.METRICS.HASNETWORKATTACKVECTOR`.

Псевдонимы трендовых уязвимостей

Для поиска активов по трендовым уязвимостям может использоваться псевдоним `@VULNERS.ISTREND`.

Для поиска активов по дате попадания уязвимости в список трендовых может использоваться псевдоним `@VULNERS.ISTRENDSINCE`.

Псевдонимы пакетов уязвимостей

Для поиска активов по идентификатору пакета уязвимостей, в котором содержится информация об уязвимостях на этих активах, может использоваться псевдоним `@VULNERS.PACKAGEID`.

Для поиска активов по версии пакета уязвимостей, в котором содержится информация об уязвимостях на этих активах, может использоваться псевдоним `@VULNERS.PACKAGEVERSION`.

Для поиска активов по описанию пакета уязвимостей, в котором содержится информация об уязвимостях на этих активах, может использоваться псевдоним `@VULNERS.PACKAGEDESCRIPTION`.

2.7.1.7. Псевдонимы полей паспорта уязвимости

Поля паспортов уязвимостей могут рассматриваться как виртуальные объекты типа VulnerPassport.<Поле>. Фильтрация уязвимостей и настройка представления данных о них могут осуществляться с помощью псевдонимов для полей паспортов уязвимостей.

Общие псевдонимы

Для поиска уязвимостей по их паспортам может использоваться псевдоним `@VULNERPASSPORT`, с помощью которого можно обращаться к полям паспорта уязвимости.

Для поиска уязвимостей по названиям может использоваться псевдоним `@VULNERPASSPORT.NAME`.

Для поиска уязвимостей по описаниям может использоваться псевдоним `@VULNERPASSPORT.DESCRIPTION`.

Для поиска уязвимостей по уровням опасности может использоваться псевдоним `@VULNERPASSPORT.SEVERITYRATING`.

Для поиска уязвимостей по датам публикаций их паспортов может использоваться псевдоним `@VULNERPASSPORT.ISSUETIME`.

Для поиска уязвимостей по способам устранения может использоваться псевдоним `@VULNERPASSPORT.HOWTOFIX`.

Для поиска уязвимостей по ссылкам из паспортов на информацию об уязвимостях может использоваться псевдоним `@VULNERPASSPORT.LINKS`.

Для поиска уязвимостей по возможности пентест-проверки для их обнаружения может использоваться псевдоним `@VULNERPASSPORT.HASPENTESTCHECK`.

Псевдонимы идентификаторов

Для поиска уязвимостей по идентификаторам их паспортов может использоваться псевдоним `@VULNERPASSPORT.ID`.

Для поиска уязвимостей по уникальному идентификатору в базе данных уязвимостей Knowledge Base в MaxPatrol VM может использоваться псевдоним `@VULNERPASSPORT.KB`.

Для поиска уязвимостей по идентификаторам паспортов может также использоваться псевдоним `@VULNERPASSPORT.IDS`, с помощью которого можно обращаться к любым идентификаторам уязвимостей в публичных базах данных (например, в CVE и банке данных угроз ФСТЭК), кроме идентификаторов в Knowledge Base.

Для поиска уязвимостей по идентификаторам паспортов в базе данных CVE может использоваться псевдоним `@VULNERPASSPORT.CVES`. Базу уязвимостей см. на сайте mitre.org.

Псевдонимы оценок и векторов по стандарту CVSS

Для поиска уязвимостей по общим оценкам может использоваться псевдоним `@VULNERPASSPORT.SCORE`. Если в паспорте заполнен базовый вектор CVSS v3, общая оценка заполняется на основании заполненного значения `@VULNERPASSPORT.CVSS3SCORE`, иначе — на основании значения `@VULNERPASSPORT.CVSS2SCORE`.

Для поиска уязвимостей по базовым оценкам могут использоваться псевдонимы `@VULNERPASSPORT.CVSS2BASESCORE` и `@VULNERPASSPORT.CVSS3BASESCORE`; по временным оценкам — псевдонимы `@VULNERPASSPORT.CVSS2TEMPORALSCORE` и `@VULNERPASSPORT.CVSS3TEMPORALSCORE`.

Для поиска уязвимостей по базовым метрикам могут использоваться псевдонимы `@VULNERPASSPORT.CVSS2BASEVECTOR` и `@VULNERPASSPORT.CVSS3BASEVECTOR`, по временным метрикам — псевдонимы `@VULNERPASSPORT.CVSS2TEMPORALVECTOR` и `@VULNERPASSPORT.CVSS3TEMPORALVECTOR`. Если в паспортах уязвимостей указаны базовые

векторы (совокупность базовых метрик), для поиска уязвимостей по общему вектору уязвимости могут использоваться псевдонимы `@VULNERPASSPORT.CVSS2VECTOR` и `@VULNERPASSPORT.CVSS3VECTOR`.

Описание оценок, метрик и векторов уязвимостей по стандарту CVSS см. на сайте first.org.

Псевдонимы метрик

Для поиска уязвимостей по метрикам из паспортов может использоваться псевдоним `@VULNERPASSPORT.METRICS`. Если в паспорте есть информация о конкретных метриках, то могут использоваться псевдонимы этих метрик:

— если есть возможность эксплуатации уязвимости — псевдоним `@VULNERPASSPORT.METRICS.EXPLOITABLE`;

— если уязвимость может быть устранена — псевдоним `@VULNERPASSPORT.METRICS.HASFIX`;

— если есть возможность эксплуатации уязвимости по сети — псевдоним `@VULNERPASSPORT.METRICS.HASNETWORKATTACKVECTOR`.

Псевдонимы уязвимого программного обеспечения

Для поиска уязвимостей по программному обеспечению, на которое они нацелены, может использоваться псевдоним `@VULNERPASSPORT.AFFECTEDCOMPONENTS`.

Для поиска уязвимостей по названию уязвимого программного обеспечения может использоваться псевдоним `@VULNERPASSPORT.AFFECTEDCOMPONENTS.NAME`; по поставщику — псевдоним `@VULNERPASSPORT.AFFECTEDCOMPONENTS.VENDOR`.

Псевдонимы трендовых уязвимостей

Для поиска трендовых уязвимостей может использоваться псевдоним `@VULNERPASSPORT.ISTREND`.

Для поиска уязвимостей по дате попадания в список трендовых может использоваться псевдоним `@VULNERPASSPORT.ISTRENDSINCE`.

Псевдонимы пакетов уязвимостей

Для поиска уязвимостей по идентификатору пакета уязвимостей, в котором содержатся паспорта этих уязвимостей, может использоваться псевдоним `@VULNERPASSPORT.PACKAGEID`.

Для поиска уязвимостей по версии пакета уязвимостей, в котором содержатся паспорта этих уязвимостей, может использоваться псевдоним `@VULNERPASSPORT.PACKAGEVERSION`.

Для поиска уязвимостей по описанию пакета уязвимостей, в котором содержатся паспорта этих уязвимостей, может использоваться псевдоним `@VULNERPASSPORT.PACKAGEDESCRIPTION`.

2.7.2. Псевдонимы колонок таблицы

Для более понятного отображения информации при выборе колонок в таблице активов и при группировке записей могут использоваться псевдонимы. В этом случае наименования полей или выражения преобразуются в выбранные имена.

Псевдоним может содержать только латинские буквы, цифры, символ подчеркивания и точку.

Синтаксис: `<Поле> as <Имя>` или `<Выражение> as <Имя>`

Пример

```
Select(Host.IpAddress as Ip, Host.FQDN as FQDN, Host.IsVirtual as IsVirtual) |
Group(count(*) as Total)
```

2.7.3. Псевдонимы запросов для операции объединения

В таблицах с результатами выполнения запросов могут быть колонки таблиц активов с одинаковыми названиями. При объединении результатов выполнения этих запросов необходимо избежать повторения названий колонок. Это можно сделать с помощью псевдонимов запросов.

В качестве псевдонима для запроса вы можете использовать один или несколько символов, которые будут добавлены к названиям всех колонок в таблице с результатами объединения запроса. Например, при использовании псевдонима A колонки будут иметь названия 1, 2, ..., n, A.1, A.2, ..., A.n.

Псевдоним запроса может содержать латинские или русские буквы, цифры, знак подчеркивания и дефис; не может содержать только цифры и не может начинаться с дефиса.

Синтаксис: `<Запрос> as <Псевдоним>`

Псевдоним запроса для операции не является обязательным. Если псевдоним не задан, для операции объединения используется название колонки.

Пример

```
Select(@Computer, Computer.Processes.Name, Computer.Processes.PID,
Computer.Processes.ParentPID) | Join(Select(@Computer, Computer.Processes.Name,
Computer.Processes.PID) as P, @Computer = P.@Computer and
Computer.Processes.ParentPID = P.Computer.Processes.PID) | Select(@Computer,
Computer.Processes.Name as child_proc, P.Computer.Processes.Name as parent_proc)
```

2.8. Операторы

При создании условия фильтрации активов на языке PDQL для объединения операндов в предикаты используются операторы.

Таблица 1. Операторы для создания предикатов условия фильтрации активов

Оператор	Значение	Синтаксис
=	Проверка на равенство. **Примечание.** `<Операнд> = null` не может применяться для псевдонимов	`<Операнд> = <Значение>`
!=	Проверка неравенства. Возвращает true, если исходное значение равно false, и наоборот	`<Операнд> != <Значение>` Для удобства работы вы можете использовать `<Операнд>` вместо `<Операнд> != null`
>	Проверка на строгое неравенство (больше)	`<Операнд> > <Значение>`
<	Проверка на строгое неравенство (меньше)	`<Операнд> < <Значение>`
>=	Проверка на нестрогое неравенство (больше или равно)	`<Операнд> >= <Значение>`
<=	Проверка на нестрогое неравенство (меньше или равно)	`<Операнд> <= <Значение>`
IN	Вхождение значения в массив или диапазон	`<Операнд> IN [<Значение 1>, …, Значение N>]` `<Операнд> IN <Сеть>`
LIKE	Проверка соответствия строки шаблону. Шаблон задается с помощью знаков подчеркивания (_) и процента (%). Знак процента заменяет в шаблоне любое количество символов, а знак подчеркивания заменяет один символ	`<Операнд> LIKE <Шаблон>` **Примечание.** Перед применением оператора все неслужебные символы приводятся к нижнему регистру
MATCH	Проверка соответствия строки шаблону. Шаблон задается с помощью регулярных выражений	`<Операнд> MATCH <Шаблон>` **Примечание.** Перед применением оператора все неслужебные символы приводятся к нижнему регистру
-	Разность — период в прошлом	`Now() - <Период>`
+	Сумма — период в будущем	`Now() + <Период>`
CONTAINS	Проверка вхождения указанного значения в список значений операнда	`<Операнд> CONTAINS <Значение>`
INTERSECT	Проверка пересечения множеств значений	`<Операнд> INTERSECT [Массив значений]`

Логические операторы используются для объединения предикатов в условие фильтрации активов.

Примечание. Все операторы регистронезависимы, то есть при обработке запроса система игнорирует регистр символов.

Таблица 2. Операторы для создания условия фильтрации активов

Оператор	Значение	Синтаксис	Комментарии
AND	Логическое И	<Предикат 1> AND <Предикат 2>	Если <Предикат 1> дает выборку setПредикат1, а <Предикат 2> — выборку setПредикат2, то <Предикат 1> AND <Предикат 2> даст выборку setПредикат1 пересечение setПредикат2
NOT	Логическое НЕ. Положение оператора ограничивает ветку актива, к которой применяется отрицание выполнения условия	NOT <Предикат> <Предикат 1> NOT LIKE <Предикат 2> **Примечание.** Вы также можете использовать конструкции NOT MATCH, NOT IN, NOT CONTAINS и NOT INTERSECT	Запрос not Host.Softs.Name like 'A' позволяет найти все сетевые узлы, на которых нет ПО, а также все сетевые узлы, на которых установлено хотя бы одно ПО, но ни одно из них не называется «А» Запрос Host.Softs.Name not like 'A' позволяет найти все сетевые узлы, на которых установлено хотя бы одно ПО, но ни одно из них не называется «А»
OR	Логическое ИЛИ	<Предикат 1> OR <Предикат 2>	Если <Предикат 1> дает выборку setПредикат1, а <Предикат 2> — выборку setПредикат2, то <Предикат 1> OR <Предикат 2> даст выборку setПредикат1 объединение setПредикат2

3. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

3.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

3.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

3.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

3.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

3.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

3.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 3).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 3. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

3.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Типы данных

В MaxPatrol VM каждое поле или ячейка имеют определенный тип данных.

Таблица 4. Используемые типы данных

Тип	Описание	Пример
Bool	Логическое значение	`True`, `False`
DateTime	Для фильтрации активов время в формате YYYY-MM-DD'T'HH:MM:SS	`2020-07-22T18:08:38`
Enum	Один из элементов предопределенного списка значений	—
IPAddress	IP-адрес стандарта IPv4 или IPv6	`192.0.2.235`, `1080:0:0:0:8:800:200C:417A`
KeyValue	Ассоциативный массив пар «ключ — значение»	`{"Красный":"Каждый", "Оранжевый":"Охотник", "Желтый":"Желает"}`
List	Список. Один список может содержать элементы разных типов	`["Порт ", 22, " открыт"]`
MACAddress	MAC-адрес	`00:53:00:B8:DF:B8`
Network	Адрес подсети с маской в формате CIDR	`192.0.2.0/24`
Null	Отсутствие данных	`null`
Number	Целое число от –223372036854775808 до 9223372036854775807	`-3`, `0`, `12`
String	Строка	`"Порт 22 открыт"`
StringList	Список, элементы которого имеют тип данных String	`["Красный", "Оранжевый", "Желтый", "Зеленый"]`
UUID	Идентификатор в формате RFC 4122 — 16-байтный (128-битный) номер	`123e4567-e89b-12d3-a456-426655440000`
UUIDList	Список идентификаторов UUID	`["00000005-9d7c-011d-f000-0001e5c6e294", "00000005-9d7c-011d-f000-0001e5c6e295"]`

Приложение Б. Математические функции для работы с данными в системе

В MaxPatrol VM вы можете использовать математические функции для анализа данных.

Функция Avg

Функция с аргументом All используется для подсчета среднего значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Avg ([All] [Поле 1]) Where [Условие фильтрации] Group by
[Поле 2] Over time [Период]
```

Функция Count

Функция используется для подсчета количества значений за указанный период. Применяется к данным любого типа. Возвращает для каждой группы единственное значение с типом данных Number.

Функция с аргументом All используется для подсчета количества всех значений с любым типом данных, кроме Null, в выбранной колонке [Поле 1] за указанный период.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Count ([All] [Поле 1]) Where [Условие фильтрации] Group
by [Поле 2] Over time [Период]
```

Функция с аргументом Distinct используется для подсчета количества уникальных значений с любым типом данных, кроме Null, в выбранной колонке [Поле 1] за указанный период.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Count ([Distinct] [Поле 1]) Where [Условие фильтрации]
Group by [Поле 2] Over time [Период]
```

Функция Count (*) используется для подсчета количества всех значений (в том числе повторяющихся и с типом данных Null) в таблице.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Count (*) Where [Условие фильтрации] Group by [Поле 2]
Over time [Период]
```

Функция Countunique

Функция используется для подсчета количества уникальных значений в выбранной колонке [Поле 1] за указанный период. Также функция может использоваться для подсчета количества уникальных записей исходной таблицы, сформированных из указанных колонок [Поле 1], ..., [Поле N]. Применяется к данным любого типа. Возвращает для каждой группы единственное значение с типом данных Number.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Countunique ([Поле 1], …, [Поле N]) Where [Условие
фильтрации] Group by [Поле 2] Over time [Период]
```

Функция Max

Функция с аргументом All используется для поиска максимального значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Max ([All] [Поле1]) Where [Условие фильтрации] Group by
[Поле 2] Over time [Период]
```

Функция Median

Функция с аргументом All используется для поиска медианного значения в выбранной колонке [Поле 1] за указанный период. Данные в колонке сортируются. Для наборов с нечетным числом элементов медианным считается значение центрального элемента, а для наборов с четным числом элементов — среднее значение двух центральных элементов. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Median ([All] [Поле1]) Where [Условие фильтрации] Group
by [Поле 2] Over time [Период]
```

Функция Min

Функция с аргументом All используется для поиска минимального значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Min ([All] [Поле 1]) WHERE [Условие фильтрации] Group by [Поле 2] Over time [Период]
```

Функция Sum

Функция с аргументом All используется для подсчета суммы всех значений в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Sum ([All] [Поле 1]) Where [Условие фильтрации] Group by [Поле 2] Over time [Период]
```

Приложение В. Значения псевдонима TypeAlias

В MaxPatrol VM при ручном создании активов и при импорте активов из файла используется псевдоним типа актива TypeAlias.

Таблица 5. Значения псевдонима TypeAlias

Значение	Тип устройства или операционная система, установленная на устройстве
acs	Система Cisco ACS
aix	Операционная система AIX
asa	Межсетевой экран Cisco ASA
bsd	Операционная система BSD, FreeBSD, macOS и OS X
checkpoint	Межсетевой экран Check Point GAiA и SPLAT
esxi	Гипервизор OVMware ESXi
fortigate	Межсетевой экран Fortinet FortiGate
fwsm	Межсетевой экран Cisco FWSM
hp_ux	Операционная система HP-UX
ios	Операционная система Cisco IOS и Cisco IOS XE
ise	Устройство Cisco ISE
junos	Операционная система Juniper Jun OS
linux	Операционная система семейства Linux
nexus	Коммутатор Cisco Nexus
omniswitch	Коммутатор Alcatel-Lucent OmniSwitch под управлением AOS
pan_os	Межсетевой экран Palo Alto под управлением PAN-OS
pix	Межсетевой экран Cisco PIX
solaris	Операционная система Solaris
vrp	Операционная система Huawei VRP
windows	Операционная система семейства Windows

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.