

# Работа с активами в MaxPatrol VM: что могут показать PDQL-запросы

Методичка к вебинару

## 1. Лайфхаки при работе с PDQL

- В Системе есть разные алиасы активов:  
(@Host, @WindowsHost, @UnixHost, @NetworkDeviceHost, @ActiveDirectory...)
- При выборе полей в SELECT'е Система будет подсказывать вам, какие поля вы можете добавить, как столбец:  
@Host, Host.<здесь появится список с подсказками>
- Вы можете присваивать псевдонимы для столбцов, чтобы вам было удобнее фильтровать данные в гриде:  
`select(@Host, Host.Endpoints<TransportEndpoint>.Port as Port) | filter(Port = 22)`

## 2. Чем вам будет полезен PDQL в MP VM?

**а) Для категоризации активов / поиска интересных данных на активах:**

**В динамических группах / В Pipeline (до SELECT):**

- Найти Windows рабочие станции:  
`WindowsHost.HostType = 'Desktop'`
- Найти сетевое оборудование Cisco:  
`NetworkDeviceHost.Vendor = 'Cisco'`

- Найти Linux / Unix активы:  
LinuxHost or UnixHost
- Найти активы с установленными VPN-клиентами:  
Computer.NetworkCard[Name like '%TAP%' or Name like '%VPN%' or Name like '%Tun%']
- Найти активы с установленным Adobe Reader 11.0.7:  
Host[Softs[Vendor = 'Adobe Systems' and Name = 'Reader' and Version = '11.0.7']]
- Найти активы из сетевого сегмента 192.168.2.0/24:  
Host.IpAddress in 192.168.2.0/24
- Найти активы, на которых не установлена KB982018:  
not (WindowsHost.Updates.UpdateId = "KB982018") and WindowsHost.Updates.UpdateId
- Найти активы, одновременно имеющие роль DNS и DHCP:  
Host.HostRoles.Role = 'Directory Service' AND Host.HostRoles.Role = 'Domain Controller'

#### **В Pipeline (после SELECT):**

- Найти активы без заданной значимости:  
select(@Host, Host.@Importance) | filter(Host.@Importance = 'ND')
- Найти активы, у которых >= 2 активных сетевых интерфейсов:  
select(@Host, Host.Interfaces.Name as name, Host.Interfaces.IsEnabled as enabled) | filter(name != "lo" and name != "Npcap Loopback Adapter" and name and enabled = true) | group(@Host, COUNT(\*) as result) | filter(result >= 2)
- Найти, какие версии Microsoft Office установлены в организации:  
Стандартный запрос "ПО Windows" + filter(SoftName = "Microsoft Office")
- Найти подобранные с помощью MP VM УЗ на активах:  
select(@Host as Host, Host.Endpoints<TransportEndpoint>.Port as Port, Host.Endpoints<TransportEndpoint>.Service.Checks<RemoteAccessAccountBruteforce>.Login as Login, Host.Endpoints<TransportEndpoint>.Service.Checks<RemoteAccessAccountBruteforce>.Password as Password) | filter(Login and Password) | sort(Host DESC)

#### **QSearch (до SELECT):**

- Найти активы, у которых встречается srv1 в Названии/Описании/ IP-адресе/FQDN'е:  
qsearch("srv1") | select(@Host)

**б) Для поиска паспортов уязвимостей:**

**Алиас: @VulnerPassport**

- Найти паспорт уязвимости CVE-2021-40444:  
`select(@VulnerPassport, VulnerPassport.CVEs) | filter(VulnerPassport.CVEs = "CVE-2021-40444")`
- Найти паспорта уязвимостей с оценкой > 9:  
`select(@VulnerPassport, VulnerPassport.Score) | filter(VulnerPassport.Score > 9)`

**в) Для поиска уязвимостей на активах:**

**Алиасы: @Vulners, @NodeVulners**

- Вывести все уязвимости:  
`select(@Host, Host.@Vulners) | filter(Host.@Vulners) | limit(0)`
- Вывести только уязвимости ОС:  
`select(@Host, Host.OsName, Host.OsVersion, Host.@NodeVulners) | filter(Host.@NodeVulners)`
- Вывести только уязвимости ПО:  
`select(@Host, Host.Softs.Name, Host.Softs.Version, Host.Softs.@NodeVulners) | filter(Host.Softs.@NodeVulners)`
- Вывести только уязвимости Linux пакетов:  
`select(@UnixHost, UnixHost.Packages.Name, UnixHost.Packages.Version, UnixHost.Packages.@NodeVulners) | filter(UnixHost.Packages.@NodeVulners)`
- Вывести только уязвимости сетевых служб:  
`select(@Host, Host.Endpoints<TransportEndpoint>.Port, Host.Endpoints<TransportEndpoint>.@Vulners) | filter(Host.Endpoints<TransportEndpoint>.@Vulners)`

**г) Для модификации виджетов:**

**Алиасы: @Vulners, @NodeVulners**

- Заходим в настройки виджета и указываем свой(-и)  
"Группы активов"/"Фильтр активов"/"Фильтр уязвимостей"/"Фильтр паспортов уязвимостей"

P.S.: Доступные варианты будут отличаться в зависимости от типа виджета

**д) Для создания «политик» по управлению сроками актуальности данных активов:**

**Алиасы:** @Vulners, @NodeVulners

- Создаём свою политику для Windows рабочих станций высокой значимости:  
WindowsHost.HostType = 'Desktop' and Host.@Importance = 'H'

**е) Для создания «политик» по управлению статусами уязвимостей:**

- Создаём свою политику для контроля устранения уязвимостей на windows рабочих станциях, у которых уже есть патчи (срок 2 месяца):

**Название:** Патчинг Windows рабочих станций

**Фильтр активов:** WindowsHost.HostType = 'Desktop'

**Фильтр уязвимостей:** Host.@NodeVulners.Metrics.HasFix = true

**Действие:** Плановое устранение

**Срок исправления:** 2 месяца

**Рассчитывать срок:** От даты публикации, взятой из паспорта уязвимости

---

**О компании**

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/PositiveTechnologies  
facebook.com/PHDays

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России – 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте [ptsecurity.com](#).