POSITIVE TECHNOLOGIES

Работа с активами в MaxPatrol VM:

что могут показать PDQL-запросы

Евгений Полян
Менеджер по продуктам
Positive Technologies

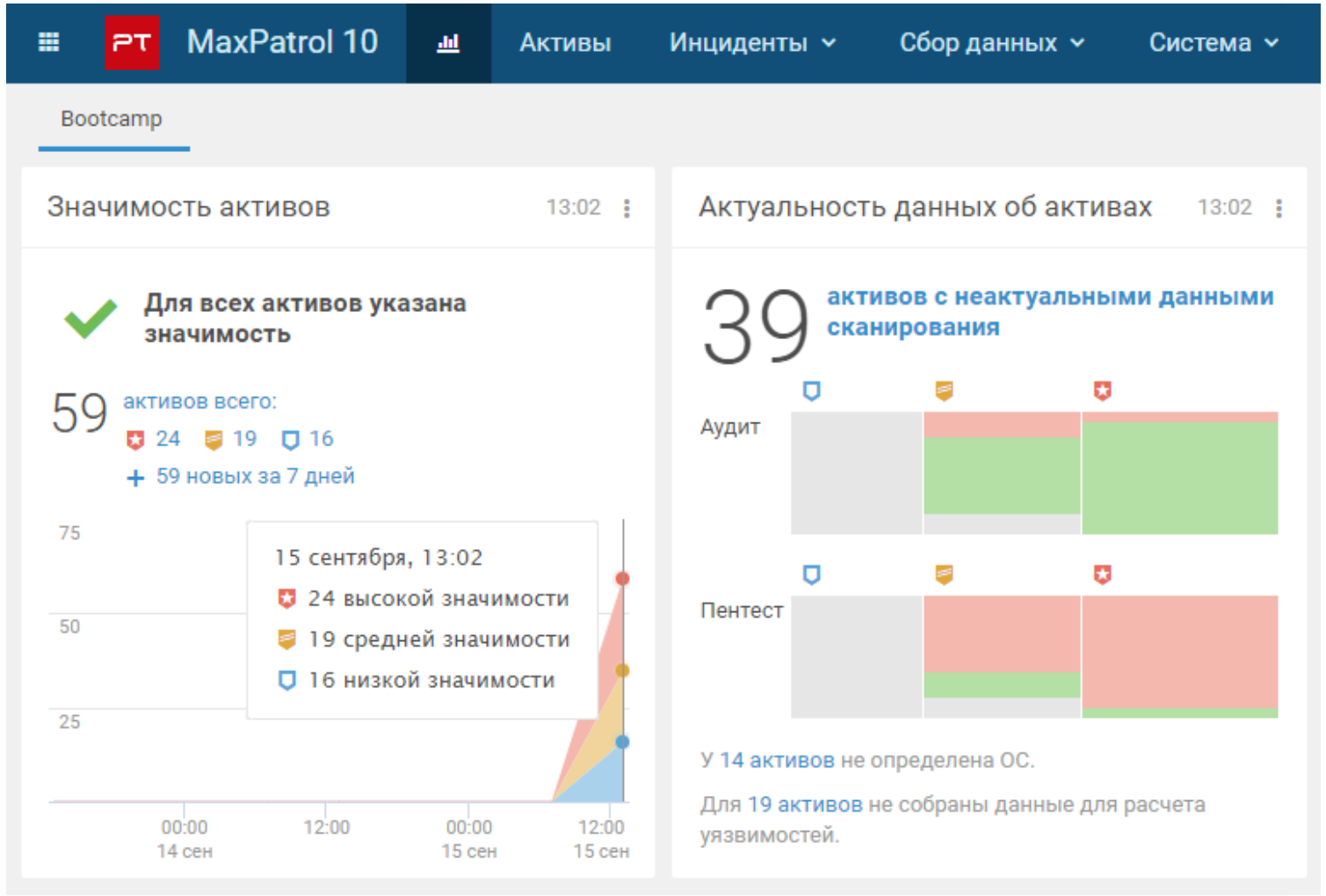
Антон Исаев
Специалист по продвижению технической экспертизы
Positive Technologies

ptsecurity.com

О ЧЕМ БУДЕТ ВЕБИНАР

01.

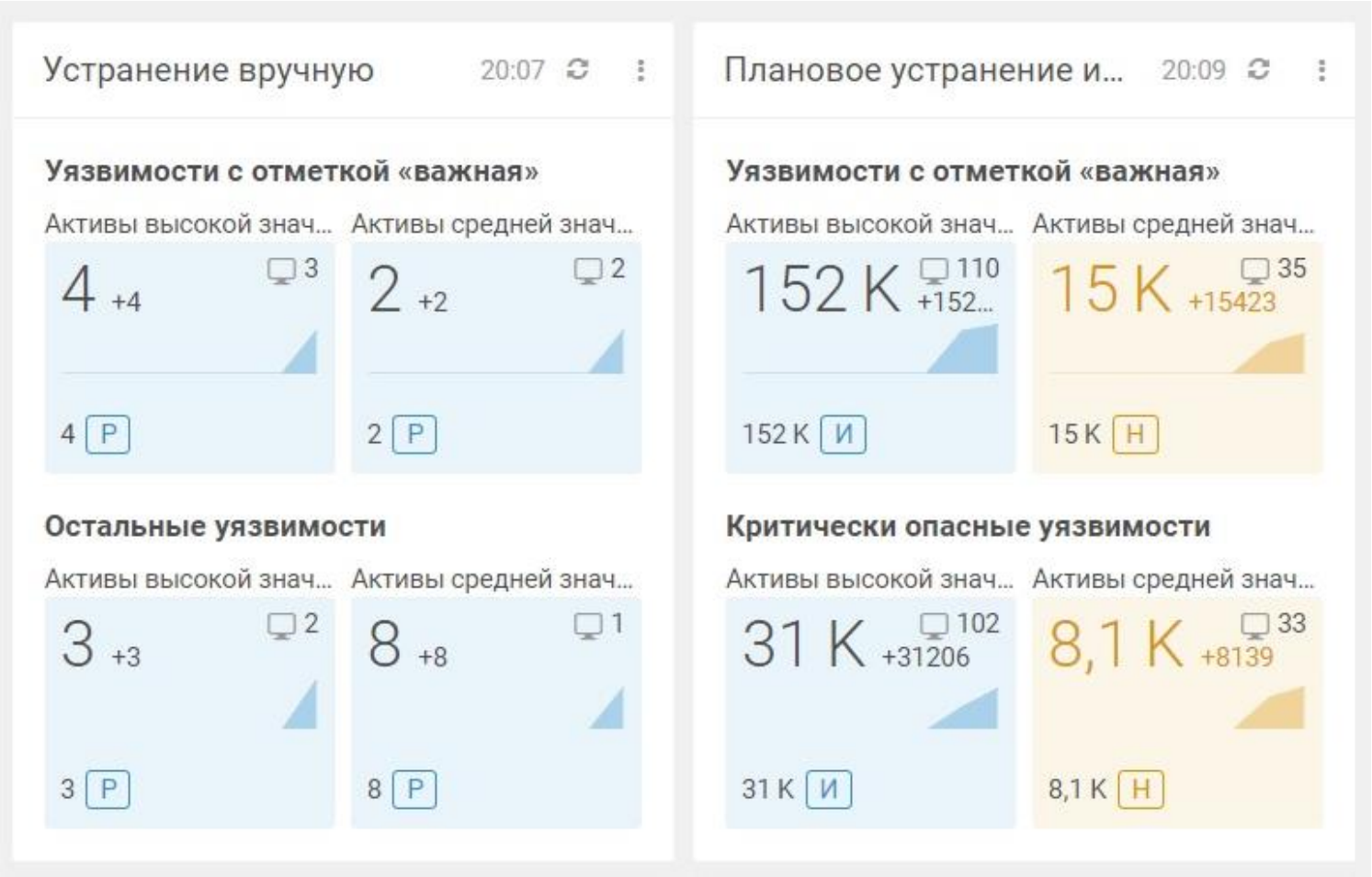
Как работать
с IT-активами



О ЧЕМ БУДЕТ ВЕБИНАР

02.

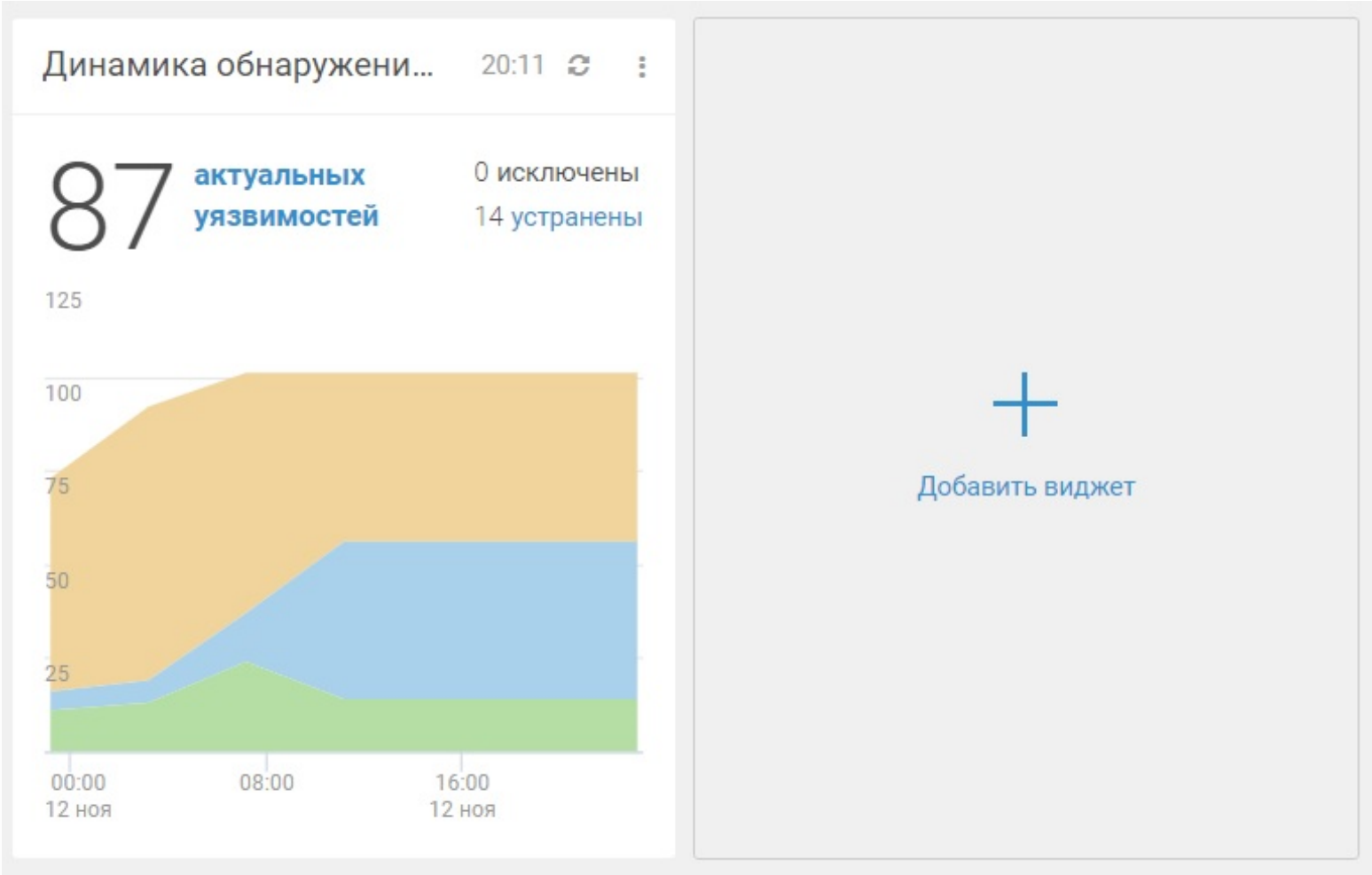
Как контролировать защищенность



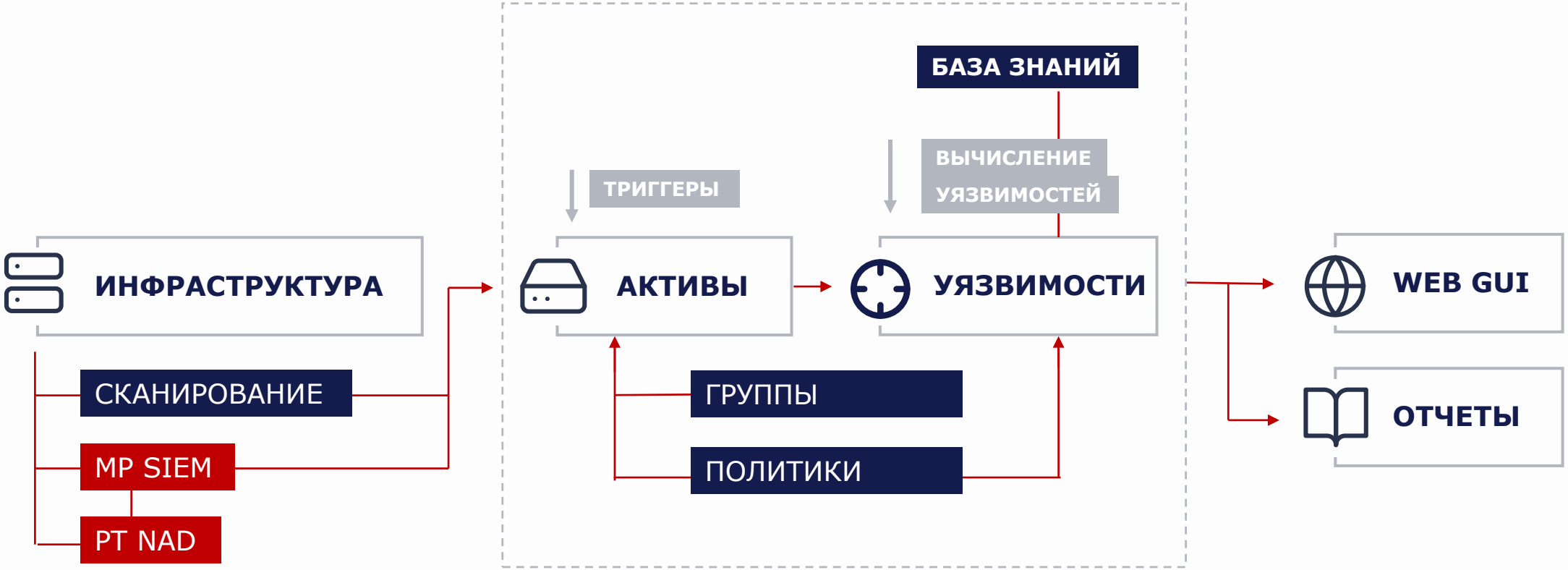
О ЧЕМ БУДЕТ ВЕБИНАР

03.

Как настроить виджеты под себя



ПОТОК ДАННЫХ MP VM



СБОР ИНФОРМАЦИИ ПО АКТИВАМ

ГРУППИРОВКА И ОЦЕНКА АКТИВОВ

ОПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ

АКТИВЫ

ptsecurity.com

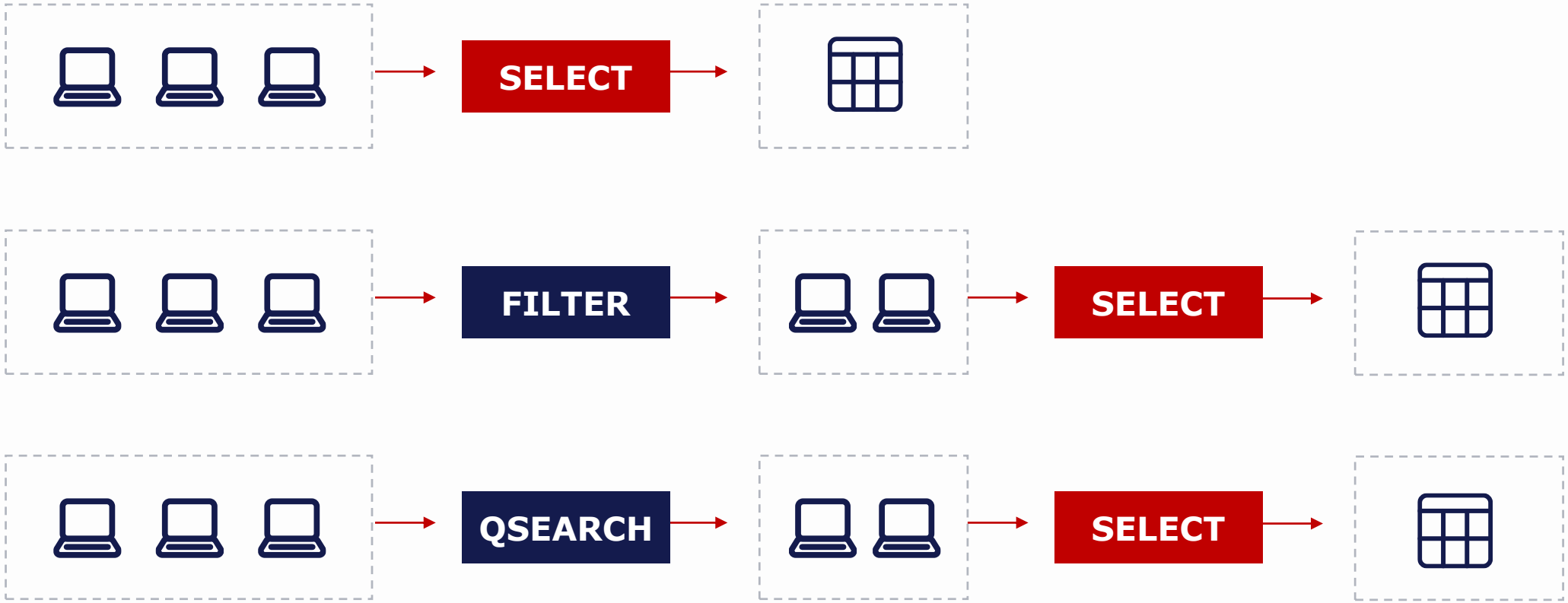
PDQL: Активы

```
select(@Host,
        Host.Fqdn,
        Host.IpAddress,
        Host.IsVirtual,
        Host.@AuditTime,
        Host.@PentestTime)
```

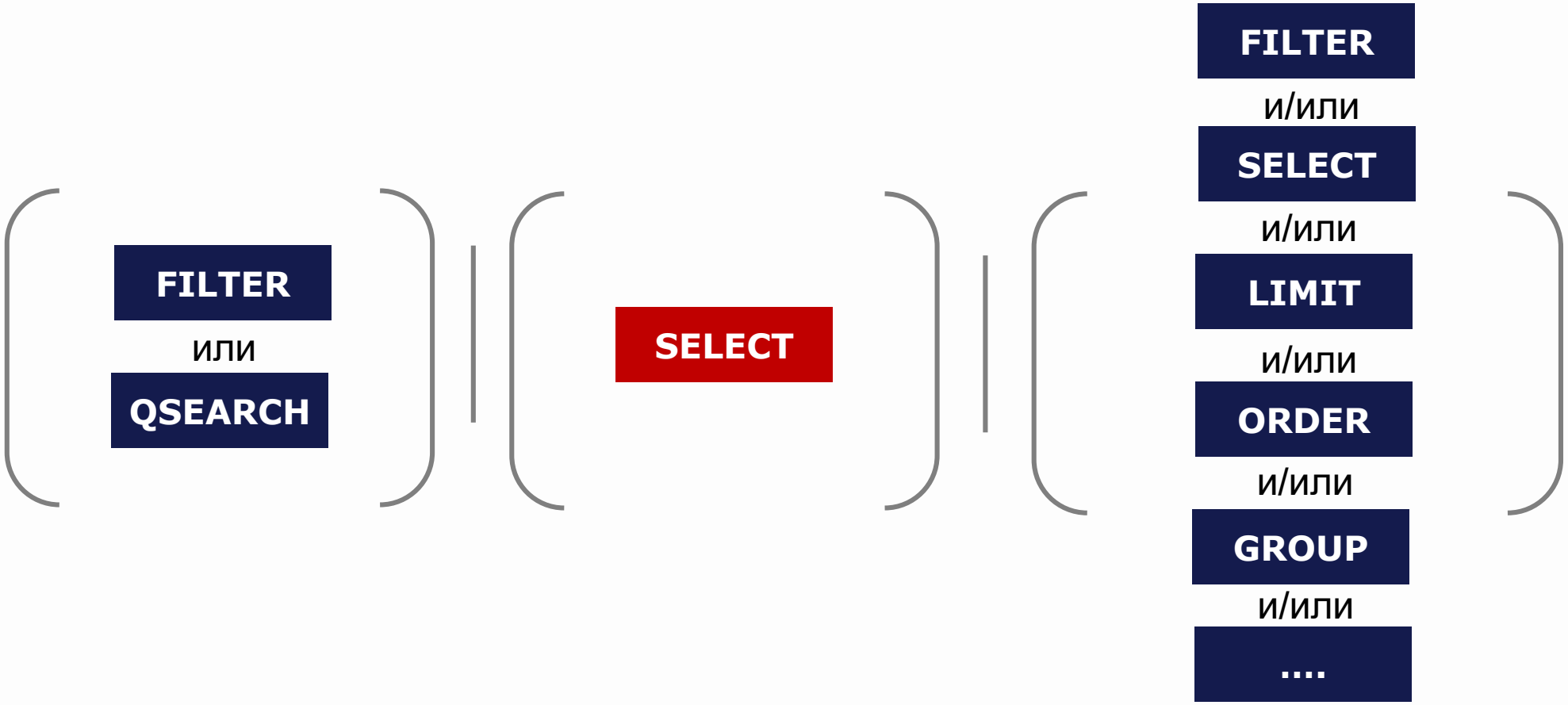
Тип актива	Графическое обозначение
Рабочая станция	
Сервер	
Маршрутизатор	
Сетевой коммутатор	
Межсетевой экран	
Точка доступа	
Неизвестное сетевое устройство	
Сетевой принтер	
Узел	

- @Host
- @WindowsHost
- @LinuxHost
- @ActiveDirectory
- @CiscoHost
- …

ФИЛЬТРЫ MP VM



СТРУКТУРА ЗАПРОСОВ



ЗАДАЧА: Поиск подобранных УЗ на активах

Конечные точки (endpoints)

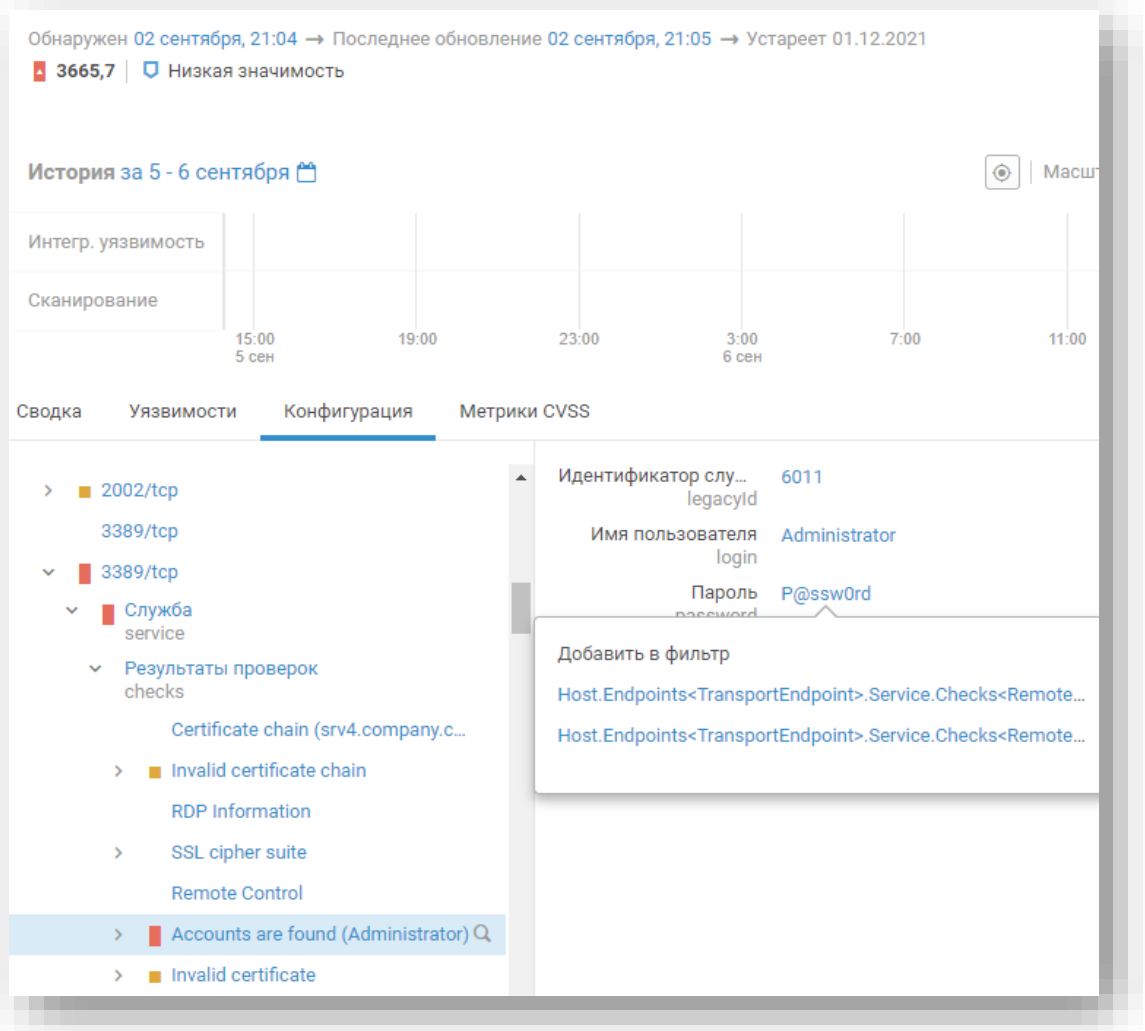
-> 3389/tcp

-> Служба (service)

-> Результаты проверок (checks)

-> Accounts are found

-> «Имя пользователя» и «Пароль»



ДОМАШНЕЕ ЗАДАНИЕ

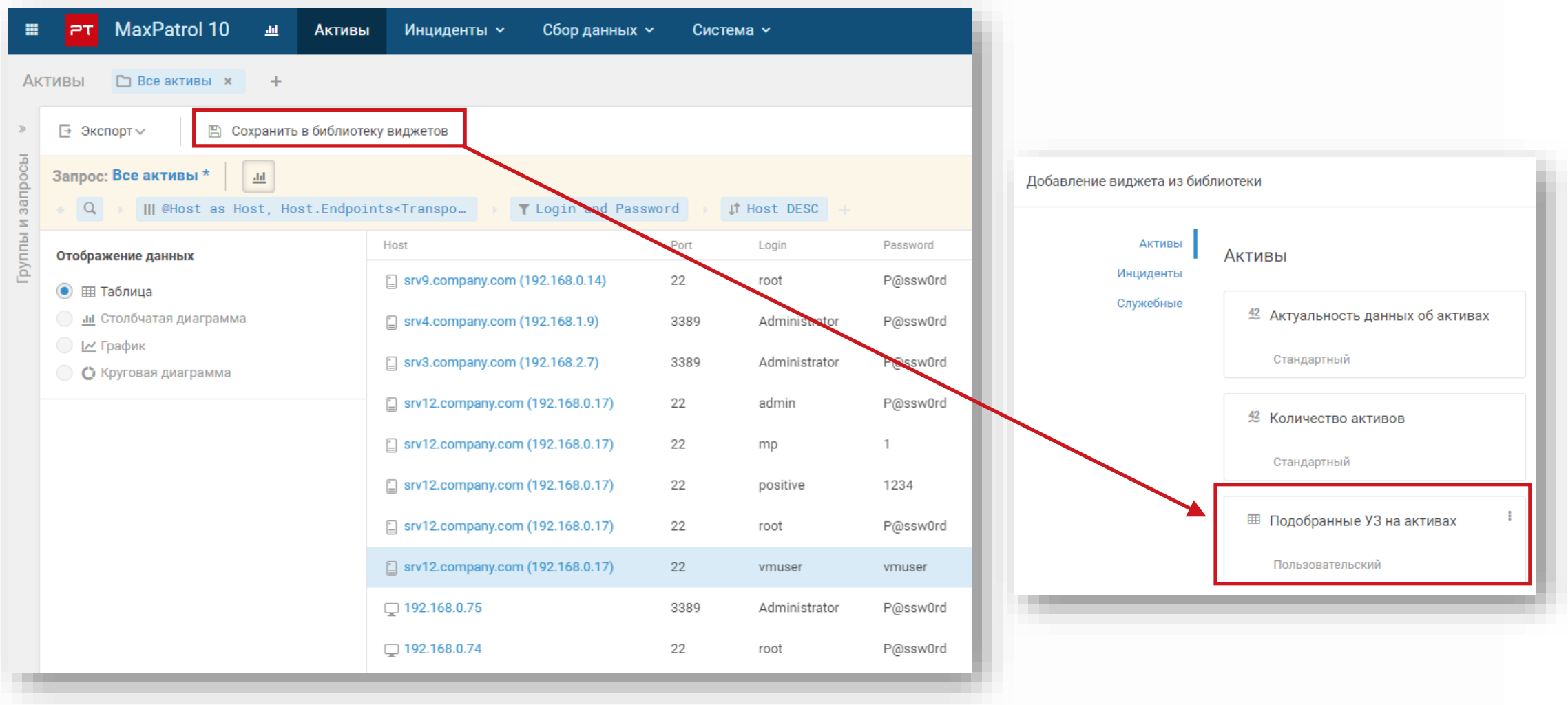
ЗАДАЧА: Поиск подобранных УЗ на активах

Запрос: Все активы *

@Host, Host.Endpoints<TransportEndpoi… | login and password | @Host DESC | Выполнить

Узел @Host	Порт Hos…	Имя пользователя login	Пароль password
srv9.company.com (192.168.0.14)	22	root	P@ssw0rd
srv4.company.com (192.168.1.9)	3389	Administrator	P@ssw0rd
srv3.company.com (192.168.2.7)	3389	Administrator	P@ssw0rd
srv12.company.com (192.168.0.17)	22	admin	P@ssw0rd
srv12.company.com (192.168.0.17)	22	mp	1
srv12.company.com (192.168.0.17)	22	positive	1234
srv12.company.com (192.168.0.17)	22	root	P@ssw0rd
srv12.company.com (192.168.0.17)	22	vmuser	vmuser
192.168.0.75	3389	Administrator	P@ssw0rd
192.168.0.74	22	root	P@ssw0rd

СОЗДАНИЕ ВИДЖЕТА ИЗ ГРИДА



НАХОДИМ УСТАНОВЛЕННОЕ ПО

Какие версии Microsoft Office установлены в организации?

Сводка | Уязвимости | Конфигурация | Метрики CVSS

Программное обеспече... softs
- Adobe Flash Player ...
- CryptoPro CSP 2.0.2...
- CryptoPro TLS 2.0.2...
- Microsoft Internet
- Microsoft Windows
- Microsoft Access 2
- Microsoft Excel 20
- Microsoft FrontPag...
- Microsoft InfoPath ...
- Microsoft Office Co...
- Microsoft Office 2003
- Microsoft OneNote ...
- Microsoft Outlook 2...

Архитектура architecture	x86
Путь установ... installPath	C:\Program files\Microsoft office\Office11\
Название	Microsoft Office
Основная ве... majorVersion	11
Ключ продук... productKey	GWH18-DGCMP-PTRC5-6J4MT-3GFDY
Пакет обнов... servicePack	3

Добавить в фильтр
- Host.Softs.Name = 'Microsoft Office'
- Host.Softs.Name != 'Microsoft Office'

Запросы
- ПО Windows
- ПО Windows, группировка по версии

Запрос: ПО Windows, группировка по версии *

WindowsHost.Softs | @WindowsHost, WindowsHost.Softs.Name ... | Уникальные | Выполнить

@WindowsHost ASC | SoftName, SoftVersion, COUNT(*) | SoftName = "Microsoft Office"

Название SoftName	Версия SoftVersion	COUNT(*)	Узел @WindowsHost	Название SoftName	Версия SoftVersion	Дата и время последнего обновлен... WindowsHost.@UpdateTime
Microsoft Office	2013	2	pc8.company.com (192.168.0.94)	Microsoft Office	2013	Сегодня, в 9:46
Microsoft Office	2010	1	pc9.company.com (192.168.0.95)	Microsoft Office	2013	Сегодня, в 9:47
Microsoft Office	2016	2				
Microsoft Office	2003	1				

ФИЛЬТР: SoftName = "Microsoft Office"

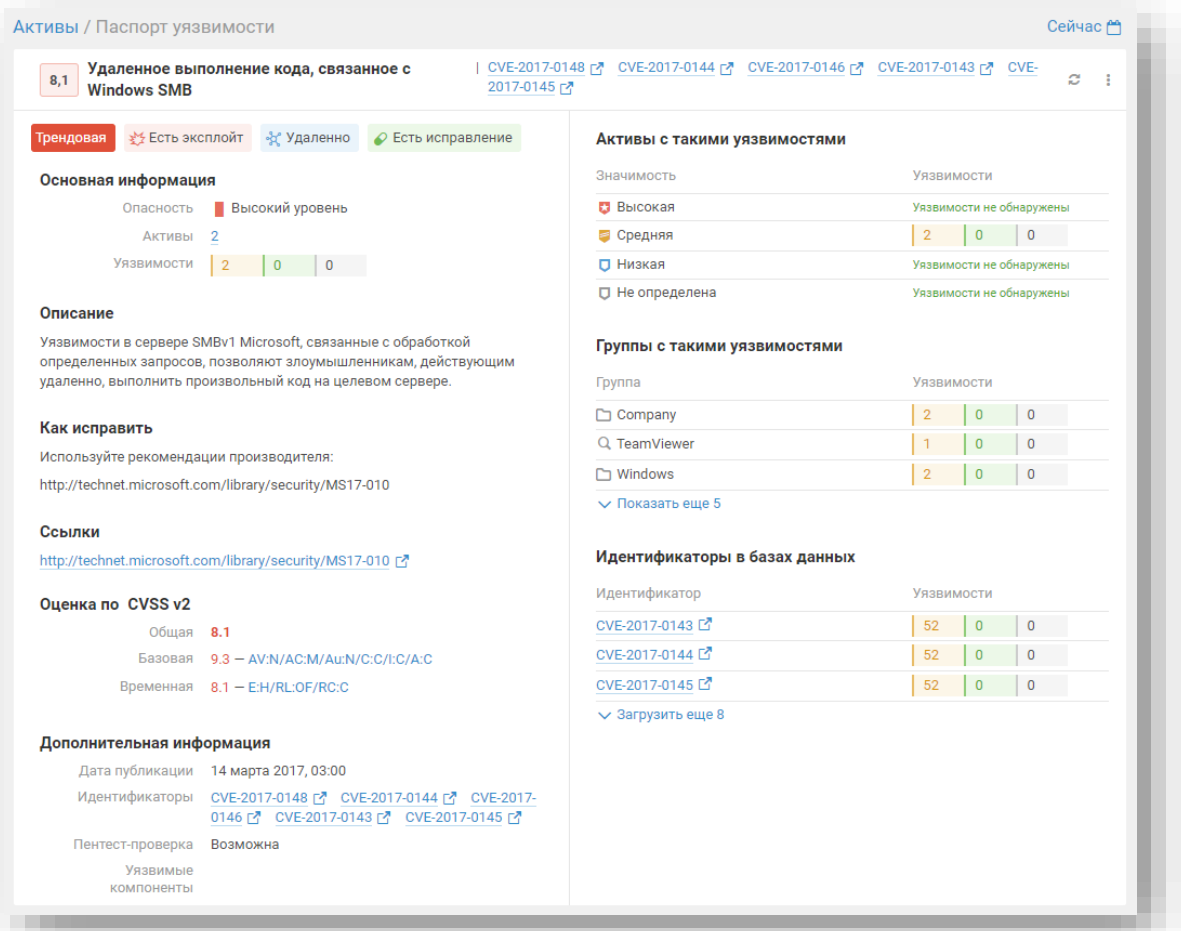
ПАСПОРТ УЯЗВИМОСТЕЙ

ptsecurity.com

PDQL: Паспорта уязвимостей

@VulnerPassport

```
select(@VulnerPassport,
        VulnerPassport.CVEs,
        VulnerPassport.SeverityRating,
        VulnerPassport.Score,
        VulnerPassport.HasPentestCheck,
        VulnerPassport.Metrics)
```



Активы / Паспорт уязвимости

Сейчас

8,1 **Удаленное выполнение кода, связанное с Windows SMB** | CVE-2017-0148 CVE-2017-0144 CVE-2017-0146 CVE-2017-0143 CVE-2017-0145

Трендовая | Есть эксплойт | Удаленно | Есть исправление

Основная информация

Опасность: Высокий уровень

Активы: 2

Уязвимости: 2 | 0 | 0

Описание

Уязвимости в сервере SMBv1 Microsoft, связанные с обработкой определенных запросов, позволяют злоумышленникам, действующим удаленно, выполнить произвольный код на целевом сервере.

Как исправить

Используйте рекомендации производителя:

http://technet.microsoft.com/library/security/MS17-010

Ссылки

http://technet.microsoft.com/library/security/MS17-010

Оценка по CVSS v2

Общая: 8.1

Базовая: 9.3 — AV:N/AC:M/Au:N/C:C/I:C/A:C

Временная: 8.1 — E:H/RL:OF/RC:C

Дополнительная информация

Дата публикации: 14 марта 2017, 03:00

Идентификаторы: CVE-2017-0148 CVE-2017-0144 CVE-2017-0146 CVE-2017-0143 CVE-2017-0145

Пентест-проверка: Возможна

Уязвимые компоненты:

Активы с такими уязвимостями

Значимость	Уязвимости
Высокая	Уязвимости не обнаружены
Средняя	2 | 0 | 0
Низкая	Уязвимости не обнаружены
Не определена	Уязвимости не обнаружены

Группы с такими уязвимостями

Группа	Уязвимости
Company	2 | 0 | 0
TeamViewer	1 | 0 | 0
Windows	2 | 0 | 0

Показать еще 5

Идентификаторы в базах данных

Идентификатор	Уязвимости
CVE-2017-0143	52 | 0 | 0
CVE-2017-0144	52 | 0 | 0
CVE-2017-0145	52 | 0 | 0

Загрузить еще 8

PDQL: Паспорта уязвимостей

Запрос: **Все активы** *

```
@VulnerPassport, VulnerPassport.CVEs, …
VulnerPassport.IssueTime DESC
```

Паспорт уязвимости @VulnerPassport	CVE-идентификат… VulnerPassport.CV…	Уровен… VulnerP…	Оценка… VulnerP…	Дата публикации … VulnerPassport.Iss…	Пентест-проверка VulnerPassport.H…	Трендовая VulnerPas…	Метрики … VulnerPas…	Эксплойт VulnerP…	Устранима VulnerPas…	Удаленная эксплуатация VulnerPassport.Metrics.H…
Использование после освобождения	CVE-2021-30600	High	6,4	16 августа, 03:00	False	False		False	True	True
Использование после освобождения	CVE-2021-30604	High	6,4	16 августа, 03:00	False	False		False	True	True
Использование после освобождения	CVE-2021-30601	High	6,4	16 августа, 03:00	False	False		False	True	True
Смешение типов	CVE-2021-30598	High	6,4	16 августа, 03:00	False	False		False	True	True
Смешение типов	CVE-2021-30599	High	6,4	16 августа, 03:00	False	False		False	True	True
Использование после освобождения	CVE-2021-30602	High	6,4	16 августа, 03:00	False	False		False	True	True
Состояние гонки	CVE-2021-30603	High	6,4	16 августа, 03:00	False	False		False	True	True
Уязвимость CVE-2021-3677	CVE-2021-3677	Medium	5,7	12 августа, 03:00	False	False		False	True	True
Уязвимость CVE-2021-29987	CVE-2021-29987	High	6,4	10 августа, 03:00	False	False		False	True	True
Повышение привилегий	CVE-2021-34487	High	6,1	10 августа, 03:00	False	False		False	True	False
Удаленное выполнение кода	CVE-2021-36947	High	8,2	10 августа, 03:00	False	False		True	True	True
Раскрытие информации	CVE-2021-26433	High	6,5	10 августа, 03:00	False	False		False	True	True

НАХОДИМ ОПАСНЫЕ УЯЗВИМОСТИ

Сколько паспортов уязвимостей с оценкой > 9?

Запрос: Все активы *

@VulnerPassport, VulnerPassport.CVEs, … | VulnerPassport.IssueTime DESC | VulnerPassport.CVEs in ['CVE-2017-014… | Выполнить

Паспорт уязвимости @VulnerPassport	CVE-идентификат… VulnerPassport.CV…	Уровен… VulnerP…	Оценка… VulnerP…	Дата публикации … VulnerPassport.Iss…	Пентест-проверка VulnerPassport.H…	Трендовая VulnerPas…	Метрики … VulnerPas…	Эксплойт VulnerP…	Устранима VulnerPas…	Удаленная эксплуатация VulnerPassport.Metrics.…
Разглашение информации, связанн…	CVE-2017-0147	Medium	5,2	14 марта 2017, 03:00	True	True		False	True	True
Удаленное выполнение кода, связа…	CVE-2017-0143	High	8,1	14 марта 2017, 03:00	True	True		True	True	True
Удаленное выполнение кода, связа…	CVE-2017-0143	High	7,1	14 марта 2017, 03:00	True	True		False	True	True
Разглашение информации, связанн…	CVE-2017-0147	Medium	5,2	14 марта 2017, 03:00	True	True		False	True	True

Оценка по CVSS v2

Общая	8.1
Базовая	9.3 — AV:N/AC:M/Au:N/C:C/I:C/A:C
Временная	8.1 — E:H/RL:OF/RC:C

ПОДСКАЗКА:
VulnerPassport.Score

НАХОДИМ УЯЗВИМЫЕ АКТИВЫ

Сколько в организации активов с уязвимостью CVE-2019-0708?

Запрос: Все активы *

@VulnerPassport, VulnerPassport.CVEs, … | VulnerPassport.IssueTime DESC | VulnerPassport.CVEs in ['CVE-2017-014… | Выполнить

Паспорт уязвимости @VulnerPassport	CVE-идентификат… VulnerPassport.CV…	Уровен… VulnerP…	Оценка… VulnerP…	Дата публикации … VulnerPassport.Iss…	Пентест-проверка VulnerPassport.H…	Трендовая VulnerPas…	Метрики … VulnerPas…	Эксплойт VulnerP…	Устранима VulnerPas…	Удаленная эксплуатация VulnerPassport.Metrics.…
Разглашение информации, связанн…	CVE-2017-0147	Medium	5,2	14 марта 2017, 03:00	True	True		False	True	True
Удаленное выполнение кода, связа…	CVE-2017-0143	High	8,1	14 марта 2017, 03:00	True	True		True	True	True
Удаленное выполнение кода, связа…	CVE-2017-0143	High	7,1	14 марта 2017, 03:00	True	True		False	True	True
Разглашение информации, связанн…	CVE-2017-0147	Medium	5,2	14 марта 2017, 03:00	True	True		False	True	True

8,1 Удаленное выполнение кода, связанное с Windows SMB

Трендовая | Есть эксплойт | Удаленно | Есть исправление

Основная информация

Опасность: Высокий уровень

Активы: 2

Уязвимости: 2 | 0 | 0

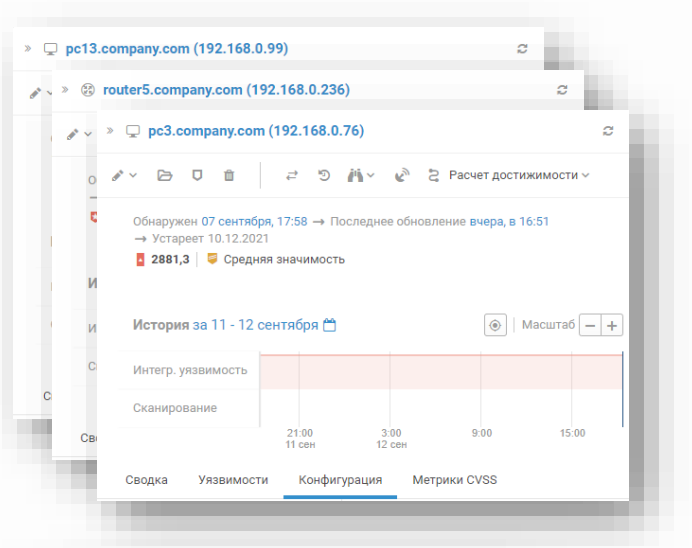
ПОДСКАЗКА:
VulnerPassport.CVEs

УЯЗВИМОСТИ НА АКТИВАХ

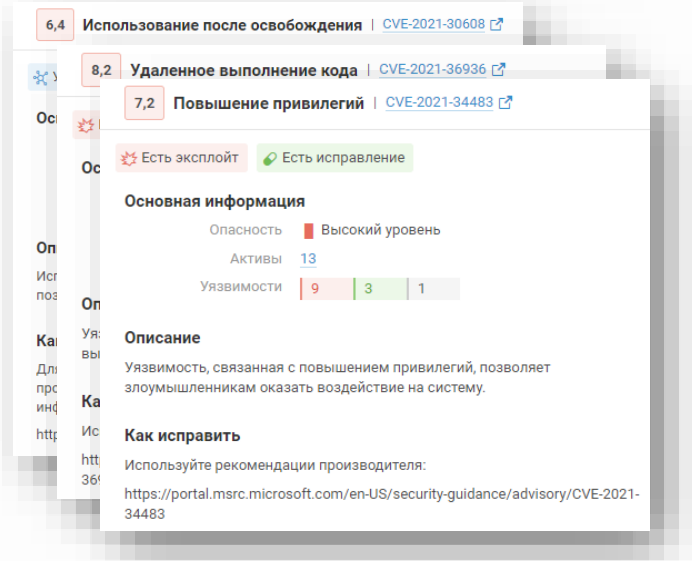
ptsecurity.com

ЭКЗЕМПЛЯРЫ УЯЗВИМОСТЕЙ НА АКТИВАХ

АКТИВЫ



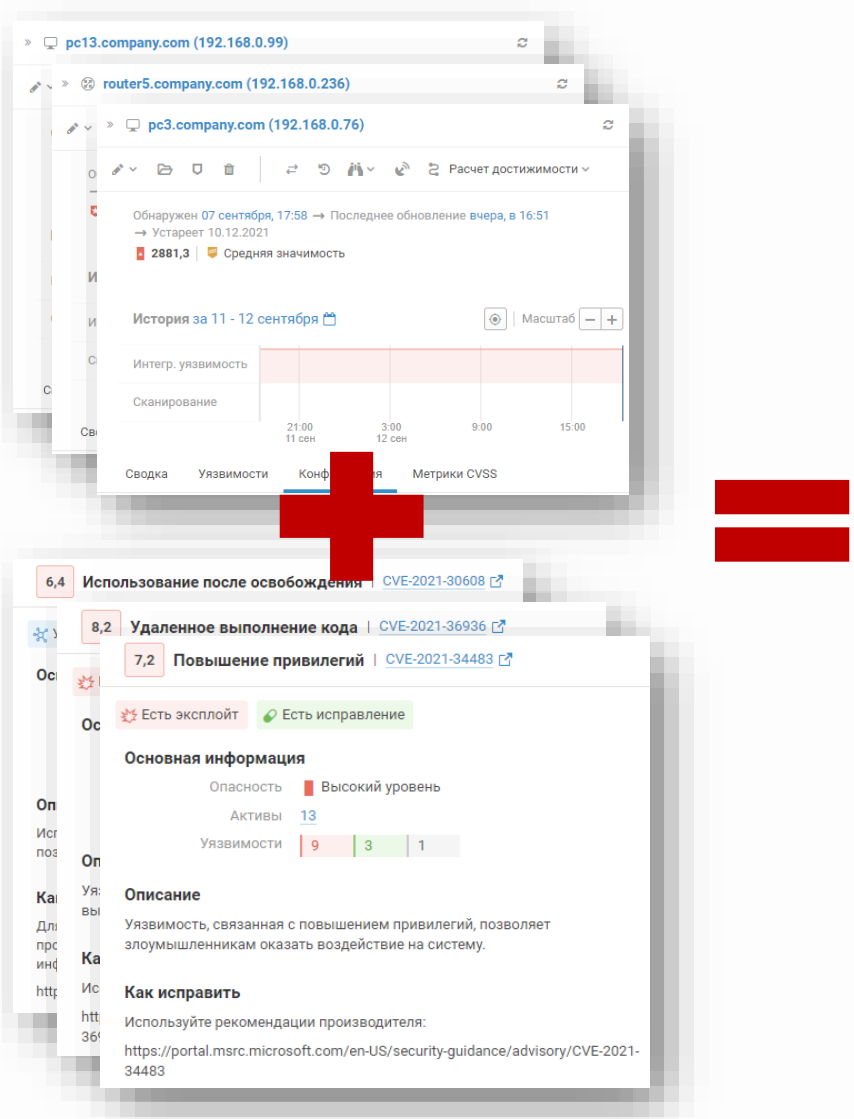
ПАСПОРТА УЯЗВИМОСТЕЙ

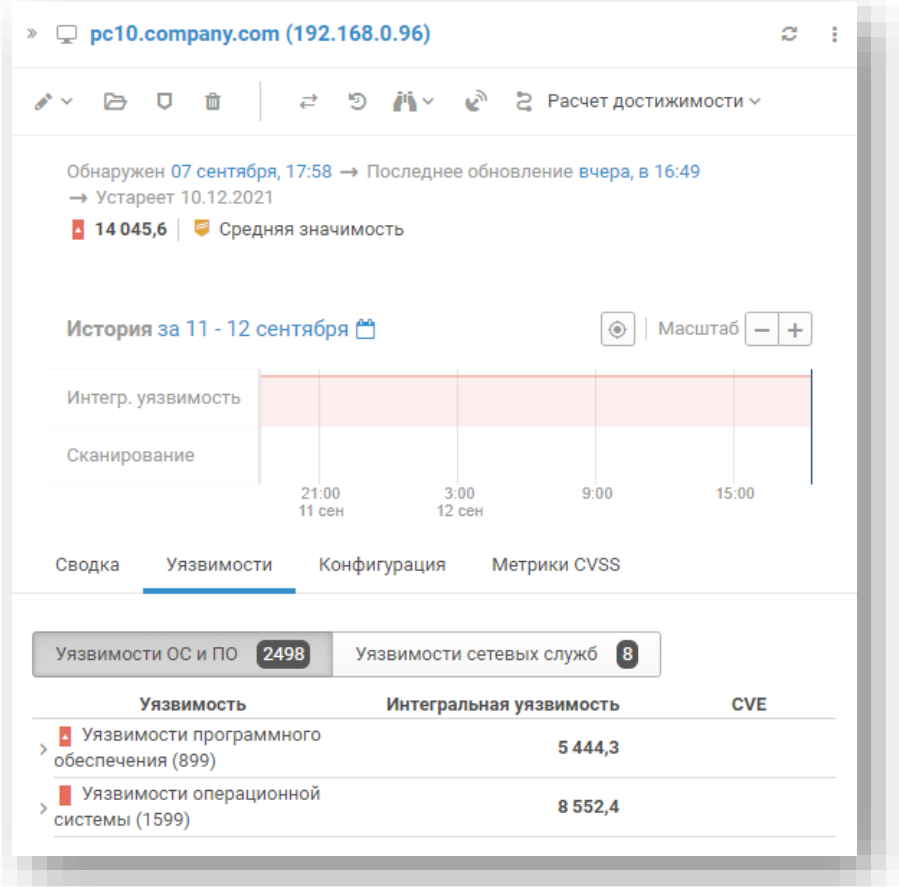


ЭКЗЕМПЛЯРЫ УЯЗВИМОСТЕЙ НА АКТИВАХ

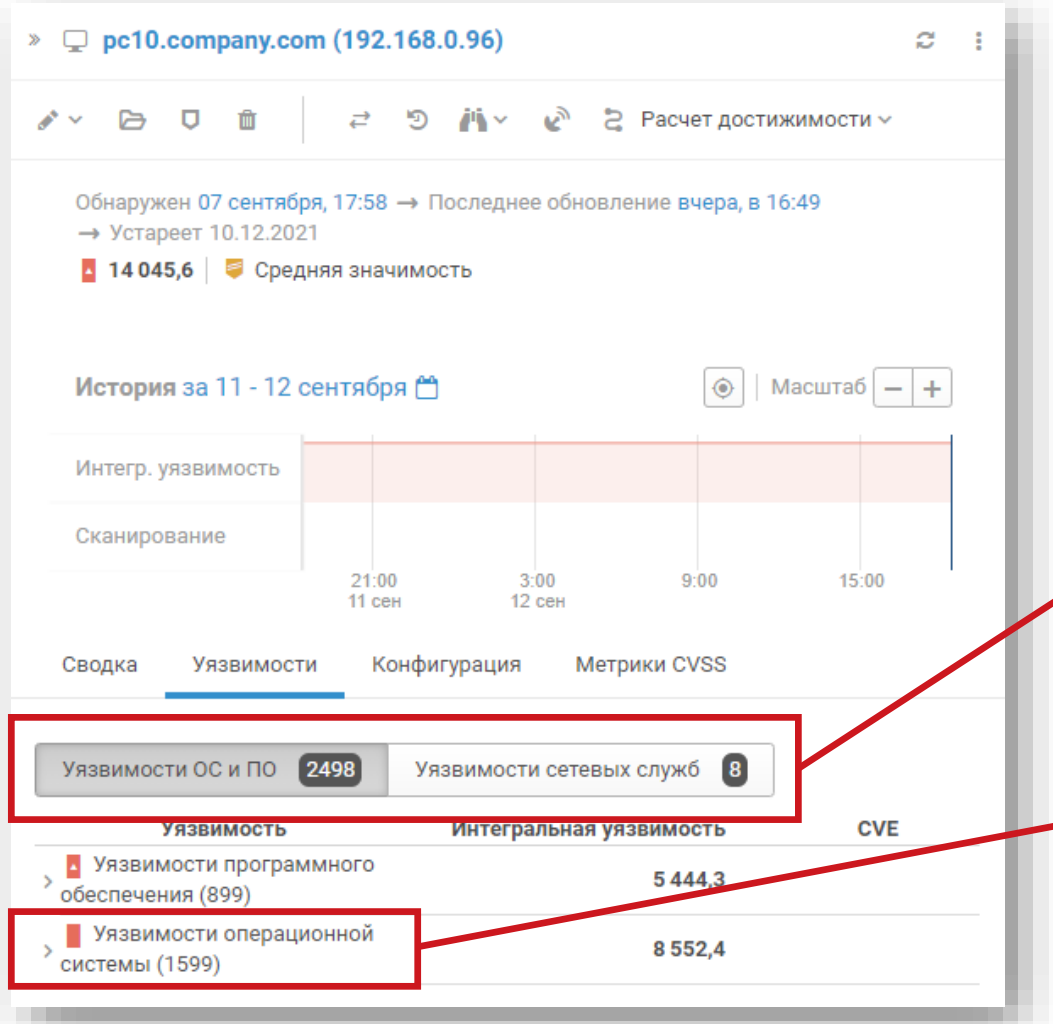
АКТИВЫ

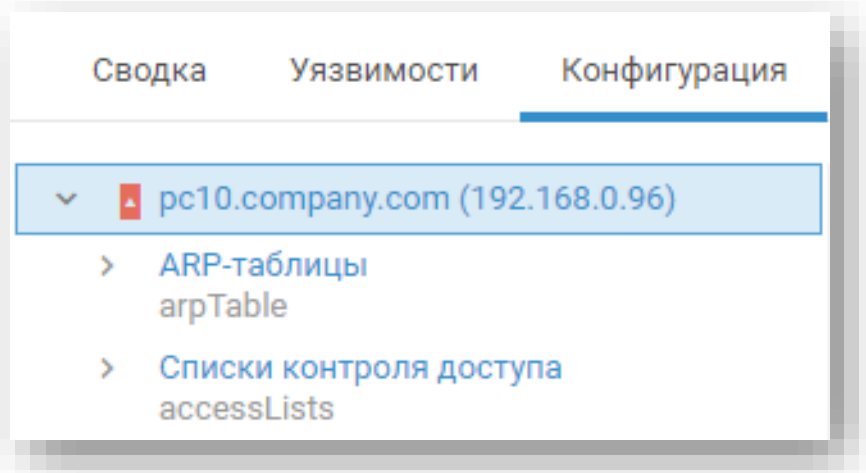
ПАСПОРТА УЯЗВИМОСТЕЙ





УЯЗВИМОСТИ ОС





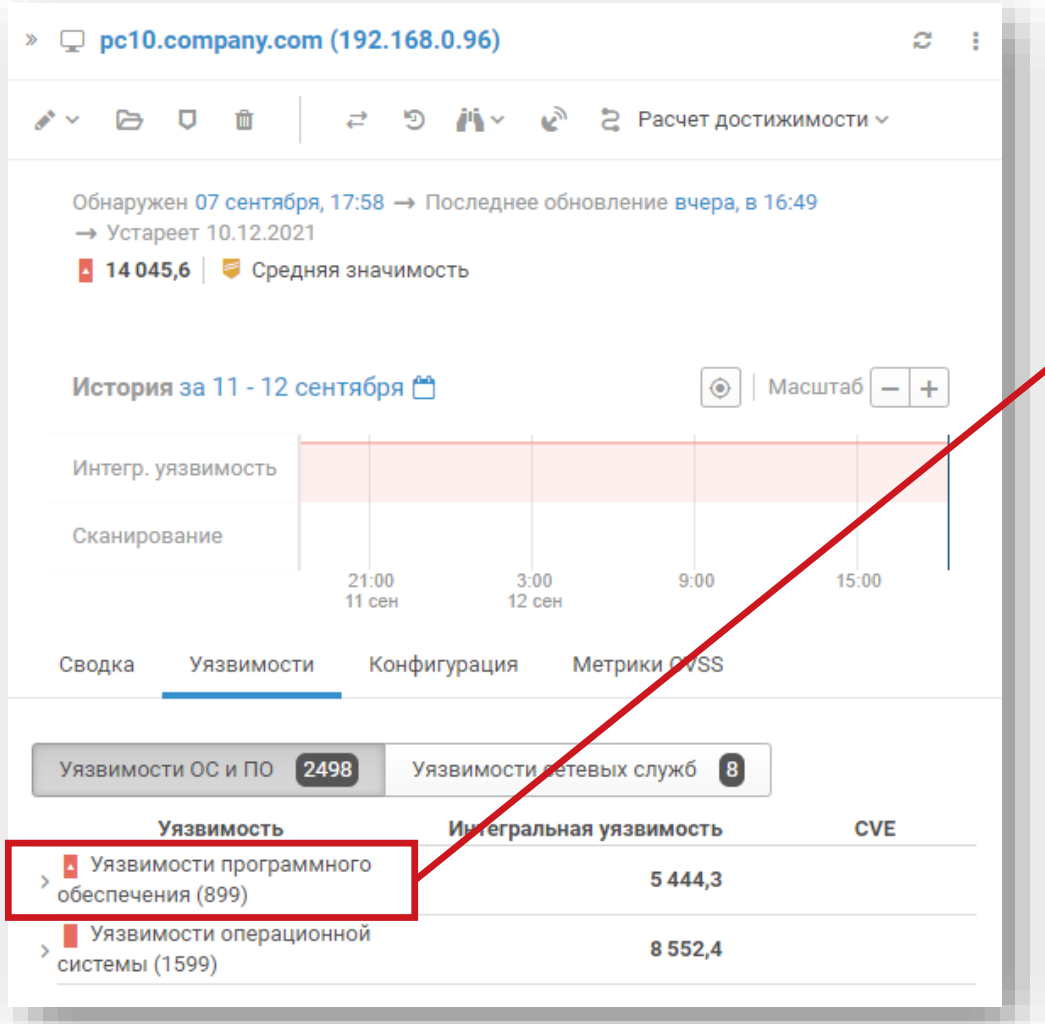
ВСЕ УЯЗВИМОСТИ НА ХОСТЕ:

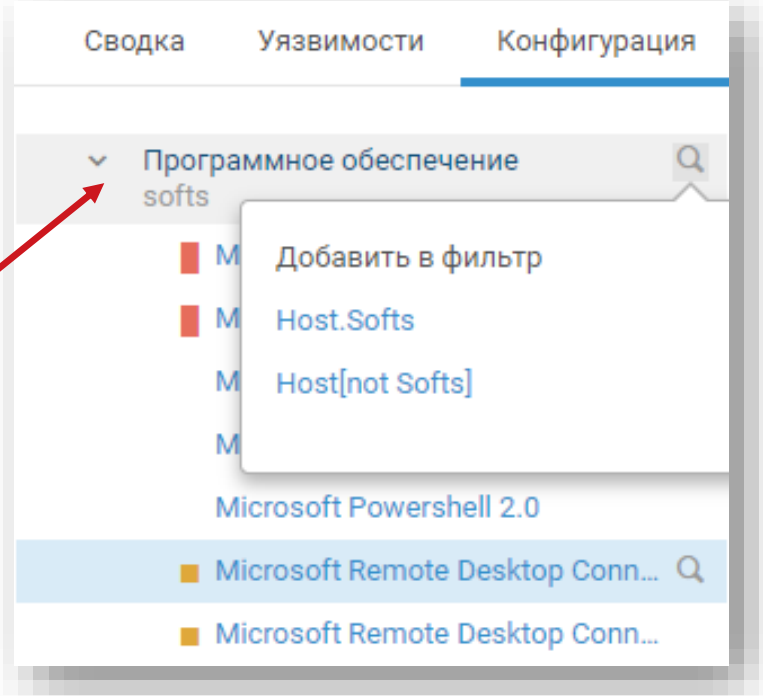
select(@Host,
Host.@**Vulners**)

ТОЛЬКО УЯЗВИМОСТИ ОС:

select(@Host,
Host.@**NodeVulners**)

УЯЗВИМОСТИ ПО





ТОЛЬКО УЯЗВИМОСТИ ПО:

select(@Host,
Host.Softs.@**NodeVulners**)

УЯЗВИМОСТИ LINUX-ПАКЕТОВ

pc10.company.com (192.168.0.96)

Расчет достижимости

Обнаружен 07 сентября, 17:58 → Последнее обновление вчера, в 16:49
→ Устареет 10.12.2021

14 045,6 | Средняя значимость

История за 11 - 12 сентября

Масштаб

Интегр. уязвимость

Сканирование

21:00 11 сен | 3:00 12 сен | 9:00 | 15:00

Сводка | Уязвимости | Конфигурация | Метрики CVSS

Уязвимости ОС и ПО 2498 | Уязвимости сетевых служб 8

Уязвимость	Интегральная уязвимость	CVE
Уязвимости программного обеспечения (899)	5 444,3	
Уязвимости операционной системы (1599)	8 552,4	

Сводка | Уязвимости | Конфигурация

Пакеты
packages

Добавить в фильтр
UnixHost.Packages
UnixHost[not Packages]

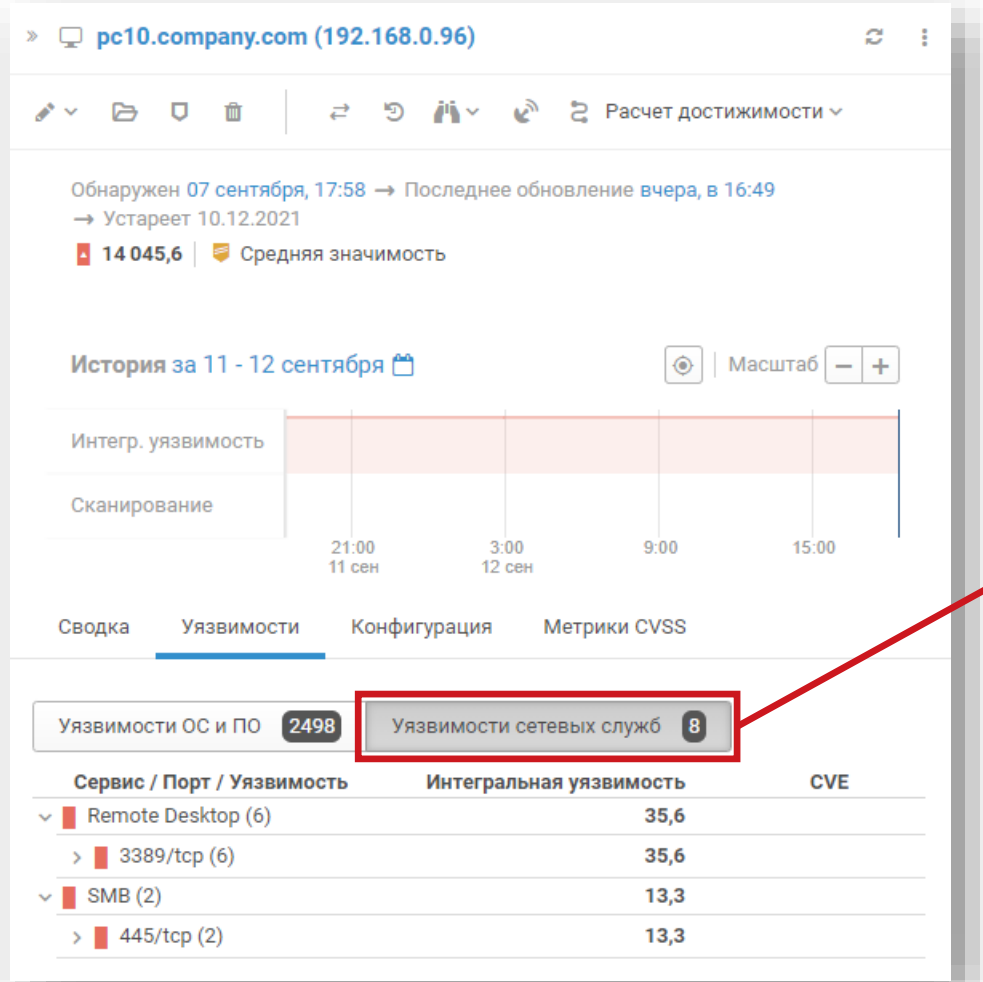
apt-transport-https (1.4.9)

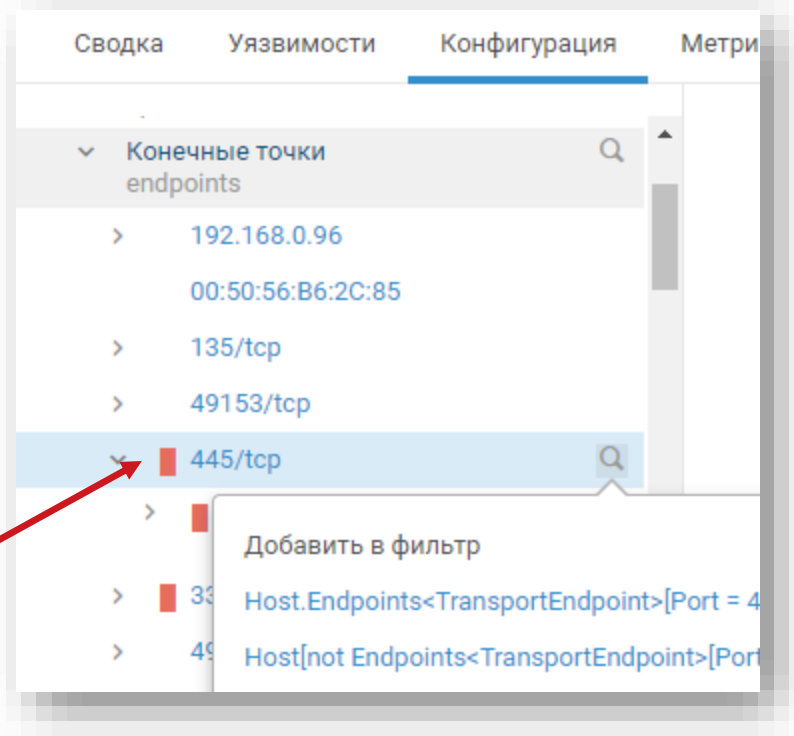
apt-utils (1.4.9)

ТОЛЬКО УЯЗВИМОСТИ LINUX ПАКЕТОВ:

select(@UnixHost,
UnixHost.Packages.@**NodeVulners**)

УЯЗВИМОСТИ СЕТЕВЫХ СЛУЖБ





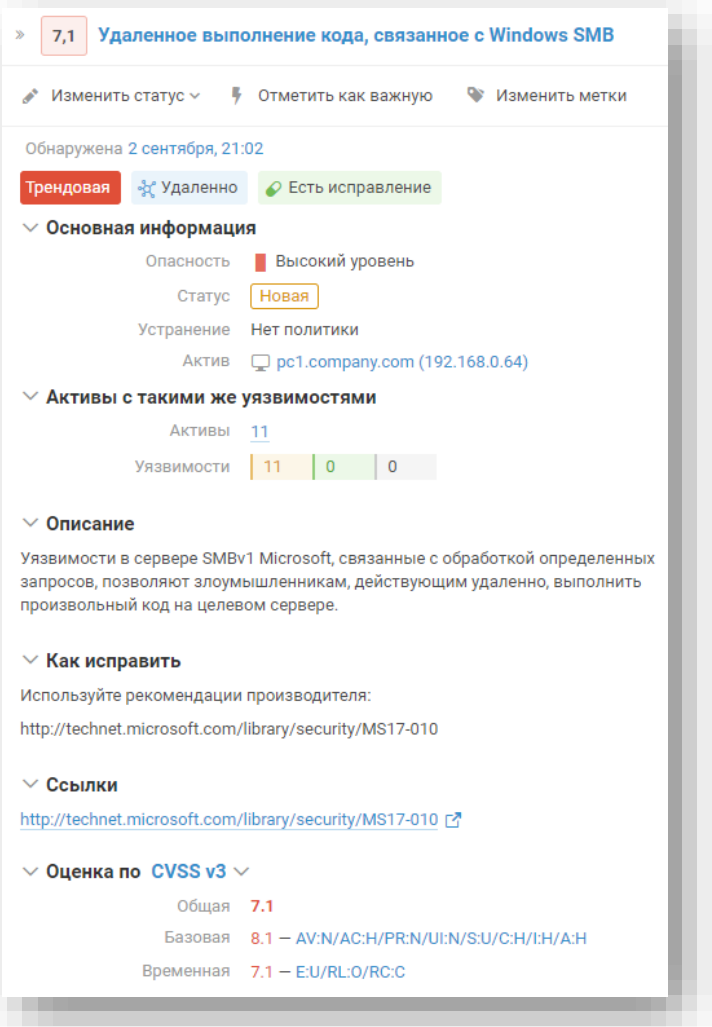
ТОЛЬКО УЯЗВИМОСТИ СЕТЕВЫХ СЛУЖБ:

select(@Host,
Host.Endpoints<TransportEndpoint>.@**Vulners**)

PDQL: Экземпляры уязвимостей на активах

» **@Vulners**
@NodeVulners

```
select(@Host,
        Host.@Vulners,
        Host.@Vulners.DiscoveryTime,
        Host.@Vulners.Status,
        Host.@Vulners.FixType,
        Host.@Vulners.DueTime,
        Host.@Vulners.LastFixTime,
        Host.@Vulners.IsDanger,
        Host.@Vulners.Tags)
```



PDQL: Экземпляры уязвимостей на активах

Запрос: Все активы *

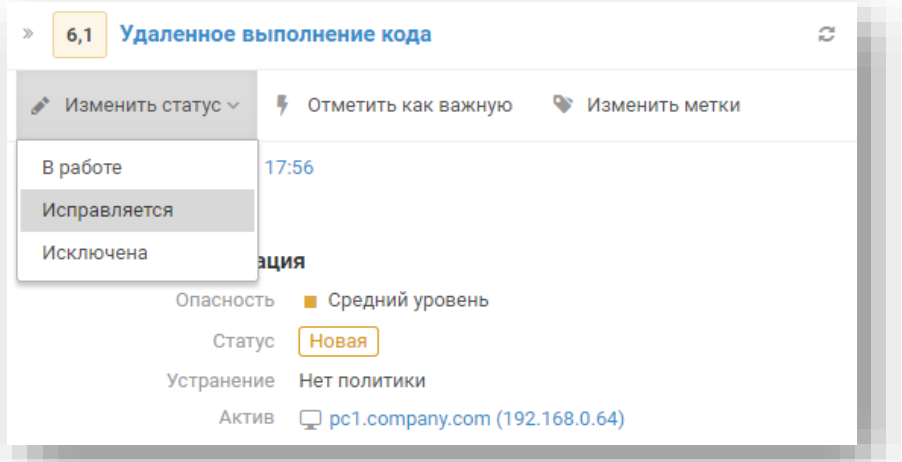
@Host, Host.@Vulners, Host.@Vulners.D… | Host.@Vulners.DiscoveryTime DESC | Выполнить

Узел @Host	Уязвимость Host.@Vulners	Дата и время обнар… Host.@Vulners.Disco…	Статус уязв… Host.@Vuln…	Устранение Host.@Vulners.F…	Важная Host.@…	Метки уязвимости Host.@Vulners.Tags
srv13.company.com (192.168.2.8)	Повышение привилегий	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Разглашение информации	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Переполнение буфера, связанное с библиотекой PDF Microsoft	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Повышение привилегий	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Повышение привилегий	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Повышение привилегий, связанное с диспетчером печати	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Удаленное выполнение кода	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Удаленное выполнение кода	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Удаленное выполнение кода	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Повышение привилегий	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Повышение привилегий	02 сентября, 21:05	Новая	Нет политики	False	null
srv13.company.com (192.168.2.8)	Повышение привилегий	02 сентября, 21:05	Новая	Нет политики	False	null

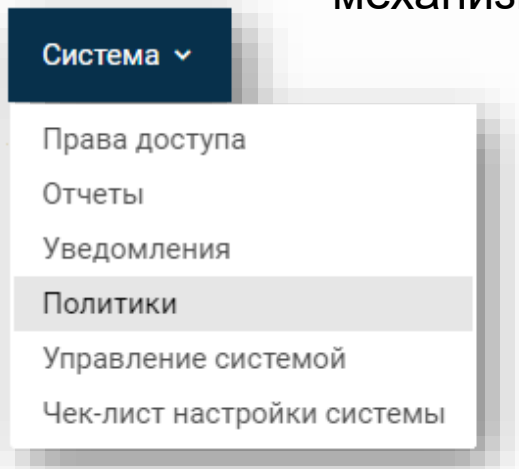
PDQL В ПОЛИТИКАХ

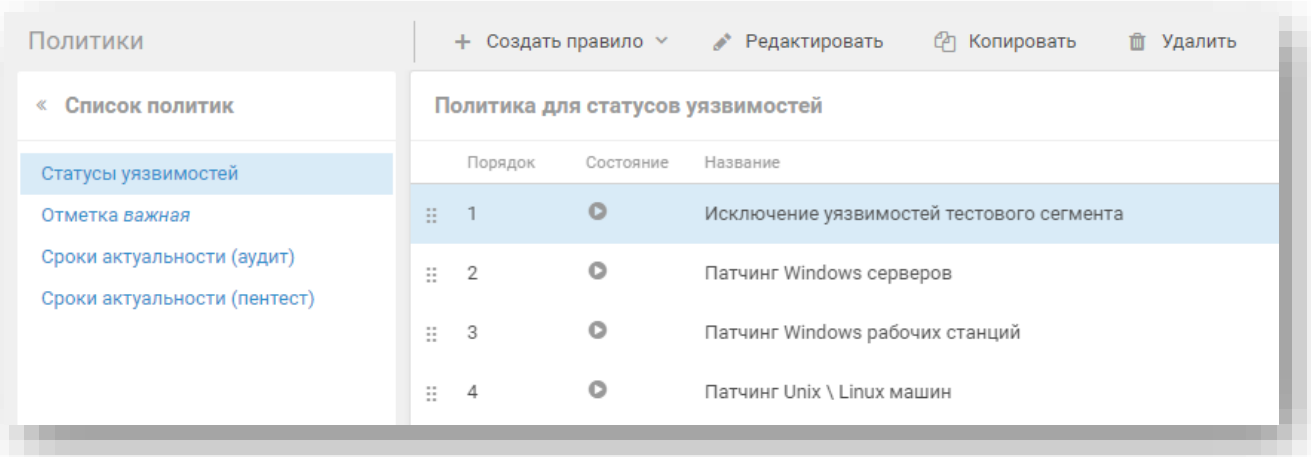
СТАТУСЫ УЯЗВИМОСТЕЙ

Ручная настройка в экземпляре уязвимости

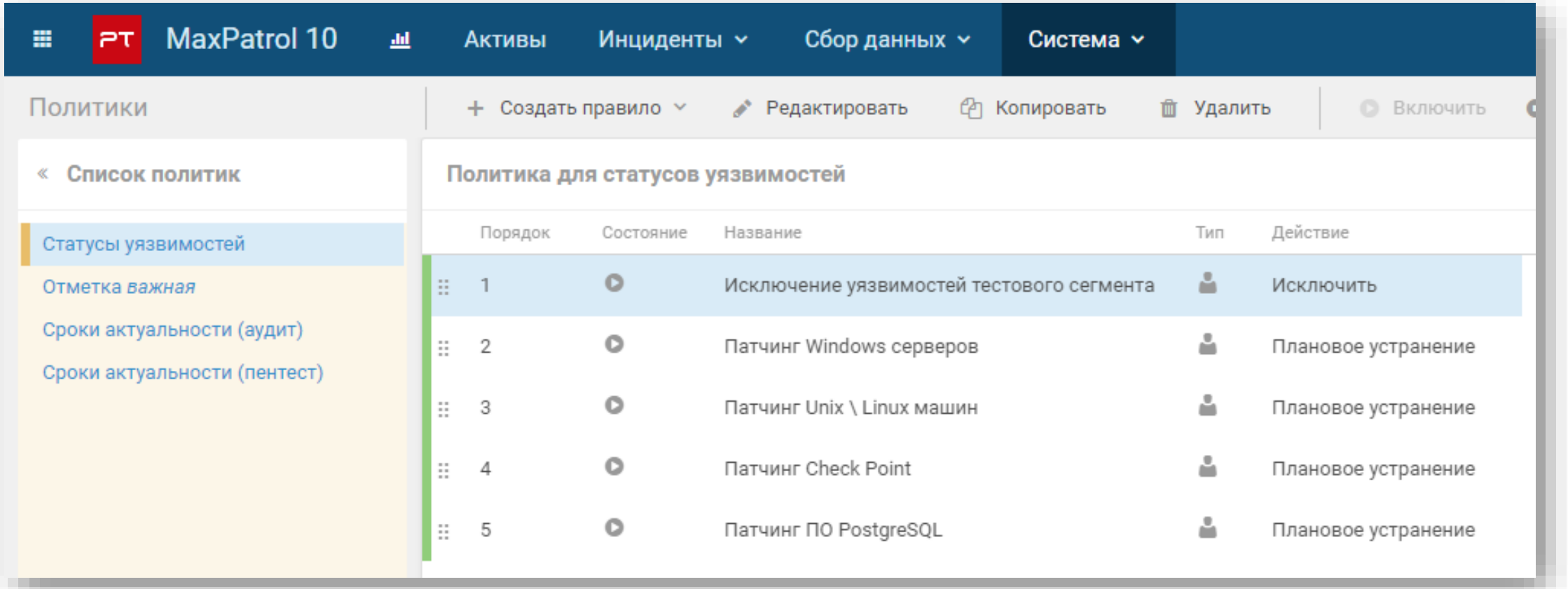


Автоматизация через механизм политик





СОЗДАЕМ ПОЛИТИКИ СТАТУСОВ УЯЗВИМОСТЕЙ



ПОЛЬЗА PDQL

ptsecurity.com

ПОЛЬЗА PDQL

01. Категоризирует и структурирует активы сети

02. Помогает находить интересное в ваших активах

03. Автоматизирует работу с уязвимостями

04. Помогает настроить системы под себя

POSITIVE TECHNOLOGIES

Портал техподдержки
support.ptsecurity.com

Отдел продаж:
sales@ptsecurity.com

Телеграм-канал о новостях продуктов Positive Technologies.

t.me/ptproductupdate

Задать вопрос о функционале MaxPatrol 10:

t.me/MPSIEMChat