
MaxPatrol VM
Не даст хакерам шанса использовать
уязвимости для взлома

Познакомимся

Олег Кочетов

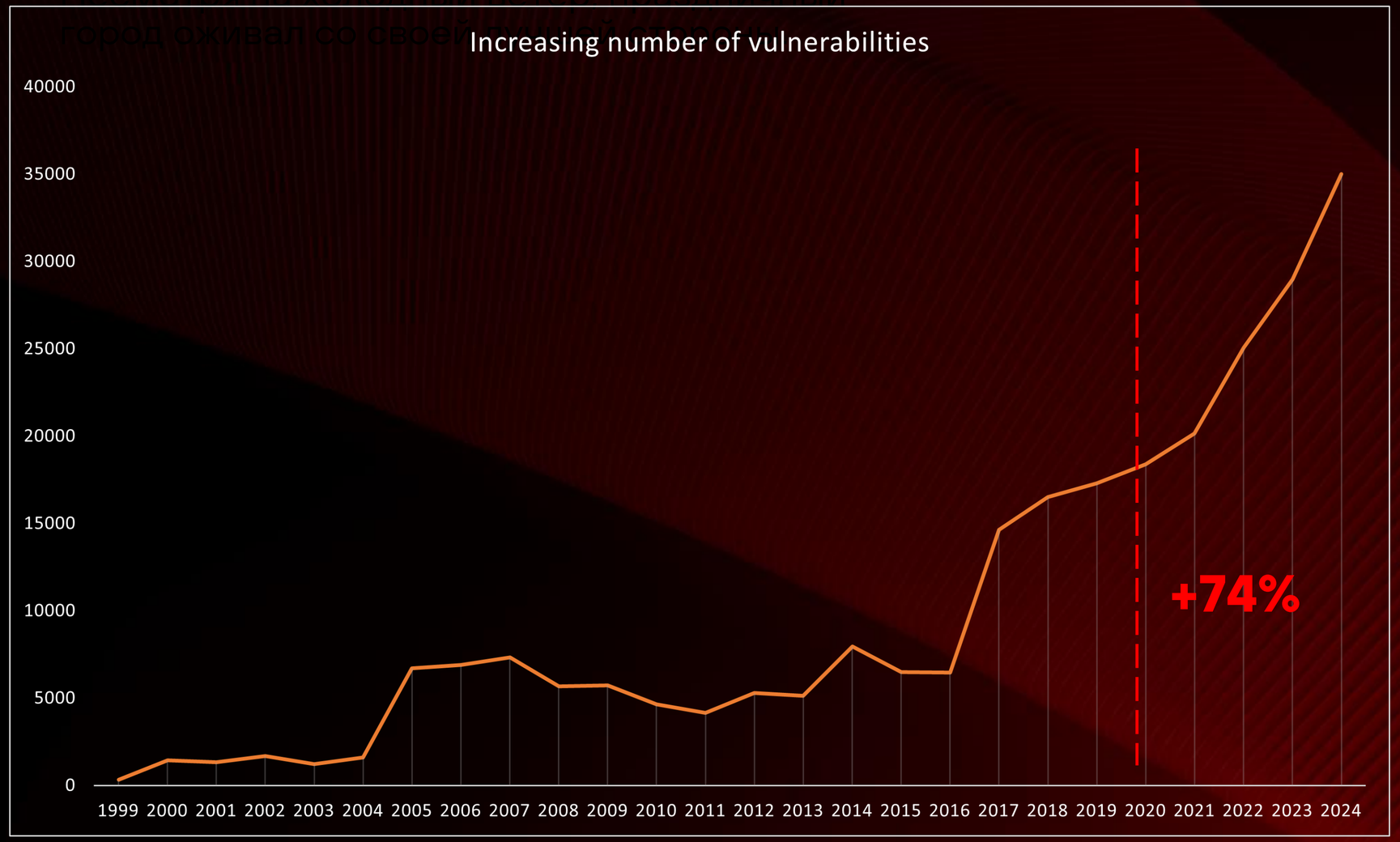
Лидер продуктовой практики
MaxPatrol VM, MaxPatrol HCC

okochetov@ptsecurity.com
+7 905 783 90 46
@Bednight

Эксперт по построению результативного процесса управления уязвимостями

Более 6 лет занимался построением и развитием процесса безопасной разработки в ведущей российской компании

Масштаб проблемы



- 40 077 CVE опубликовано в 2024-м
- 28 961 CVE опубликована в 2023-м
- 25 059 CVE опубликовано в 2022-м
- 20 161 CVE опубликована в 2021-м
- 18 375 CVE опубликовано в 2020-м

Три поколения сканеров

Сетевые сканеры уязвимостей

Сканирование в режиме черного ящика, определение открытых портов

1

XSpider 2002

Системы анализа защищенности

Централизованное сканирование узлов и сетевого оборудования в режиме черного и белого ящика, сравнение результатов

2

MaxPatrol 8 2009

Системы управления уязвимостями нового поколения

Управление активами, построение процесса приоритизации, контроля за устранением уязвимостей

3

MaxPatrol VM 2021

Что мешает работать с уязвимостями

1 Нет полноты охвата IT-инфраструктуры

- Присутствуют задержки в получении актуальных данных о сети
- Нет возможности часто сканировать инфраструктуру
- Ибэшник проверяет только те узлы, о которых знает

2 Уязвимостей слишком много

- Все уязвимости закрыть невозможно
- Нет понимания, какие уязвимости наиболее опасны для конкретной инфраструктуры
- Имеются сложности с приоритизацией задач на устранение уязвимостей

3 Нужно договариваться с IT-отделом

- В компании отсутствует плановый патч-менеджмент
- Необходимо каждый раз объяснять IT-специалистам, зачем нужно устранять конкретную уязвимость
- Нет возможности контролировать статус и сроки устранения уязвимостей

Что предлагает MaxPatrol VM

1 **Нет полноты охвата IT-инфраструктуры**

2 **Уязвимостей слишком много**

3 **Нужно договариваться с IT-отделом**

Технология Asset Management

собирает более 3000 параметров IT-активов и позволяет провести полную инвентаризацию инфраструктуры

Контроль уязвимостей

с учетом отечественного ПО и ОС, выявление уязвимостей в Docker-контейнерах. Отчеты экспертов Positive Technologies известны за пределами России

Процесс управления

уязвимостями позволяет учитывать значимость активов, опасность уязвимостей, а также обрабатывать их в соответствии с регламентом

MaxPatrol VM

Архитектура MaxPatrol VM

Как MaxPatrol VM собирает данные

MaxPatrol VM

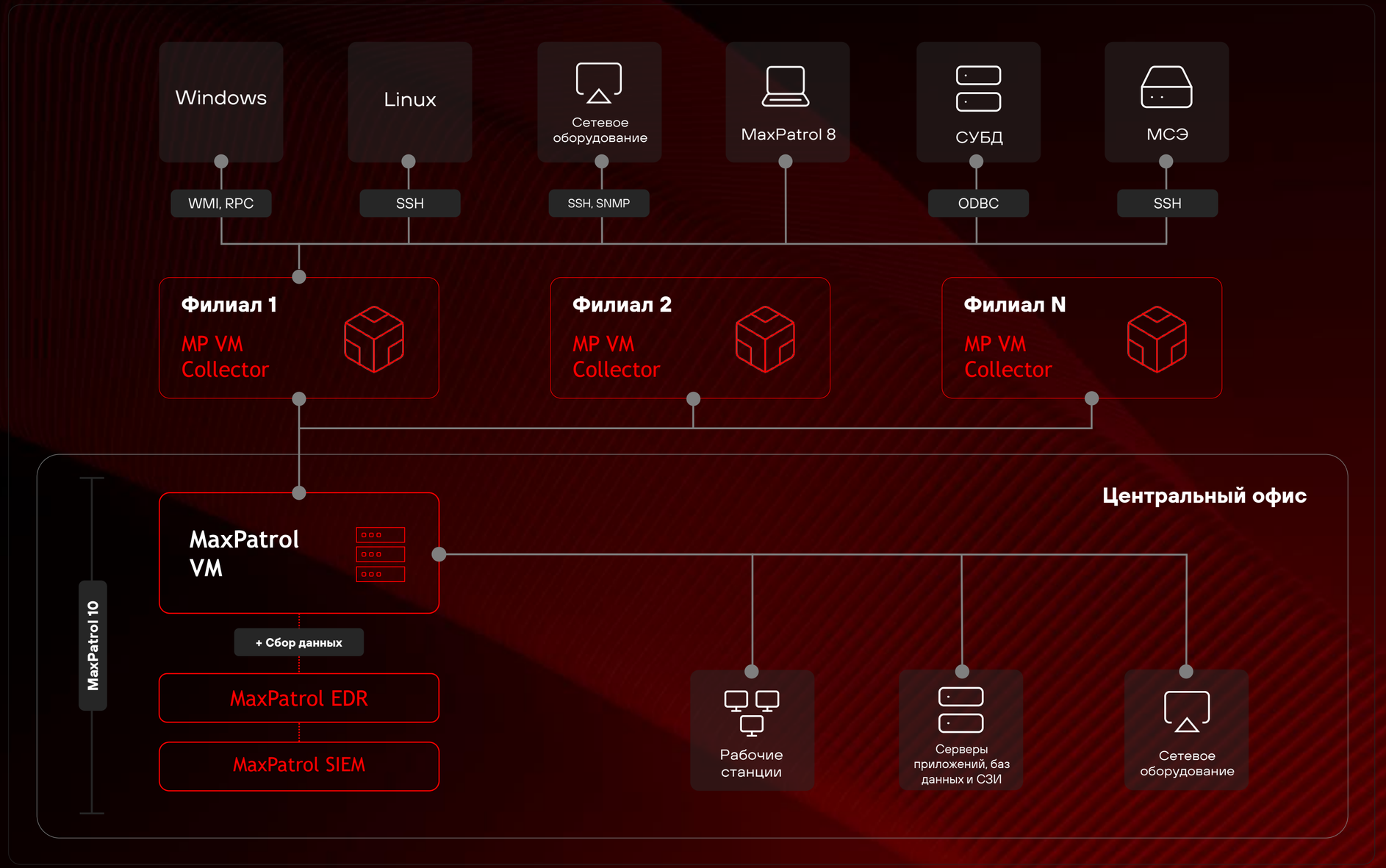
Позволяет сканировать узлы, расположенные в отдельных сетевых сегментах

Коллектор

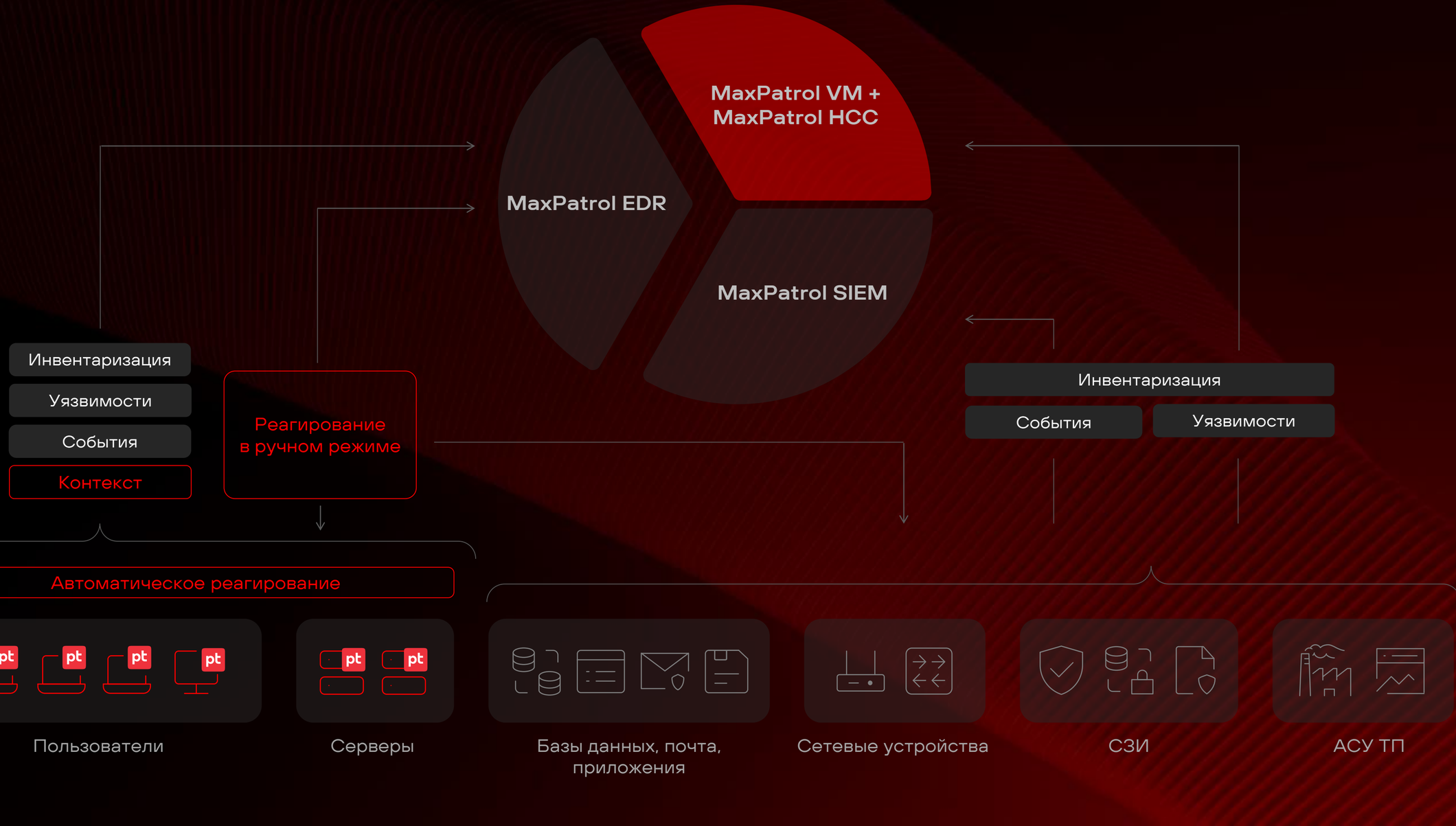
- Собирает и хранит более 3000 параметров активов
- Использует безагентский режим сканирования

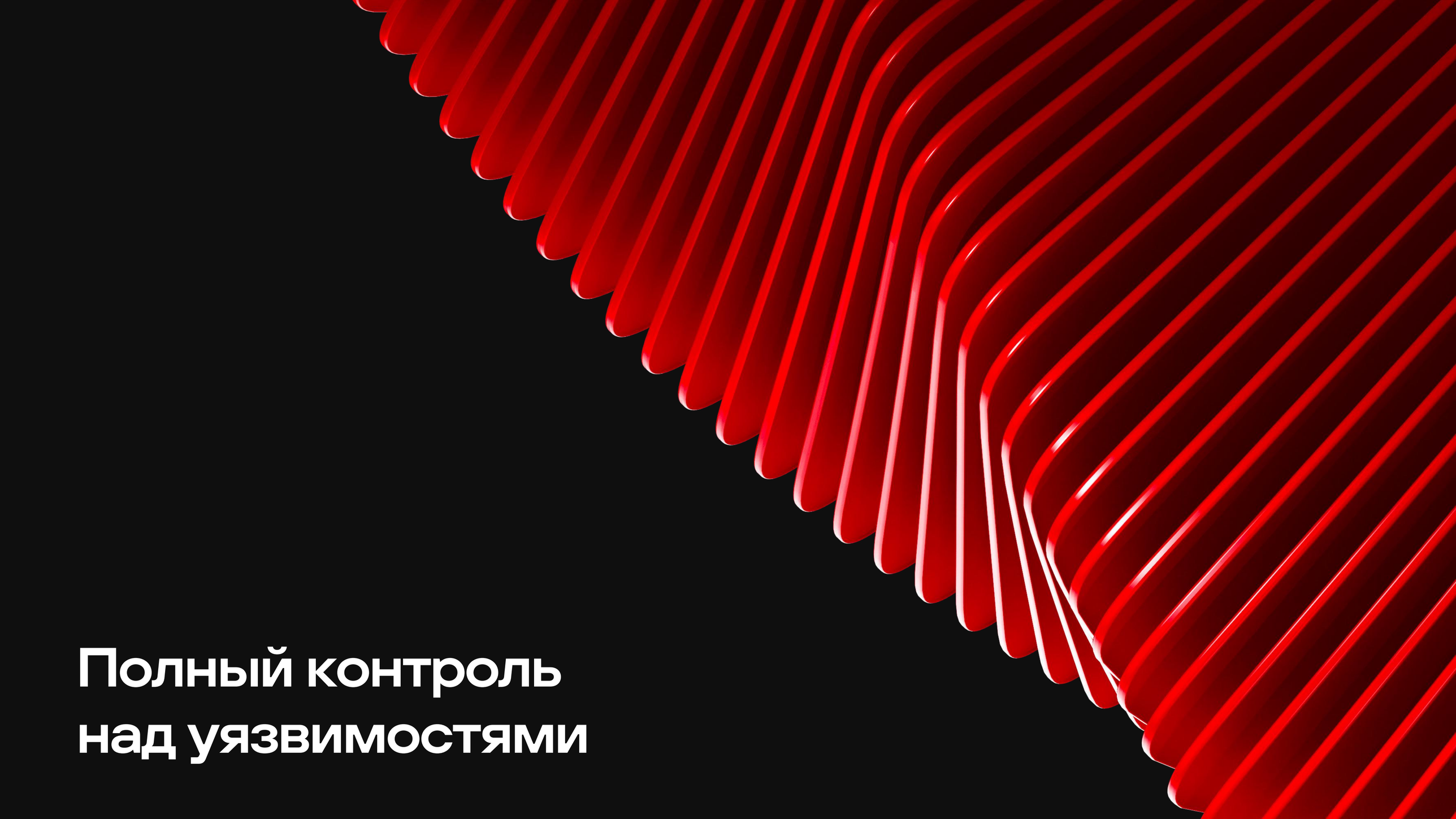
Агентский сбор

Позволяет использовать MaxPatrol EDR для задач сканирования, а также удаленного управления



MaxPatrol SIEM + MaxPatrol EDR + MaxPatrol VM




Полный контроль
над уязвимостями

Обнаружение активов

Классификация и оценка активов

Распределение активов по группам

- По принадлежности к структурным подразделениям
- По принадлежности к АС
- По принадлежности к IP-сетям
- По наличию определенных ОС и ПО

Классификация активов

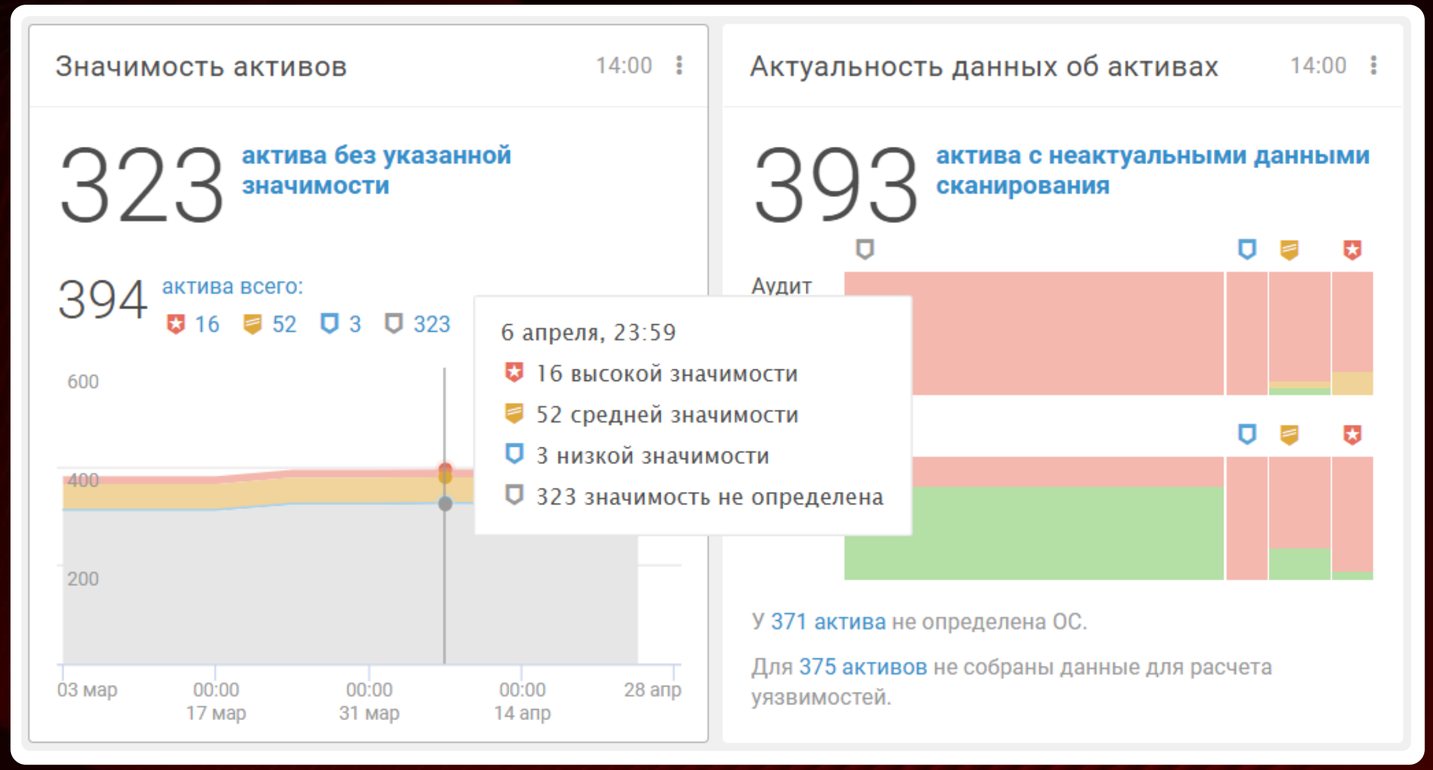
- Динамические группы
- Статические группы
- Триггеры для контроля изменений состава групп

Контроль активов

- Классификация, оценка, регулярное сканирование
- Проверка устаревания

Оценка активов

- Задание степени значимости



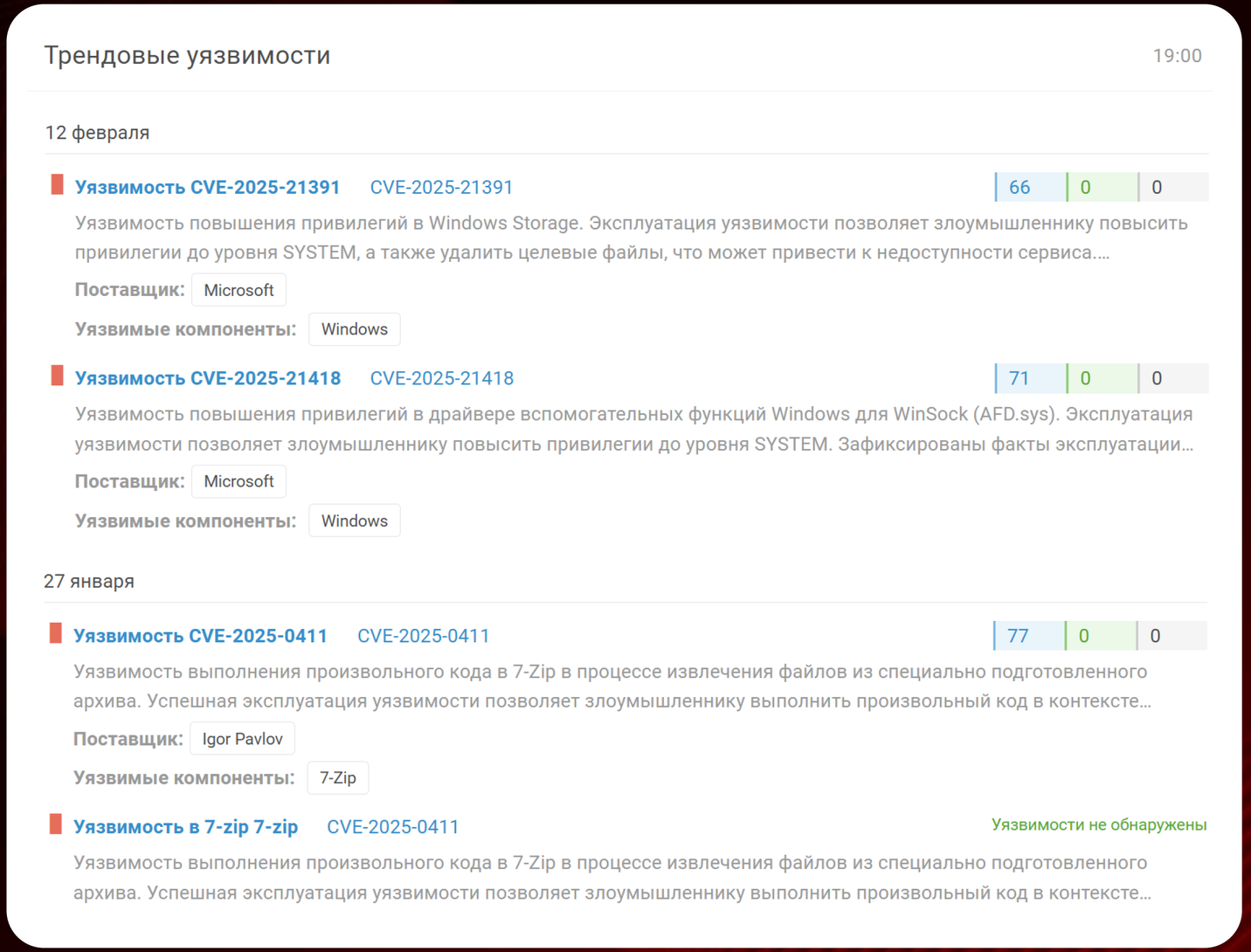
Трендовые уязвимости

Критерии трендовости

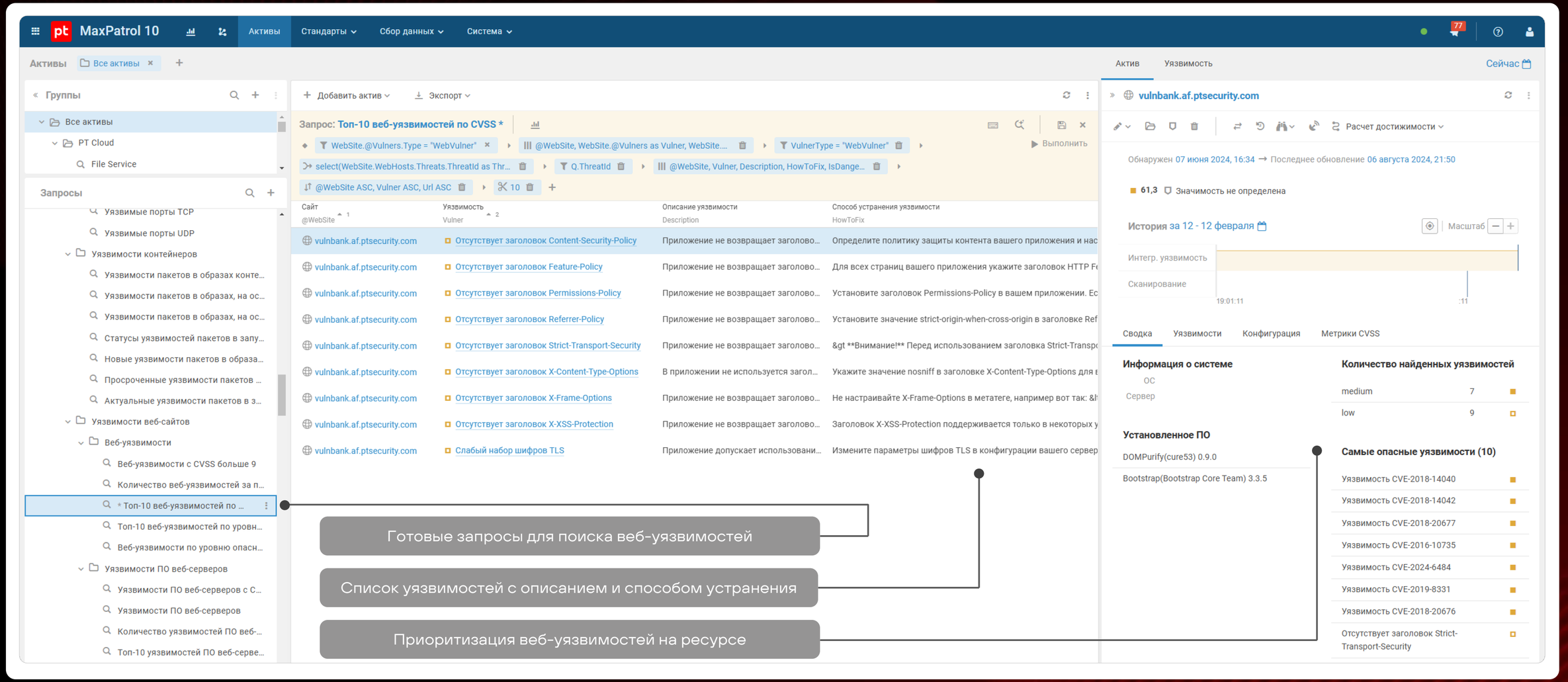
- Наличие эксплойта для уязвимости
- Популярное ПО для России
- CVSS 3.1 выше 7 баллов (высокая опасность)

Информация о трендовых уязвимостях поступает в MaxPatrol VM в течение 12 часов

Исследовательский центр Positive Technologies



Уязвимости в веб-приложениях



ERP- и CRM-системы

Средства разработки и деплоя

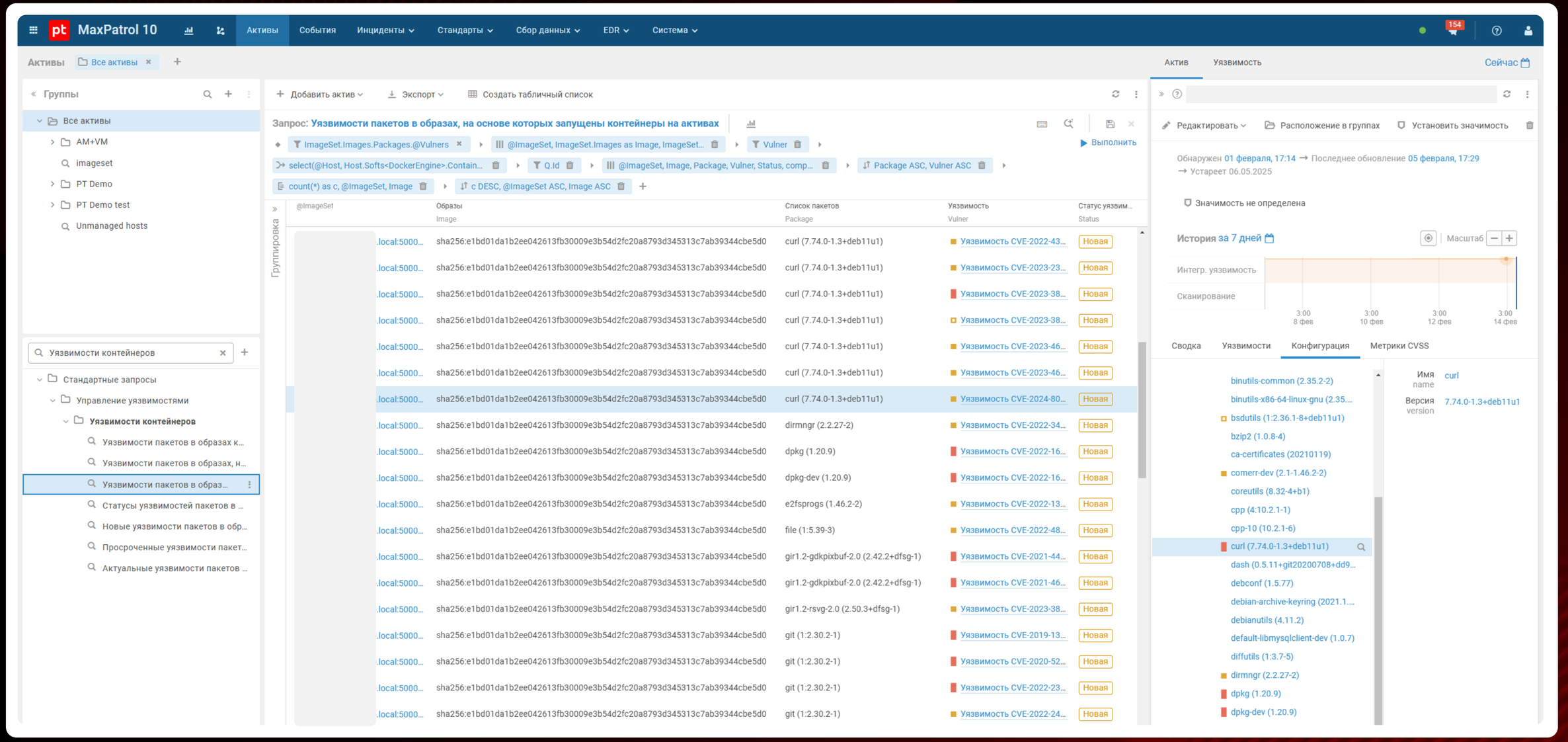
Веб-инструменты для совместной работы

Корпоративные веб-порталы

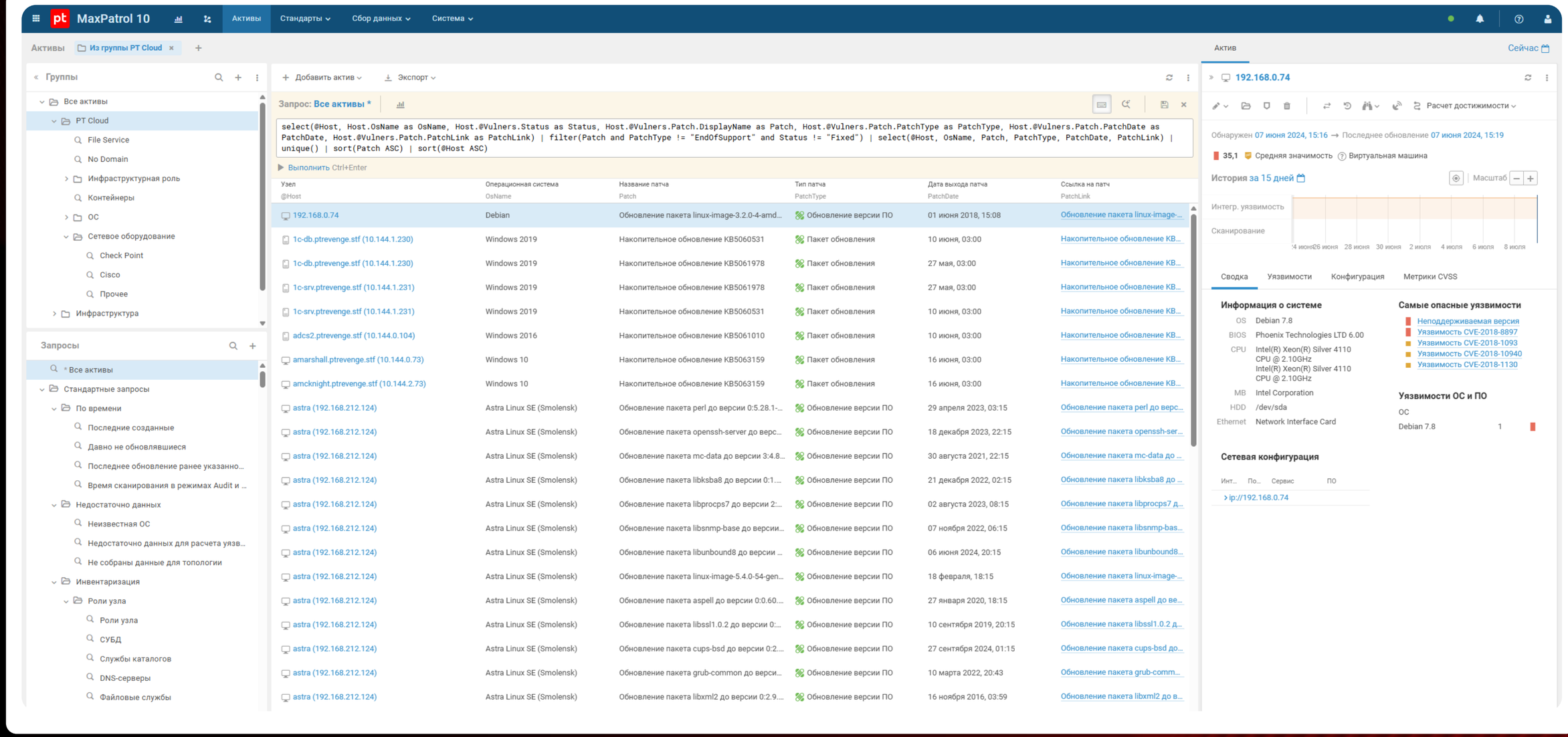
Онлайн-магазины

Одностраничные сайты

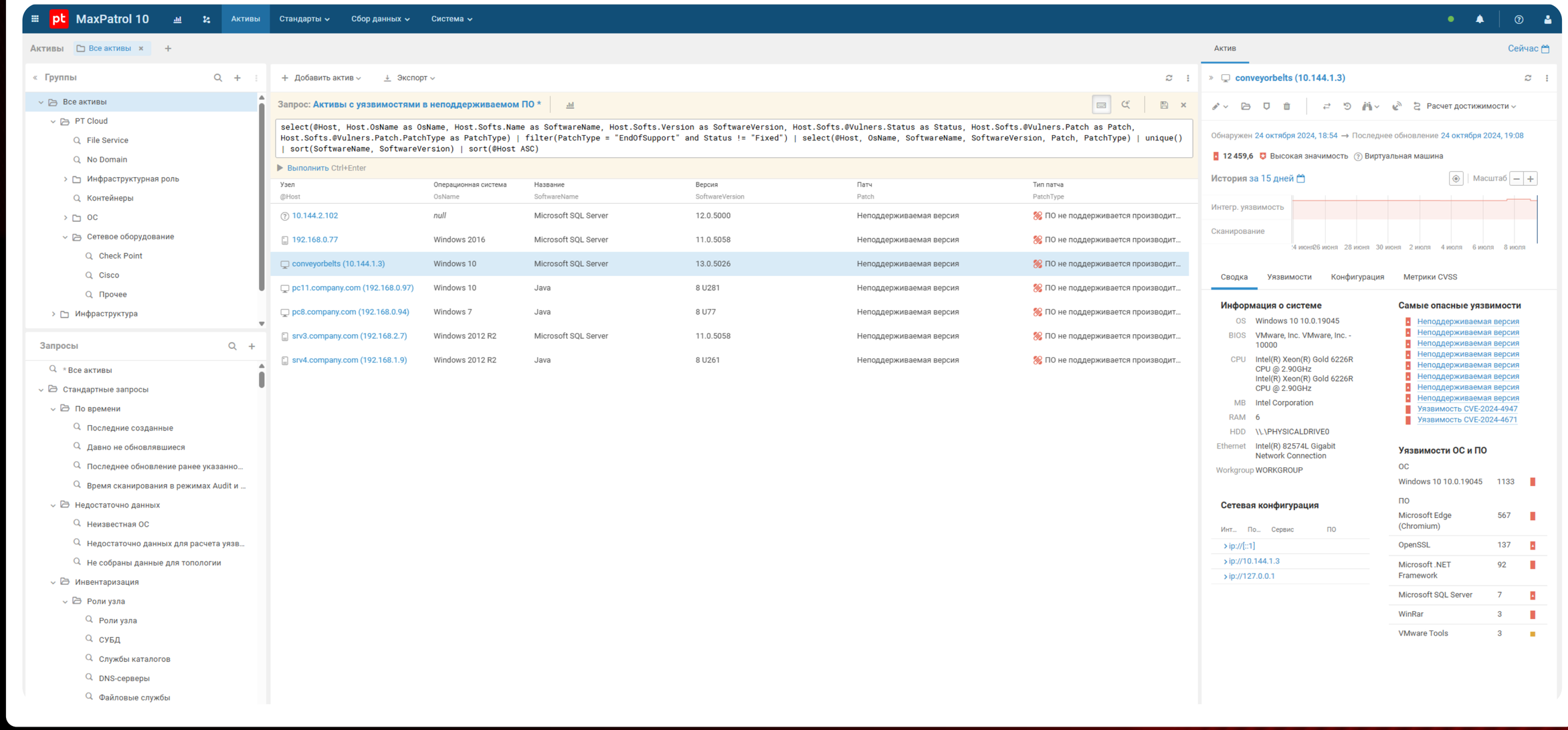
Уязвимости в Docker-контейнерах



Ссылки на патчи безопасности



EOL, EOS — конец срока поддержки ПО

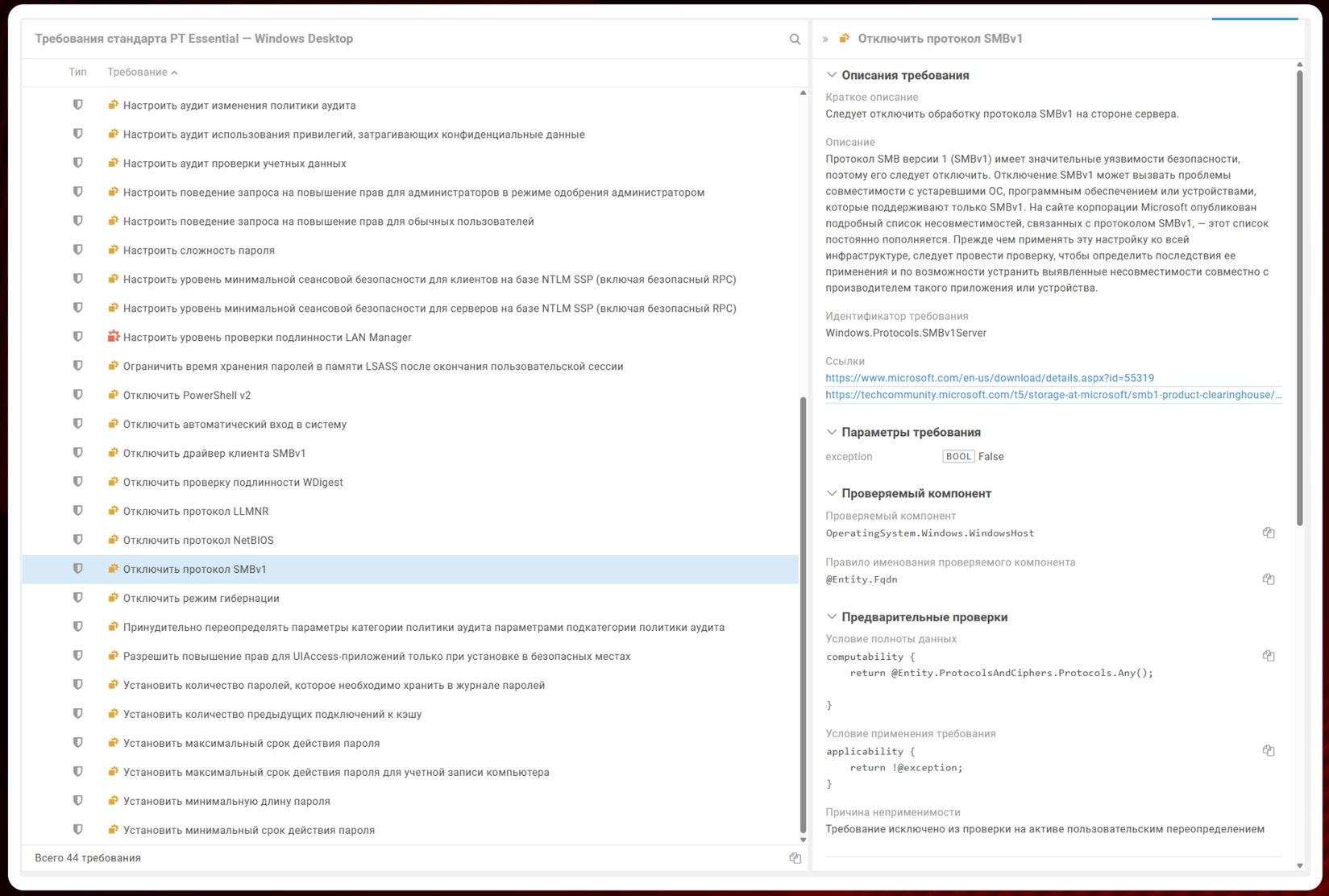


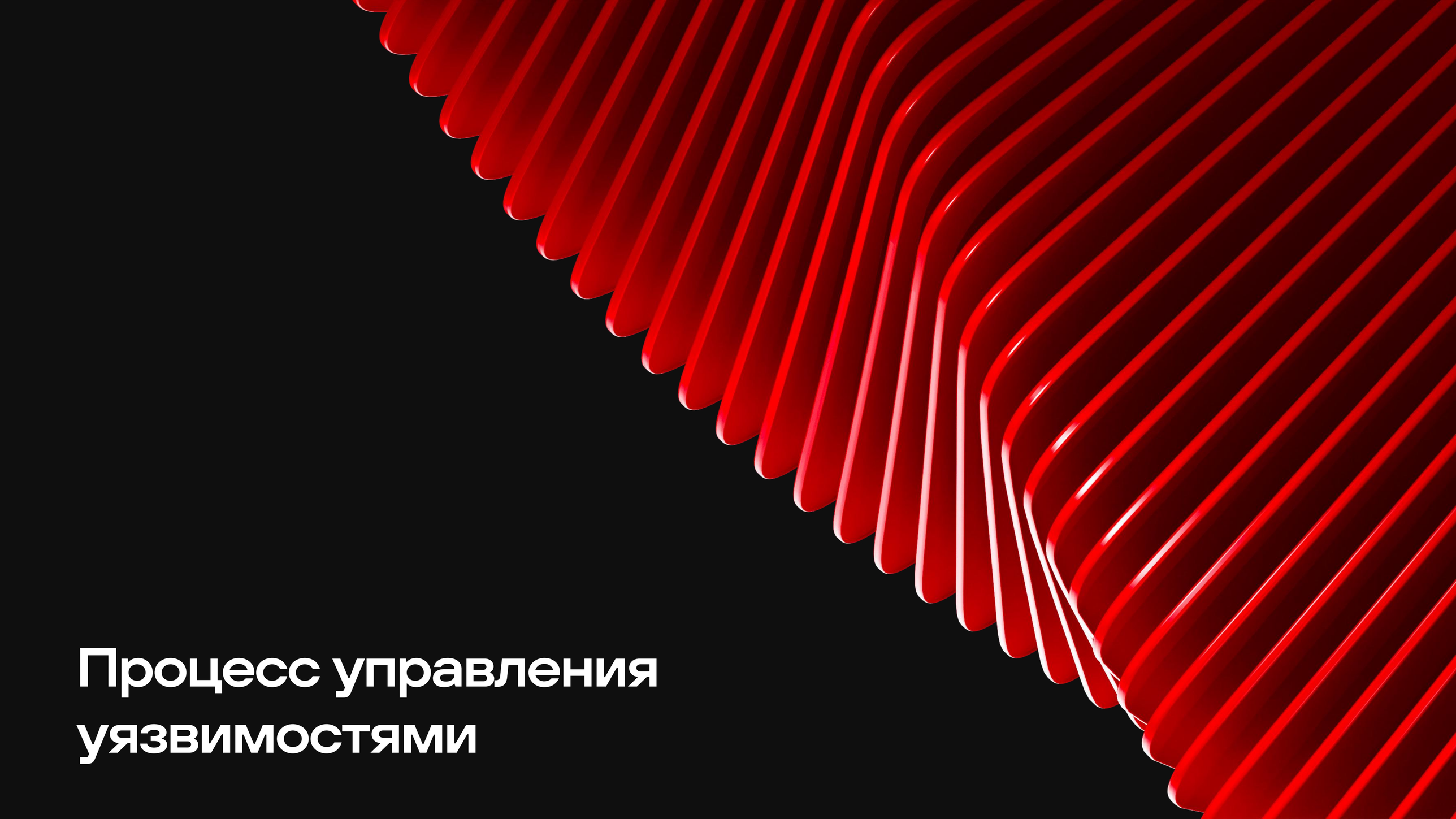
Host compliance control

MaxPatrol HCC — комплаенс для результативной безопасности

Модуль позволяет:

- Проверять инфраструктуру на соответствие стандартам безопасности и отдельным требованиям
- Приоритизировать найденные риски
- Просматривать актуальные данные о выполнении требований на динамических дашбордах
- Устанавливать сроки, в которые несоответствия стандартам должны быть устранены, и контролировать их соблюдение





Процесс управления уязвимостями

Перед тем как начать

Заранее провести предварительные мероприятия

Определить перечень **недопустимых событий**

Распределить **роли** и **функции** среди всех участников процесса

Убедиться, что эти роли есть кому **исполнять**

Согласовать параметры процесса между всеми участниками

Оценить заранее:

- Ресурсы команды
- Технические детали: учетные записи и профили сканирования активов
- SLA и KPI
- Нагрузку на сеть и систему в организации
- Важность источников информации об уязвимостях

Плановая обработка уязвимостей

Два пути обработки уязвимостей

Процесс VM

Плановая обработка уязвимостей

- В IT-отделе принят патч-менеджмент, не зависящий от службы ИБ
- Служба ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с IT-отделом

Особо опасные уязвимости

- Фокус смещается на трендовые уязвимости и на те, что имеют эксплойт и расположены на важных активах
- О сроках устранения каждой уязвимости служба ИБ и IT-отдел договариваются отдельно

Контроль устранения

Статусы уязвимостей

- Исключена
- Новая
- В работе
- Исправляется
- Требуется проверка
- Просрочена
- Устранена

Значимость актива

- Высокая
- Средняя
- Низкая

Плановое устранение

Вчера

Уязвимости с отметкой «важная»

Активы высокой значимос...	Активы средней значимос...
813 −340	0
99	0
110 Н 703 Т	

Остальные уязвимости

Активы высокой значимос...	Активы средней значимос...
31 K −17023	72 −52
52	1
31 K Н	72 Н

Трендовые уязвимости

Вчера

Актуальные

Активы высокой значимос...	Остальные активы
2,3 K +29	0
131	0
114 Н 2,2 K Т 12 И	

Исправленные

Исключенные	Устраненные
0 −8	3,7 K
0	73
И	У

Важная

Уязвимости можно автоматически присваивать отметку «Важная» в зависимости от критериев (например, наличие эксплойта) или актива, на котором она была обнаружена

Отчетность

Уязвимость CVE-2024-20359 CVE-2024-20359 Cisco Cisco ASA

Есть эксплойт | Можно исправить | 1 | 0 | 0

Уязвимость микропрограммного обеспечения межсетевых экранов Cisco Adaptive Security Appliance (ASA) и Cisco Firepower Threat Defense (FTD) связана с неверным управлением генерацией кода. Эксплуатация уязвимости может позволить нарушителю выполнить произвольный код с привилегиями root с помощью специально созданного файла

Дата публикации
24 апреля 2024, 00:00

Как исправить
Использование рекомендаций производителя: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h

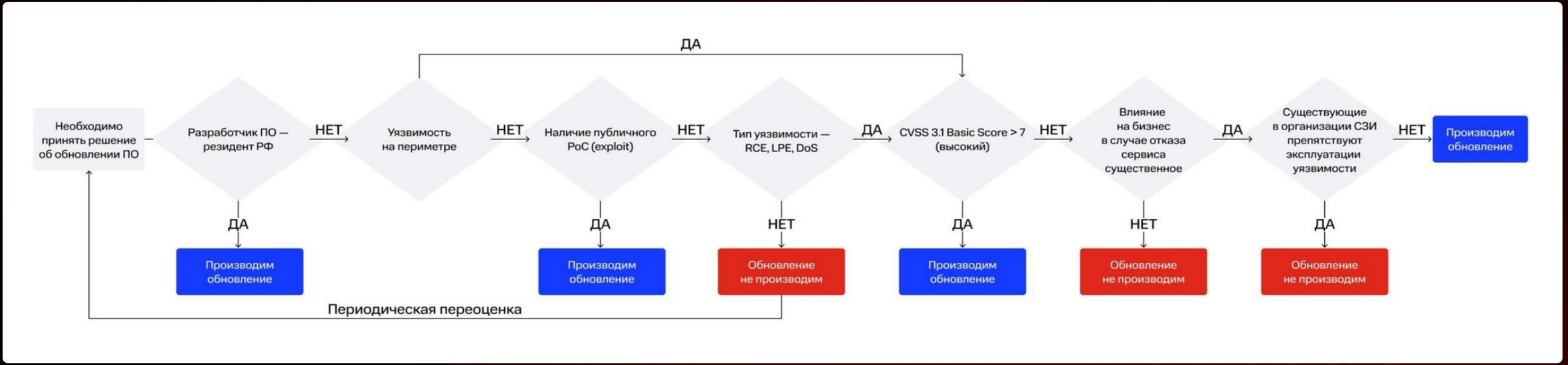
Ссылки
https://bdu.fstec.ru/vul/2024-03264
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-rce-FLsNXF4h
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Статус	Уязвимость на активе	Обнаружена
Новая	fw10.company.com (192.168.0.231) Устранение: Нет политики Cisco Cisco ASA 9.12(3)12	6 сен 2024, 05:33

Другие возможности MaxPatrol VM

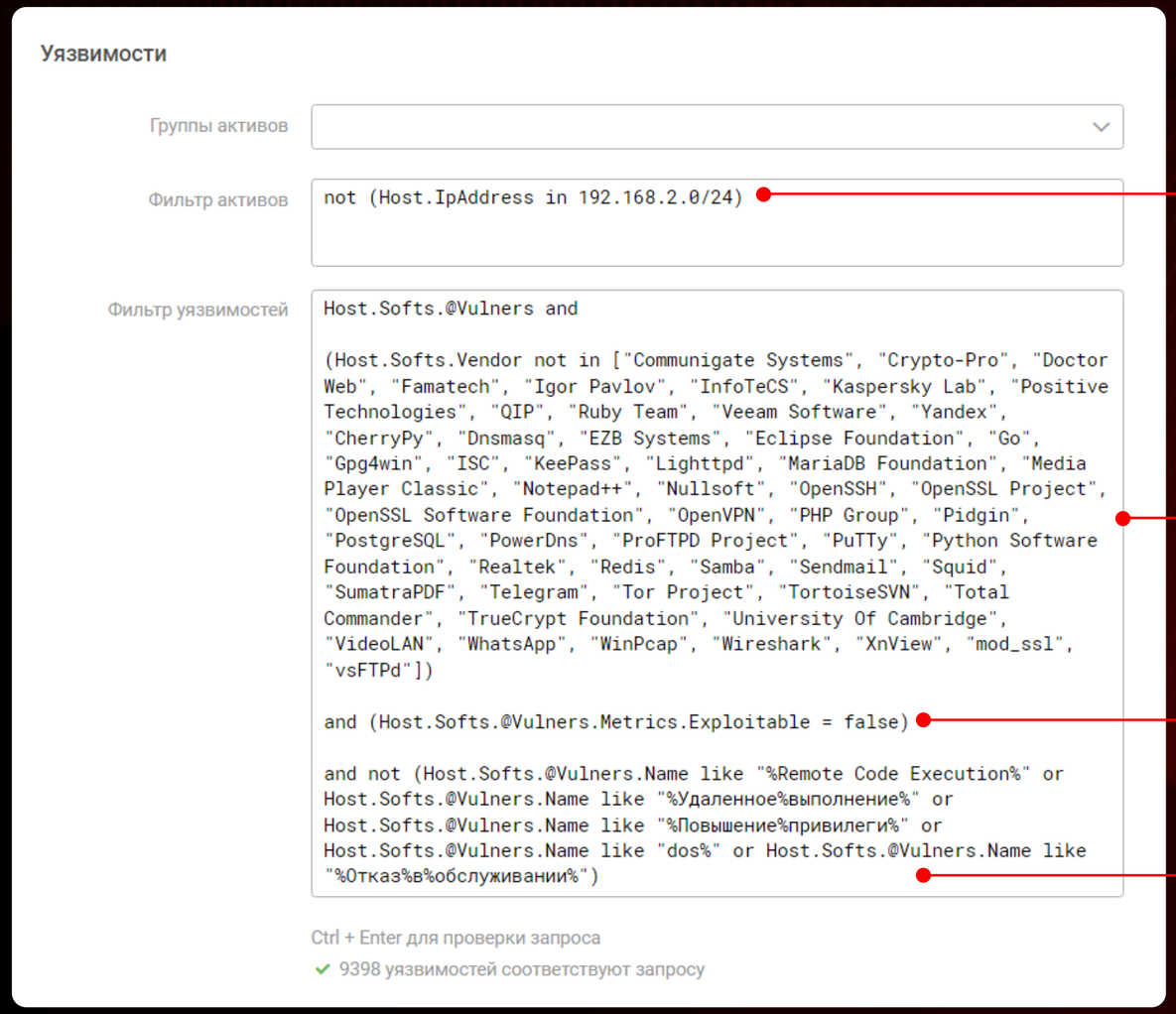
- Рекомендации НКЦКИ для принятия решения по обновлению критически значимого ПО
- Оценка уязвимостей по методике ФСТЭК

Алгоритм принятия решения по обновлению ПО



Скачать документ
с рекомендациями

Алгоритм принятия решения по обновлению ПО



Уязвимость **не** на периметре

Разработчик ПО **не** резидент России

Публичный эксплойт **отсутствует**

Тип уязвимости **не** RCE, LPE, DoS

Оценка уровня опасности уязвимостей по методике ФСТЭК

$$V = I_{cvss} \times I_{infr},$$

где I_{cvss} – показатель, характеризующий уровень опасности уязвимости;

I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационной системы.

2.6. Показатель I_{cvss} определяется путем расчета базовых, временных и контекстных метрик применительно к конкретной информационной системе по методике Common Vulnerability Scoring System (CVSS) 3.0 или 3.1[1].

2.7. Показатель I_{infr} определяется по следующей формуле:

$$I_{infr} = k * K + l * L + p * P, \text{ где}$$

K – показатель, характеризующий тип компонента информационной системы, подверженного уязвимости;

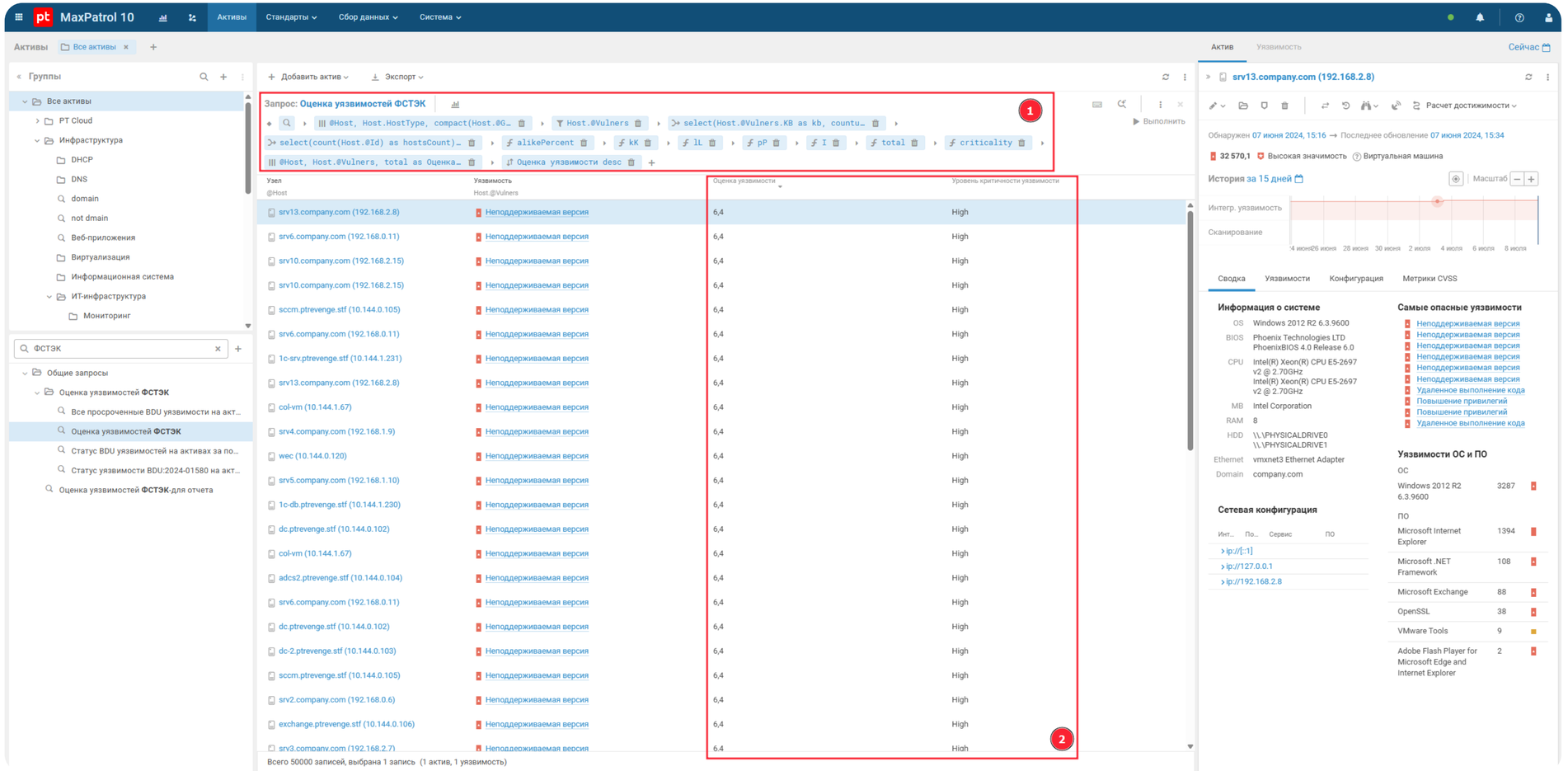
L – показатель, характеризующий количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов);

P – показатель, характеризующий влияние уязвимого компонента на защищенность периметра информационной системы;

k, l, p – весовые коэффициенты показателей.

№ п/п	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
1	7,0 ≤ V ≤ 10,0	Критичный
2	4,5 ≤ V < 7,0	Высокий
3	1,5 ≤ V < 4,5	Средний
4	V < 1,5	Низкий

Оценка уязвимостей по методике ФСТЭК в MaxPatrol VM



Спасибо!

Олег Кочетов

Лидер продуктовой практики
MaxPatrol VM, MaxPatrol HCC

okochetov@ptsecurity.com
+7 905 783 90 46
@Bednight

Новости о продуктах
Positive Technologies:
t.me/ptproductupdate

Телеграм-чат о MaxPatrol VM,
MaxPatrol SIEM и PT XDR:
t.me/MPSIEMChat