Владимир Ан
Пресейл-инженер

Как не пропустить критическую уязвимость?

MaxPatrol VM, MaxPatrol HCC, XSpider PRO

01

Про уязвимости ПО

Результаты пилотных проектов MaxPatrol VM

Среднее количество уязвимостей, обнаруженных в одном пилотном проекте

3%

уязвимостей являются крайне опасными. При этом они могут не иметь максимальной оценки по CVSS

«Как выстроен процесс управления уязвимостями в российских компаниях», Positive Technologies

31 000+

уязвимостей всех типов

861

трендовая уязвимость (их нужно устранить как можно скорее)

9000+

критически опасных уязвимостей по оценке CVSS

42

трендовые уязвимости на активах высокой значимости

Уязвимости в тренде

Киберпандемия Log4Shell

- Затронуты миллионы устройств по всему миру
- Существует более 60 эксплойтов для уязвимости
- Экспертами зафиксировано около 100 попыток атак в минуту

45 минут

потребуется на взлом, если на периметре компании есть трендовая уязвимость

80%

критически опасных уязвимостей по оценке CVSS

Трендовые уязвимости, обнаруженные в 2025 году, с публичными эксплойтами

- RARLAB CVE-2025-6218
- Microsoft CVE-2025-53770
- Apache CVE-2024-384757
- Kubernetes CVE-2025-1974
- Palo Alto Networks CVE-2025-0108

Что мешает эффективно работать с уязвимостями

Нет полноты охвата ИТ-инфраструктуры

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

Уязвимостей слишком много

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

Нужно договариваться с ИТ-отделом

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

Как должно быть?

Процесс VM

Плановая обработка уязвимостей

- В ИТ-отделе принят патч-менеджмент, не зависящий от службы ИБ
- Служба ИБ следит не за появлением и устранением уязвимостей, а за соблюдением договоренностей с ИТ-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 ИТ-отдел договариваются отдельно

Управление уязвимостями

1

Следим за постоянной актуализацией данных об активах

2

Оцениваем и классифицируем активы

3

Договариваемся с отделом ИТ и фиксируем политики

4

Система определяет и сортирует уязвимости

5

Следим за устранением уязвимостей и за соблюдением политик

6

Проверка устранения уязвимостей

Asset Management
Управление активами

Выделение особо опасных уязвимостей

Оперативное реагирование на них вне процесса

02

Решение Positive Technologies

MaxPatrol VM

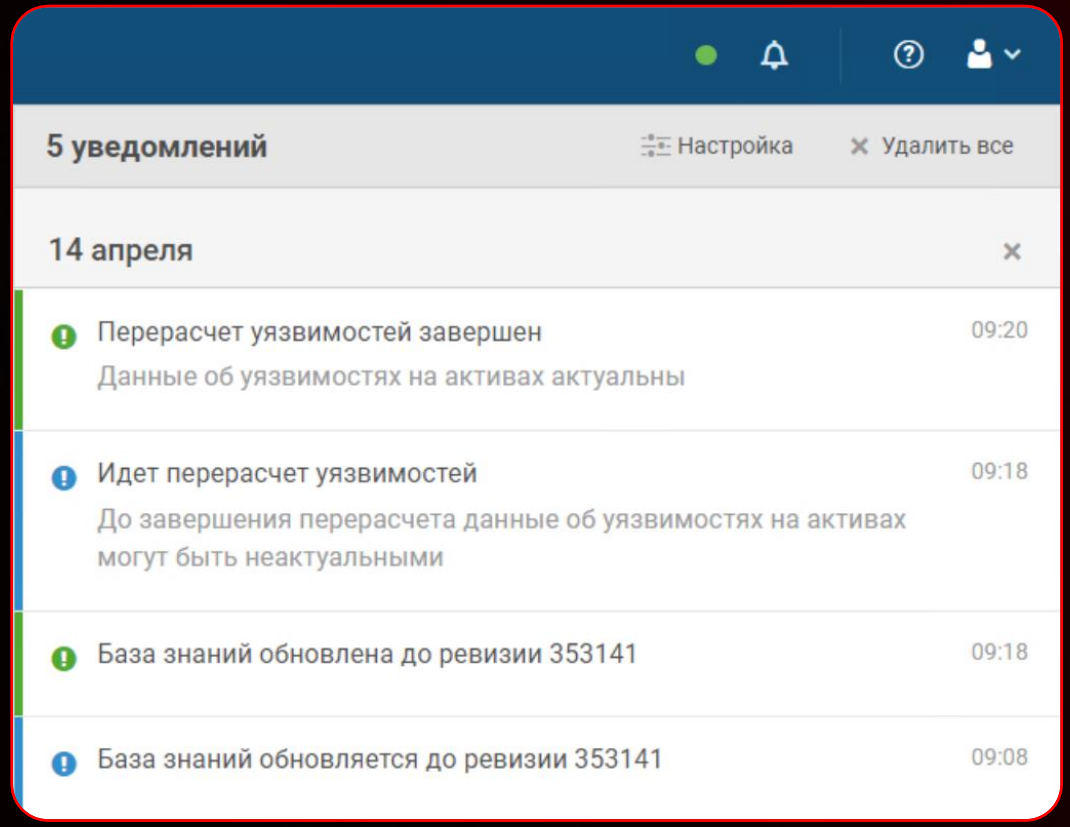
Единственное VM-решение с гарантированным сроком доставки информации о самых опасных, трендовых уязвимостях — 12 часов

Это позволит устранить критически опасные уязвимости быстрее, чем злоумышленники успеют разработать для них эксплойты

MaxPatrol VM не даст хакерам шансов использовать уязвимости ПО для взлома

Выявление уязвимостей без повторного сканирования

Информация об уязвимостях
актуализируется автоматически
после обновления базы знаний



MaxPatrol VM

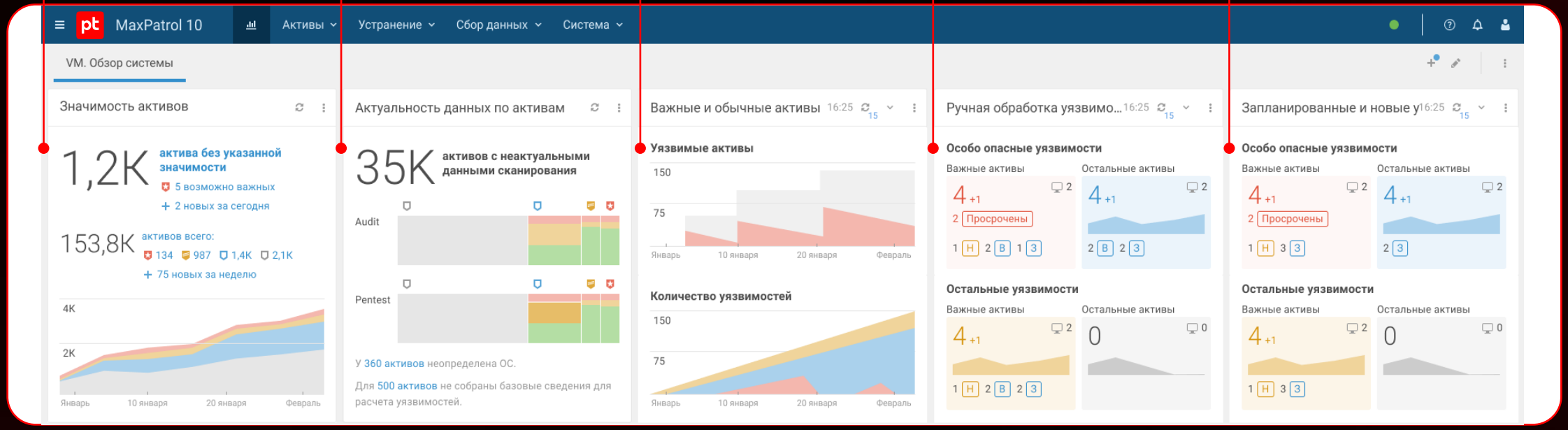
MaxPatrol VM находит все активы в сети. Приоритизируйте их, чтобы знать, что важно

Получайте свежую информацию об активах и их уязвимостях. Задайте политики сканирования

Контролируйте, что происходит на важных активах. Отслеживайте появление новых активов

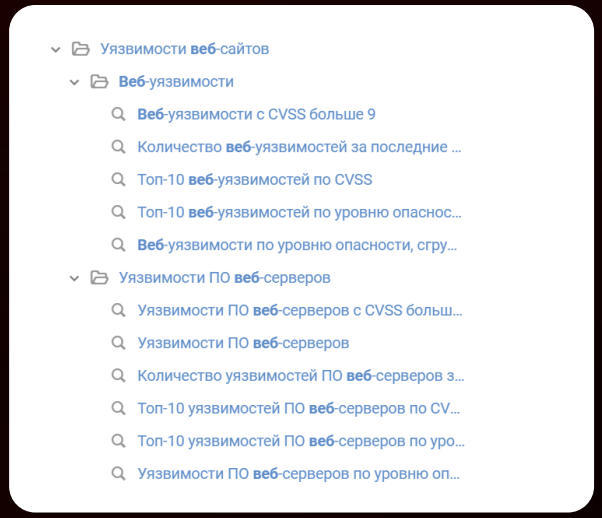
Обычные уязвимости исправляет ИТ-отдел в рамках политик. Специалист по ИБ контролирует только особо опасные недостатки

Специалист по ИБ отслеживает нарушения политик. Контролируйте своевременное устранение недочетов

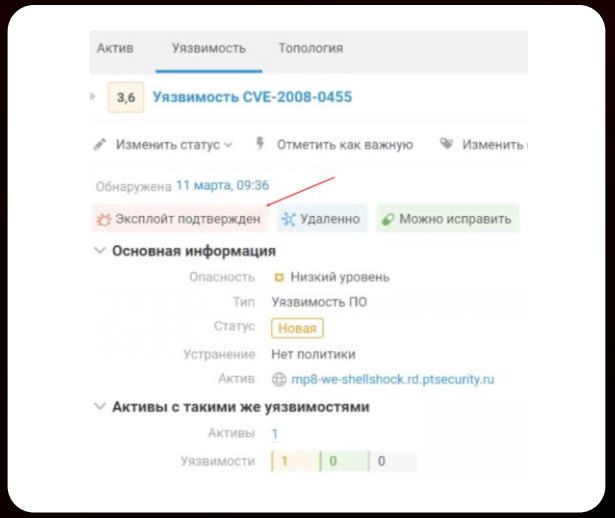


Сканирование веб-приложений

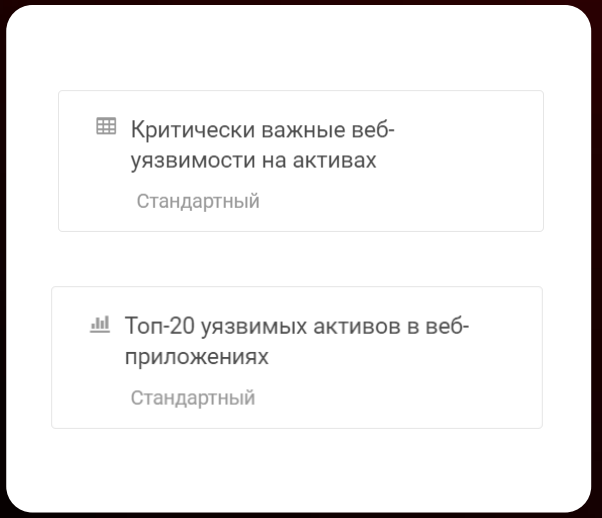
Новые системные запросы



Подтверждение наличия уязвимостей скриптами

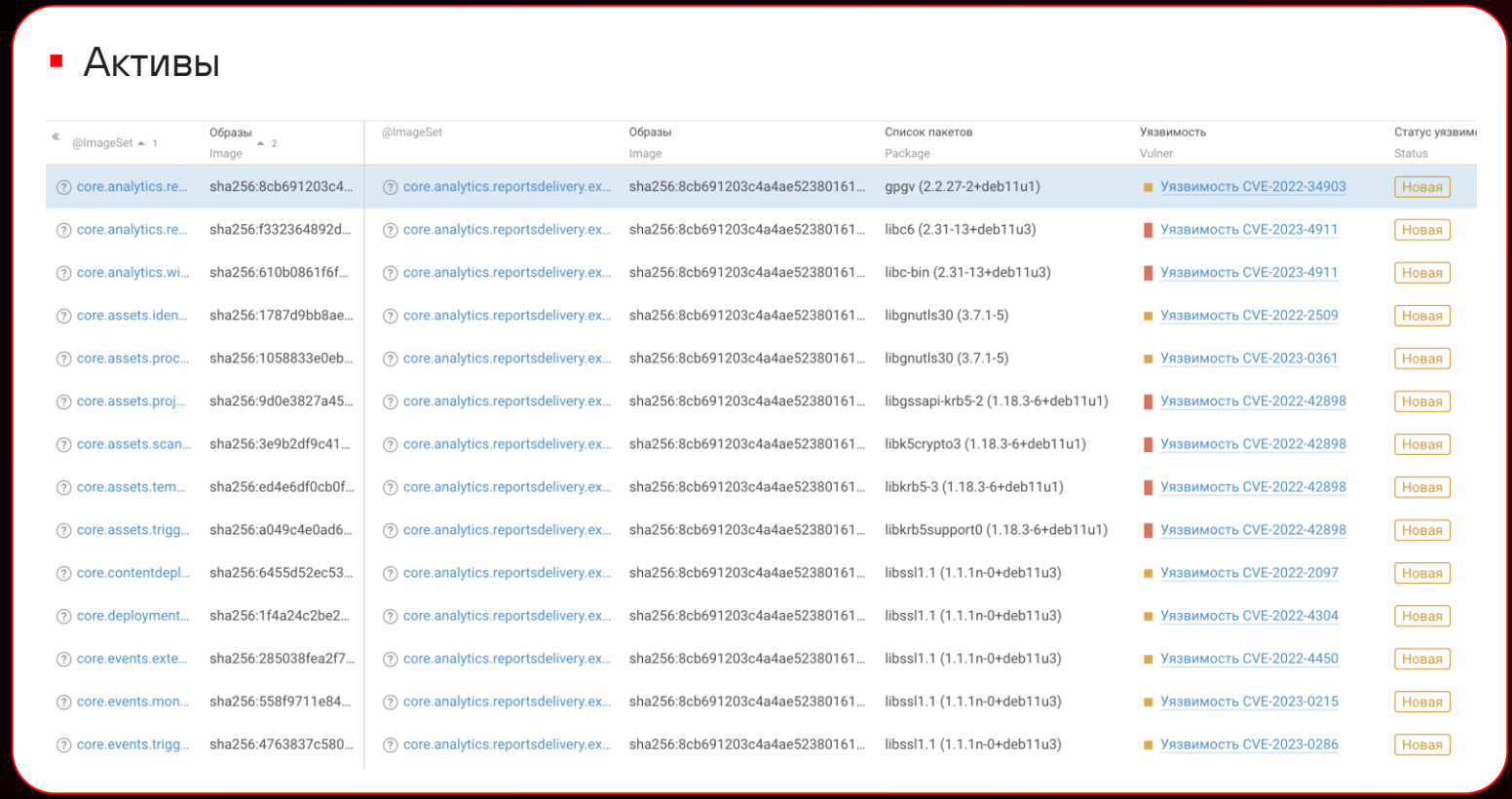


Новые системные дашборды



Уязвимости пакетов в Docker-контейнерах

MaxPatrol VM начиная с версии 2.5 рассчитывает уязвимости в пакетах для ОС Ubuntu, Debian и Alpine Linux, обнаруженные в Docker-контейнерах



@ImageSet	Образы Image	@ImageSet	Образы Image	Список пакетов Package	Уязвимость Vulner	Статус уязвим Status
core.analytics.re...	sha256:8cb691203c4...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	gpgv (2.2.27-2+deb11u1)	Уязвимость CVE-2022-34903	Новая
core.analytics.re...	sha256:f332364892d...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libc6 (2.31-13+deb11u3)	Уязвимость CVE-2023-4911	Новая
core.analytics.wi...	sha256:610b0861f6f...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libc-bin (2.31-13+deb11u3)	Уязвимость CVE-2023-4911	Новая
core.assets.iden...	sha256:1787d9bb8ae...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libgnutls30 (3.7.1-5)	Уязвимость CVE-2022-2509	Новая
core.assets.proc...	sha256:1058833e0eb...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libgnutls30 (3.7.1-5)	Уязвимость CVE-2023-0361	Новая
core.assets.proj...	sha256:9d0e3827a45...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libgssapi-krb5-2 (1.18.3-6+deb11u1)	Уязвимость CVE-2022-42898	Новая
core.assets.scan...	sha256:3e9b2df9c41...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libk5crypto3 (1.18.3-6+deb11u1)	Уязвимость CVE-2022-42898	Новая
core.assets.tem...	sha256:ed4e6df0cb0f...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libkrb5-3 (1.18.3-6+deb11u1)	Уязвимость CVE-2022-42898	Новая
core.assets.trigg...	sha256:a049c4e0ad6...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libkrb5support0 (1.18.3-6+deb11u1)	Уязвимость CVE-2022-42898	Новая
core.contentdepl...	sha256:6455d52ec53...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libssl1.1 (1.1.1n-0+deb11u3)	Уязвимость CVE-2022-2097	Новая
core.deployment...	sha256:1f4a24c2be2...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libssl1.1 (1.1.1n-0+deb11u3)	Уязвимость CVE-2022-4304	Новая
core.events.exte...	sha256:285038fea2f7...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libssl1.1 (1.1.1n-0+deb11u3)	Уязвимость CVE-2022-4450	Новая
core.events.mon...	sha256:558f9711e84...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libssl1.1 (1.1.1n-0+deb11u3)	Уязвимость CVE-2023-0215	Новая
core.events.trigg...	sha256:4763837c580...	core.analytics.reportsdelivery.ex...	sha256:8cb691203c4a4ae52380161...	libssl1.1 (1.1.1n-0+deb11u3)	Уязвимость CVE-2023-0286	Новая

03

Оценка уязвимостей по методике ФСТЭК

Оценка уровня критичности уязвимостей по методике ФСТЭК

$$V = I_{cvss} \times I_{infr} \times (I_{at} + I_{imp}),$$ где

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

I_{infr} – показатель, характеризующий влияние уязвимости программных, программно-аппаратных средств на функционирование информационных систем;

I_{at} – показатель, характеризующий возможность эксплуатации уязвимости программных, программно-аппаратных средств в информационных системах;

I_{imp} - показатель, характеризующий последствия эксплуатации уязвимости программных, программно-аппаратных средств в информационных системах.

13. В качестве показателя I_{cvss} берется значение, рассчитанное разработчиком (вендором) программного обеспечения по базовым метрикам в соответствии с методикой Common Vulnerability Scoring System[2] (CVSS) 3.1, которая содержится в Банке данных угроз безопасности информации ФСТЭК России[3], а также иных известных базах данных уязвимостей. В случае отсутствия для уязвимости оценки уровня опасности по базовым метрикам в соответствии с методикой Common Vulnerability Scoring System (CVSS) 3.1, специалист самостоятельно определяет версию CVSS, по которой производится оценка критичности уязвимости.

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

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

K – показатель, характеризующий тип компонента информационной системы[4], 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 или периметра сегмента информационной системы (в случае сегментирования информационной системы);

k, l, p – весовые коэффициенты показателей (значения приведены в таблице 1 настоящей Методики).

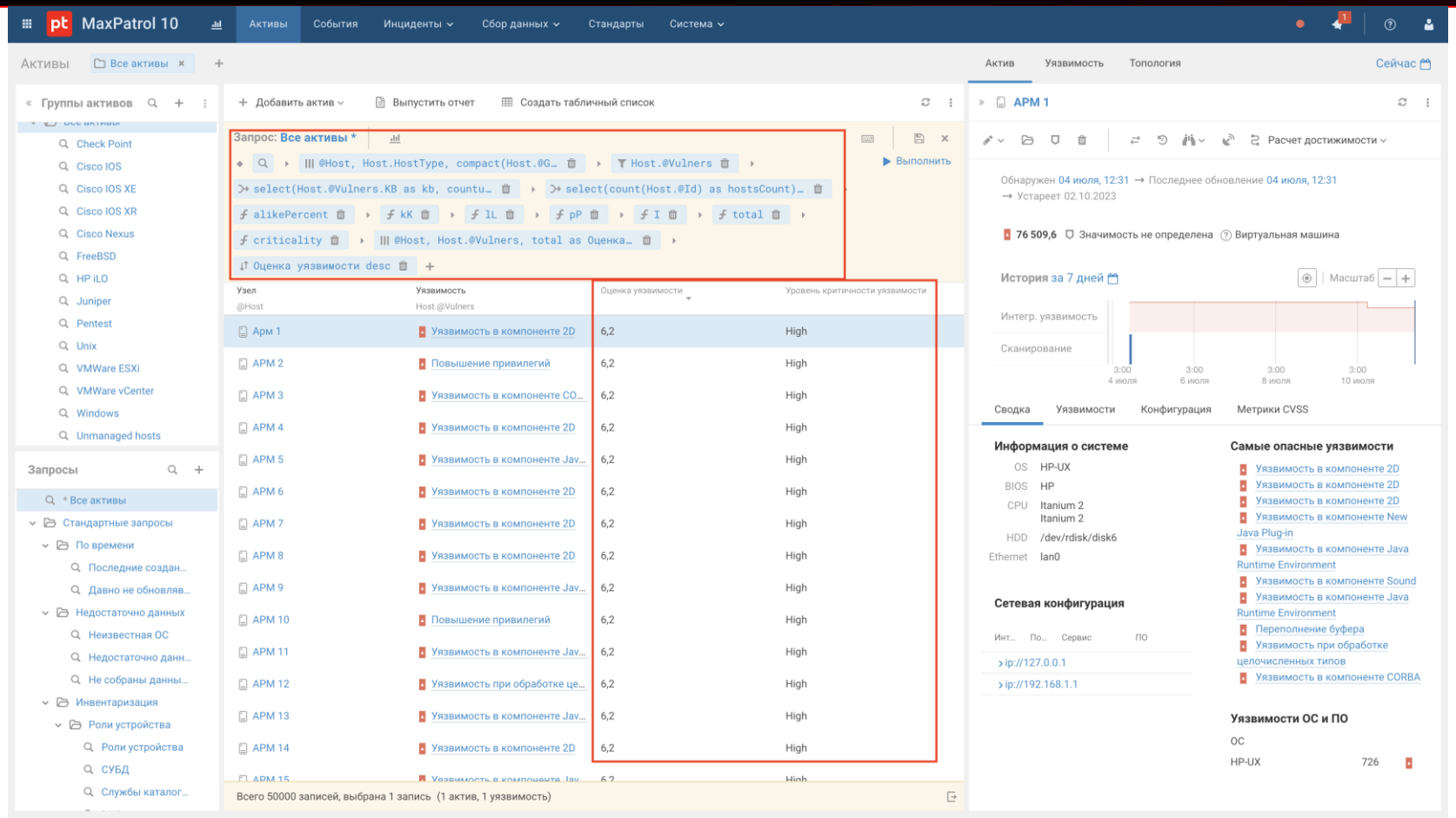
№ п/п	Суммарное количество баллов уязвимости	Оценка уровня критичности уязвимости
1	$7,0 \leq V \leq 10,0$	Критичный
2	$4,5 \leq V < 7,0$	Высокий
3	$1,5 \leq V < 4,5$	Средний
4	$V < 1,5$	Низкий

Утвержден ФСТЭК России. 30 июня 2025 г.

Оценка уровня критичности уязвимостей по методике ФСТЭК

	ПОКАЗАТЕЛЬ	ВЕС	ЗНАЧЕНИЕ	ОЦЕНКА	ИТОГ (k × Ki, I × Lj, p × Pm)
1	Тип компонента информационной системы, подверженного уязвимости (K)	0,4	Уязвимости подвержены компоненты информационной системы, обеспечивающие реализацию критически важных процессов (бизнес-процессов), функций, полномочий	1	0,4
			Уязвимости подвержены серверы	0,8	0,32
			Уязвимости подвержено телекоммуникационное оборудование, система управления сетью передачи данных	0,8	0,32
			Уязвимости подвержены автоматизированные рабочие места	0,5	0,20
			Уязвимости подвержены другие компоненты	0,5	0,20
2	Количество уязвимых компонентов информационной системы (автоматизированных рабочих мест, серверов, телекоммуникационного оборудования, средств защиты информации и других компонентов) (L)	0,2	Более 70% от общего числа компонентов в информационной системе	1	0,2
			50–70% от общего числа компонентов в информационной системе	0,8	0,16
			10–50% от общего числа компонентов в информационной системе	0,6	0,12
			Менее 10% от общего числа компонентов в информационной системе	0,5	0,10
3	Влияние на эффективность защиты периметра системы, сети (P)	0,4	Уязвимое программное, программно-аппаратное средство доступно из интернета	1	0,4
			Уязвимое программное, программно-аппаратное средство недоступно из интернета	0,5	0,2

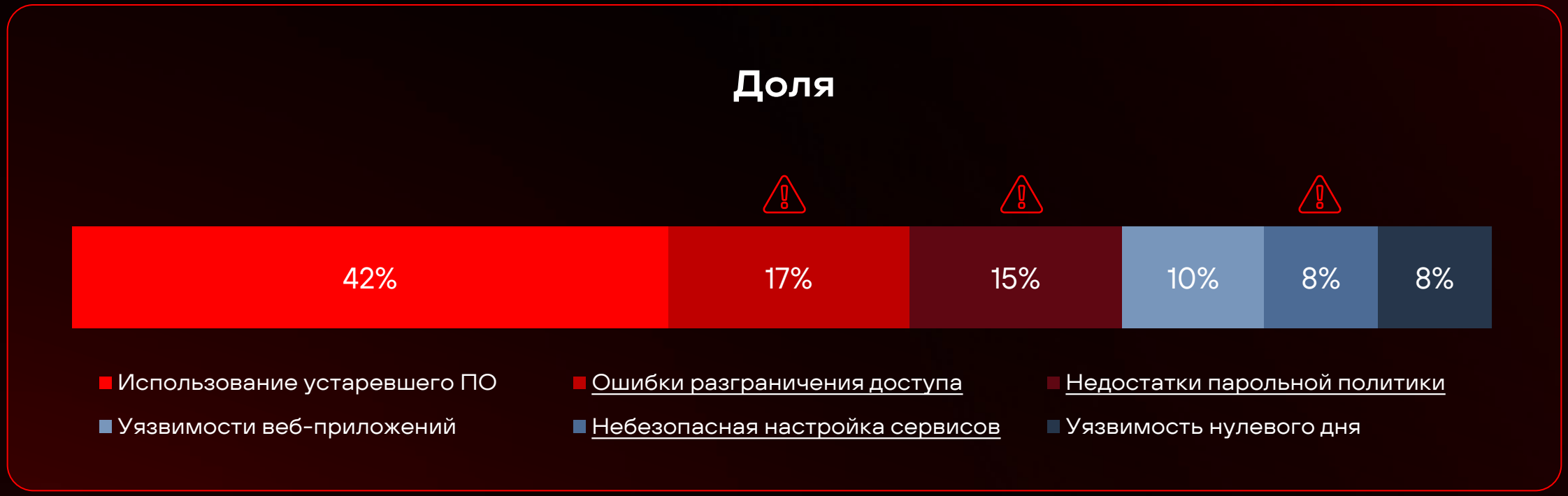
Оценка уровня критичности уязвимостей по методике ФСТЭК



04

Про уязвимости конфигураций

40% уязвимостей — это проблемы в конфигурациях и недостатки контроля доступа



Что мешает устранять уязвимости конфигураций

Их сложно обнаружить

- Нет единого реестра с уязвимостями конфигураций
- Нельзя обнаружить простым сканированием
- В отличие от уязвимостей стороннего ПО, конфигурационные уязвимости могут существовать только в одной среде

Неясно, как настроить правильно

- Необходимо глубоко разбираться в ландшафте инфраструктуры и технических особенностях ПО и ОС
- Нет понимания, какие ошибки в параметрах наиболее опасны для конкретной инфраструктуры
- Нет готовых патчей, нельзя просто установить готовое обновление

Нужно договариваться с ИТ-отделом

- Нет понимания, зачем что-то менять, если все и так работает
- Необходимо каждый раз объяснять ИТ-специалистам, зачем нужно менять параметры
- Нет возможности контролировать статус и сроки устранения несоответствий

MaxPatrol HCC

Ваш инструмент для харденинга инфраструктуры и комплаенс-контроля

Полная инвентаризация инфраструктуры

Отслеживайте состояние всех активы в инфраструктуры благодаря технологии Asset Management в MaxPatrol HCC

Проверка активов на соответствие требованиям

Определяйте необходимые стандарты для технических и программных средств компании, а MaxPatrol HCC проконтролирует их выполнение на активах сети

Управление безопасностью конфигураций систем

Выявляйте ошибки в конфигурации ИТ-активов, настраивайте параметры устройств и отображение актуальных данных об активах, чтобы обезопасить компанию от взлома

Уменьшение поверхности атаки

Выявляйте некорректные параметры активов (слабые пароли, незащищенные системы, неконтролируемый гостевой доступ и т. п.), чтобы снизить уязвимость инфраструктуры

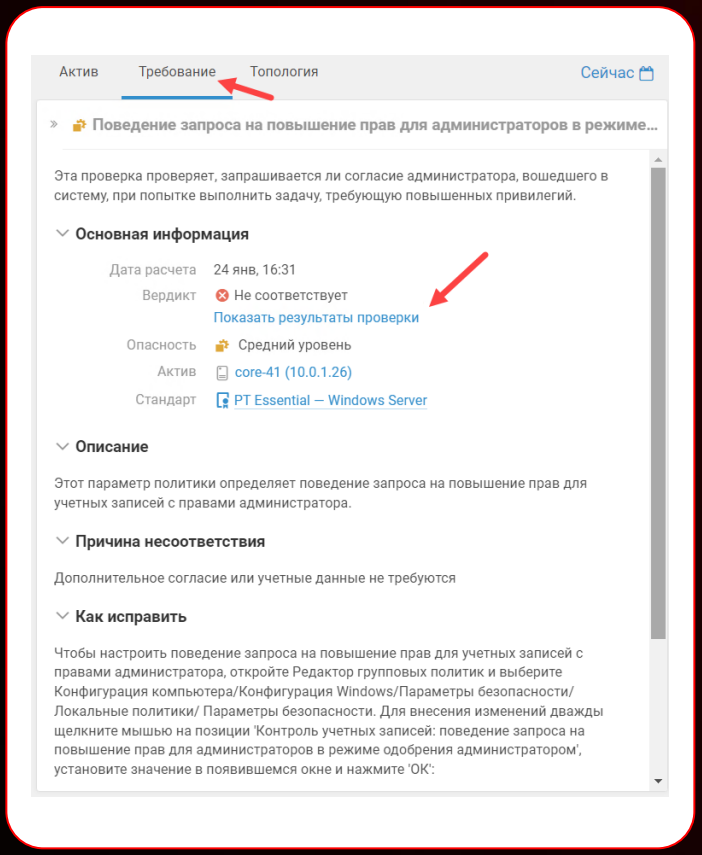
Что делает MaxPatrol HCC

1. Рассчитывает применимость требования на активе

2. Показывает результат проверки и уровень опасности конфигурации

3. Дает объяснение причины несоответствия

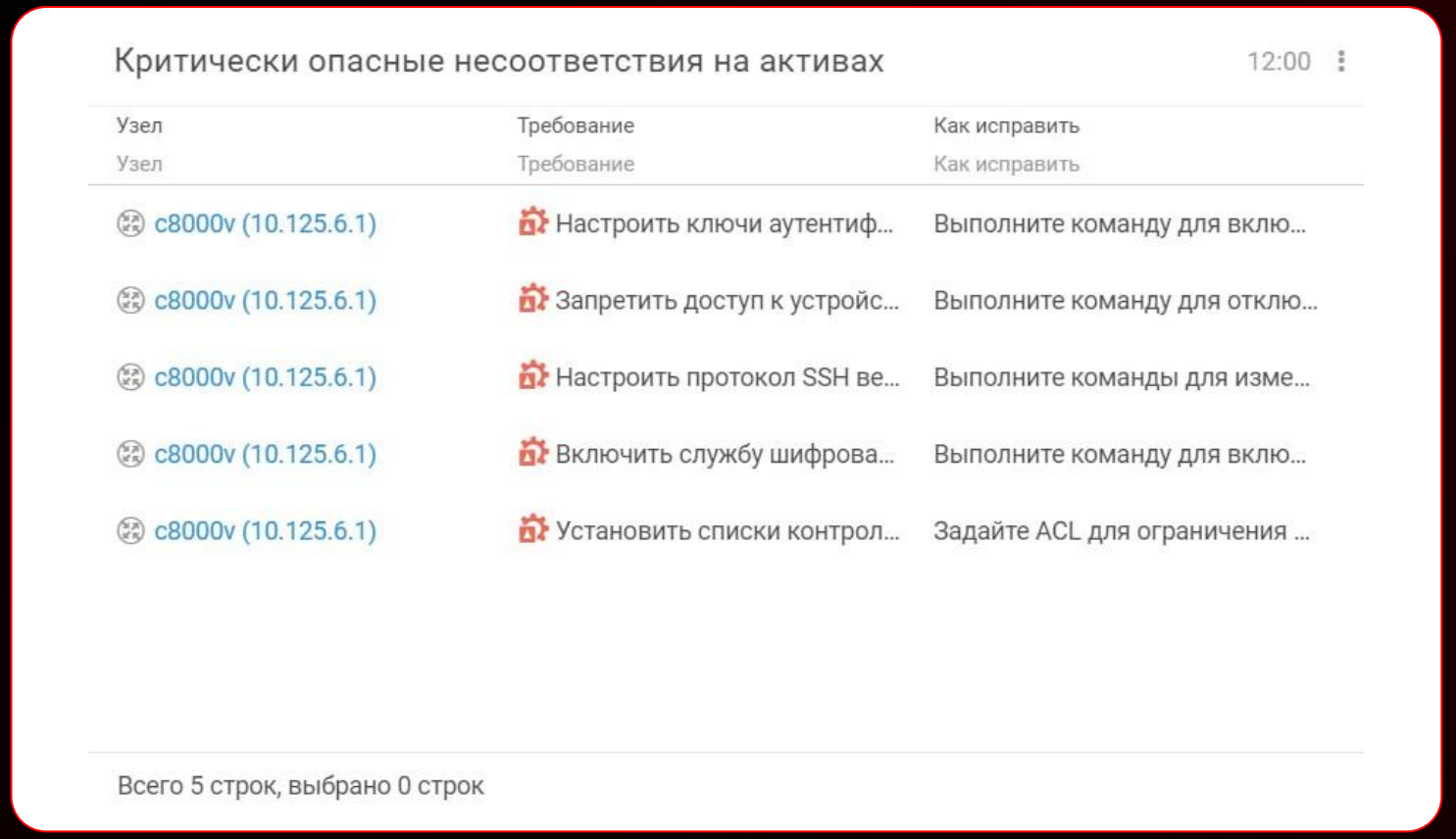
4. Дает рекомендации по исправлению и правильной настройке конфигурации



Приоритизированный список несоответствия на активах

MaxPatrol HCC находит критически опасные несоответствия на активах

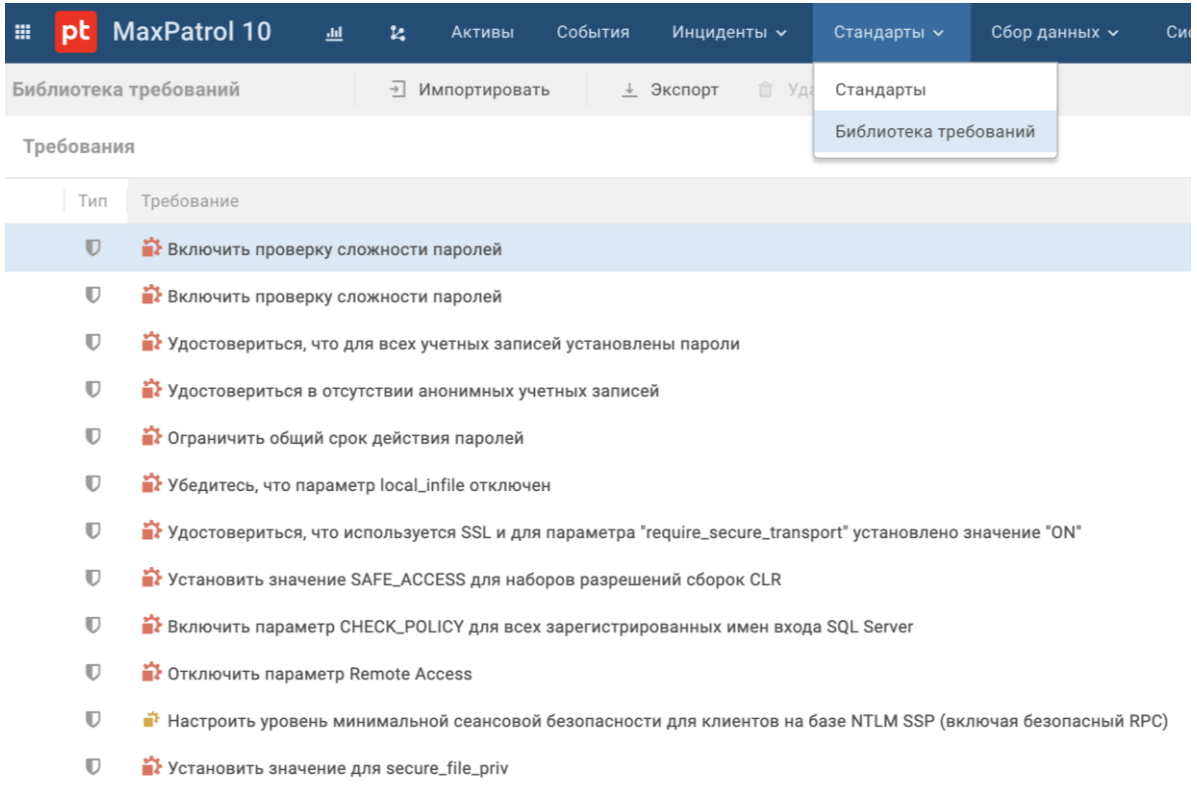
Вы не пропустите критически опасные уязвимости конфигураций



Собственные требования безопасности

Кастомизируйте готовые требования под свои нужды

Добавляйте любые внутренние требования безопасности в продукт и проверяйте их выполнение на активах



Соответствие требованиям ФСТЭК по безопасности Linux

Многолетняя экспертиза по безопасности ядра Linux теперь в MaxPatrol HCC

- Наш набор рекомендаций по безопасной настройке ядра Linux вошел в методический документ ФСТЭК России от 25 декабря 2022 года
- Более 20 ключевых параметров ядра, корректная настройка которых существенно усложняет задачу атакующему

Методический документ ФСТЭК России от 25 декабря 2022 года

Результативность с MaxPatrol HCC

Реальная безопасность

Созданы на основе мировых стандартов безопасности и опыте экспертов Positive Technologies в проведении пентестов. Содержат оптимальный набор проверок, которые повышают защищенность систем

Харденинг инфраструктуры

Усиление безопасности систем и сервисов за счет устранения уязвимостей, связанных с ошибками конфигураций, и уменьшения количества возможных точек атаки

Понятные рекомендации

Конкретные советы по устранению рисков, которые помогут укрепить защиту компании без значительных изменений инфраструктуры

Поддержка распространенного ПО и ОС

Более 25 стандартов для безопасной настройки самых распространенных операционных систем, в том числе для Astra Linux, «РЕД ОС» и ОС «Альт»

Стандарты PT Essential

- PT Essential — Windows Desktop
- PT Essential — Windows Server
- PT Essential — Microsoft SQL Server
- PT Essential — Generic Linux
- PT Essential — Oracle Database
- PT Essential — VMware ESXi
- PT Essential — VMware vCenter
- PT Essential — Microsoft Exchange
- PT Essential — HP UX
- PT Essential — IBM AIX
- PT Essential — RHEL-based Linux

- PT Essential — Linux Kernel
- PT Essential — Docker
- PT Essential — Cisco IOS
- PT Essential — Cisco IOS XE
- PT Essential — Cisco ASA
- PT Essential — Cisco Nexus
- PT Essential — 1C-Bitrix
- PT Essential — CheckPoint GAiA
- PT Essential — Cisco IOS XR
- PT Essential — MariaDB
- PT Essential — MySQL

Устраняйте уязвимости ПО и конфигураций

Экспертиза Positive Technologies

Возможности

MaxPatrol VM

База знаний об уязвимостях

Построение процесса управления уязвимостями

- Обнаружение и приоритизация уязвимостей
- Контроль выявления и устранения уязвимостей

+

MaxPatrol HCC

Пакеты стандартов

Построение процессов комплаенс-контроля и харденинга

- Использование экспертных стандартов
- Возможность создавать свои требования

Основа

Технология
Asset Management

- Сбор полной информации об инфраструктуре
- Автоматическое определение активов, непрерывная актуализация данных, учет изменений

05

pt

XSpider PRO

XSpider PRO

Сканер безопасности нового поколения, который покажет полную картину уязвимостей в вашей инфраструктуре

Обнаруживает уязвимости в сети и системах

- Выявляет уязвимости на рабочих станциях, серверах и сетевых устройствах
- Анализирует популярные ОС (Windows, Linux) на наличие известных уязвимостей
- Сканирует веб-серверы и базы данных, чтобы выявить уязвимости, связанные с некорректными параметрами, устаревшими версиями ПО или избыточными правами доступа

Дает рекомендации по устранению

- После завершения сканирования продукт генерирует подробный отчет с полным перечнем обнаруженных уязвимостей
- Предоставляет информацию обо всех уязвимостях и рекомендации по их устранению

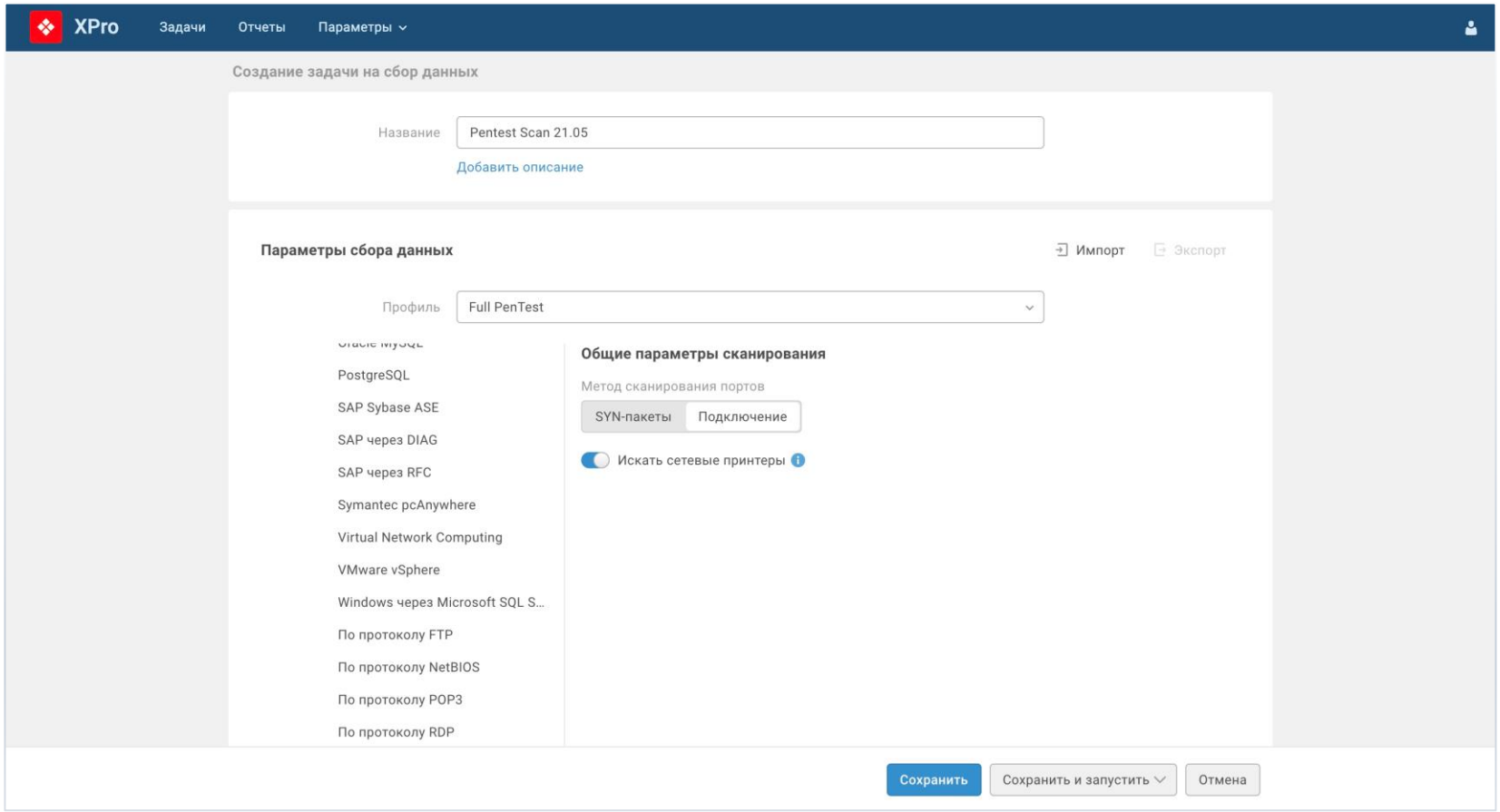
Что изменилось в сканере уязвимостей

	XSpider PRO	XSpider 7.8
Сканирование в режиме Pentest	+	+
Сканирование в режиме Audit	+	-
Поиск уязвимостей в веб-приложениях	+	+
Поиск уязвимостей в Docker-контейнерах	+	-
Актуализация информации о новых уязвимостях в поддерживаемом ПО	+	-
Поддержка нового ПО для поиска уязвимостей	+	-
Инвентаризация инфраструктуры	Инвентаризация инфраструктуры для выгрузки в отчет	Базовая инвентаризация
Консоль управления	Легкий веб-интерфейс	Тяжелый клиент
Установка на ОС	Linux	Windows
Лицензирование	По сканируемым IP-адресам и функциональности	По сканируемым IP-адресам
Сертификация ФСТЭК	Ожидаем к концу 2025 года	Заканчивается в конце 2025 года Техподдержка до конца 2030 года

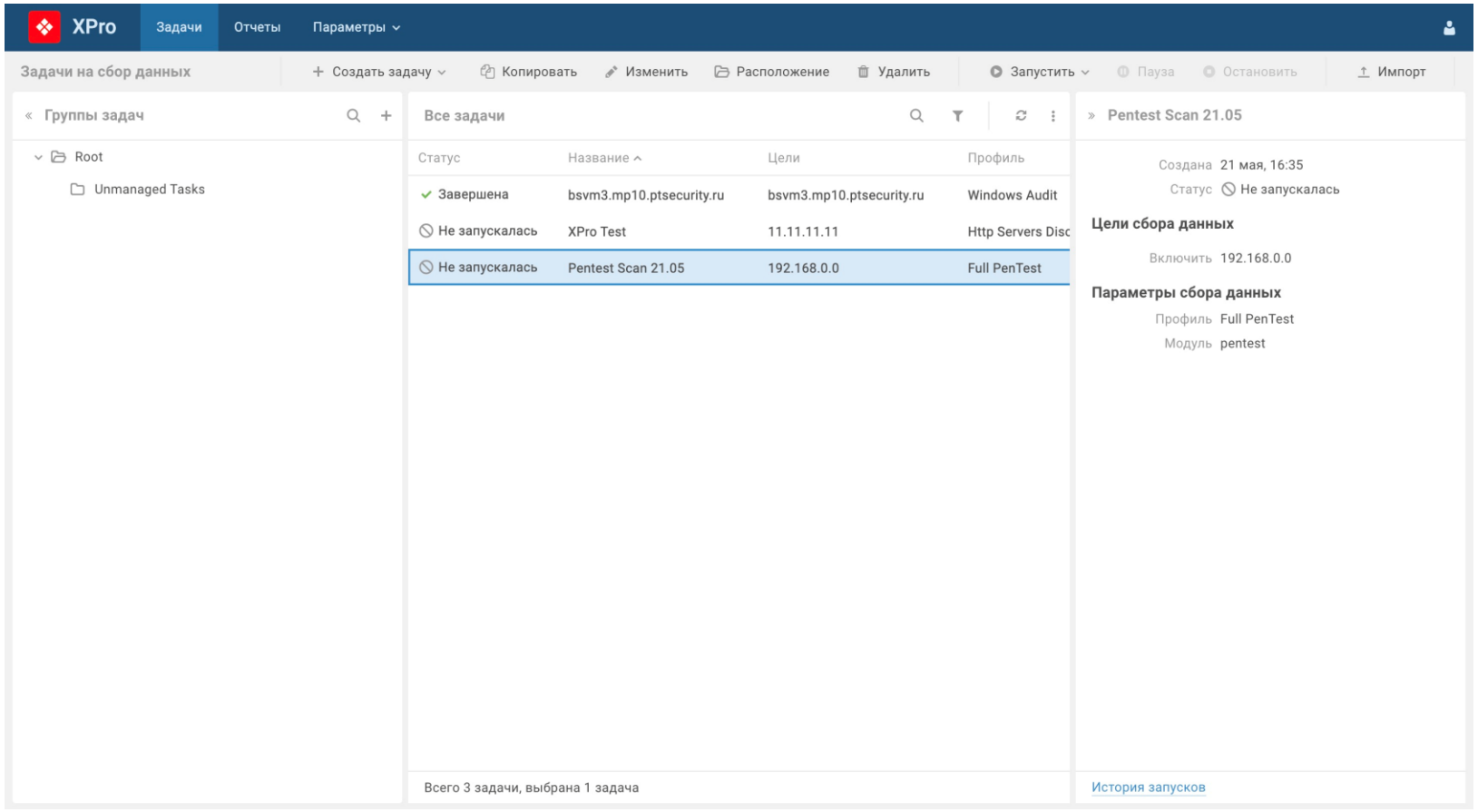
А если сравнить с MaxPatrol VM/HCC

	XSpider PRO	MaxPatrol VM/HCC
Сканирование в режиме Pentest	+	+
Сканирование в режиме Audit	+	+
Поиск уязвимостей в веб-приложениях	+	+
Поиск уязвимостей в Docker-контейнерах	+	+
Пополнение списка поддерживаемого ПО	+	+
Поддержка нового ПО для поиска уязвимостей	+	+
Инвентаризация инфраструктуры	Инвентаризация инфраструктуры для выгрузки в отчет	Полная инвентаризация и возможность самостоятельного расширения скриптов
Консоль управления	Веб-интерфейс	Веб-интерфейс
Лицензирование	По сканируемым IP-адресам и функциональности	По активам и дополнительной функциональности
Сертификация ФСТЭК России	Ожидаем к концу 2025 года	Действителен
Перерасчет уязвимостей без повторного сканирования	-	+
Группировка и определение критичности активов	-	+
Контроль устранения уязвимостей	-	+
Поддержка методологии ФСТЭК России для расчета критичности уязвимостей и алгоритма НКЦКИ	-	+
Поддержка трендовых уязвимостей	-	+
Проверка на соответствие требованиям ИБ и формирование рекомендаций по харденингу	-	+

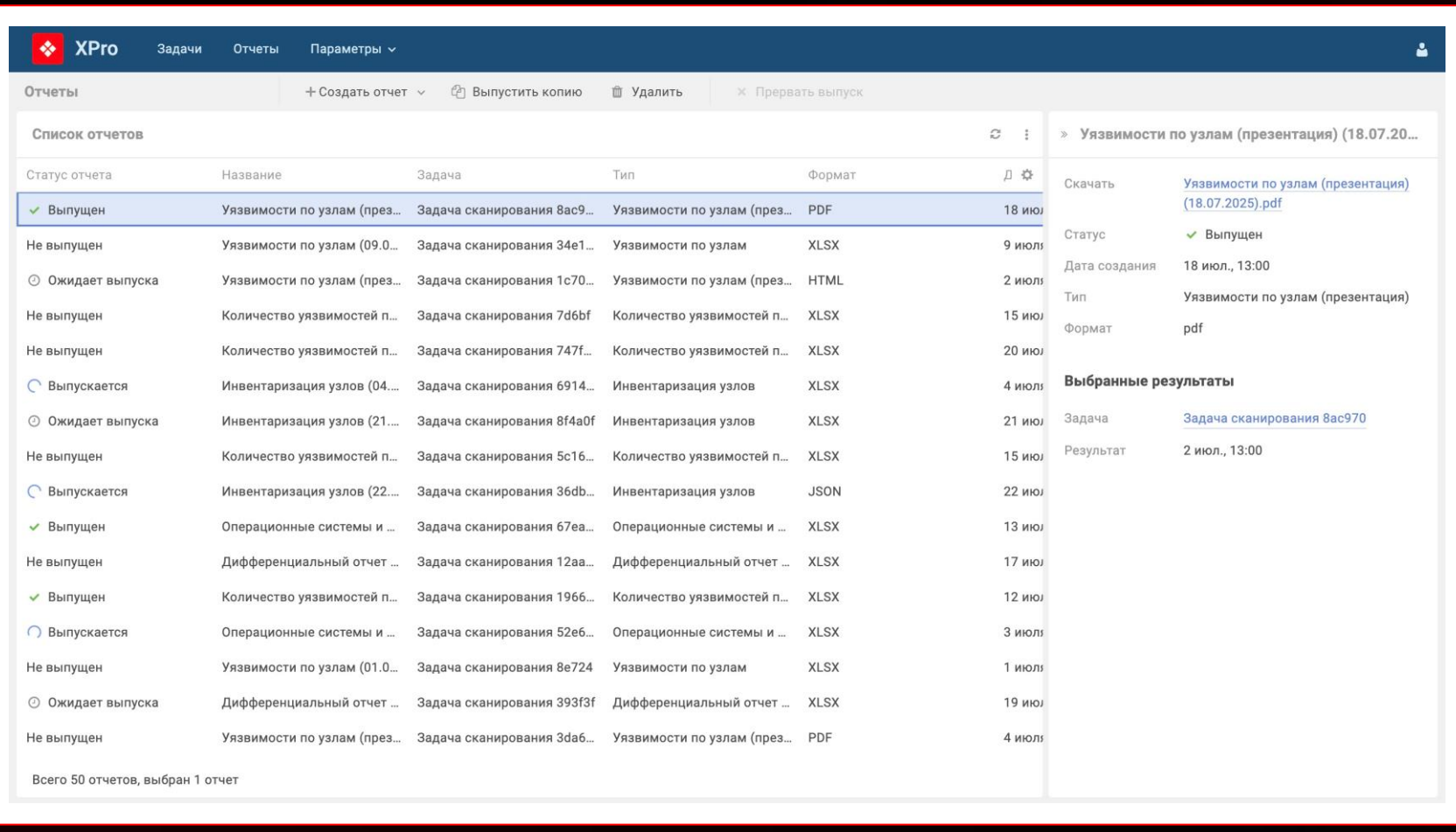
Создавайте задачи на сканирование



Отслеживайте статус задач



Выпускайте отчеты по итогам сканирования



Задать вопрос по теме выступления

pt@ptsecurity.com

ptsecurity.com

Спасибо!